Gerrit Hornung

Die digitale Identität

Rechtsprobleme von Chipkartenausweisen: Digitaler Personalausweis, elektronische Gesundheitskarte, JobCard-Verfahren

Dieses Dokument entspricht ab der folgenden Seite – auch hinsichtlich der insoweit zitierbaren Seitenzahlen – der vergriffenen Buchveröffentlichung:

Gerrit Hornung, Die digitale Identität. Rechtsprobleme von Chipkartenausweisen: Digitaler Personalausweis, elektronische Gesundheitskarte, JobCard-Verfahren. Reihe „Der elektronische Rechtsverkehr“, hrsg. von Prof. Dr. Alexander Roßnagel in Zusammenarbeit mit dem TeleTrusT Deutschland e.V., Band 10, Nomos Verlagsgesellschaft, Baden-Baden 2005, ISBN 3-8329-1455-2

Vorwort des Herausgebers

Gegenstand der Arbeit ist die Verwendung von Chipkarten als Ausweise. In diesem Verwendungszusammenhang darf die Chipkarte nicht nur als ein kleiner tragbarer Prozessor zur Speicherung und Verarbeitung von Daten gesehen werden. Chipkarten sind zugleich die sichtbaren und greifbaren verteilten Bestandteile mehrerer, viele Teilnehmer umfassenden und verbindenden Infrastrukturen. Die Chipkarte kann als ein auf den Einzelnen personalisierter Träger von Identitätsinformationen Teil einer Identifizierungs- und Kontrollinfrastruktur sein. In dieser Funktion kann sie durch das Speichern von Wissensdaten oder Daten zu biometrischen Merkmalen Bestandteil automatisch arbeitender Überprüfungsverfahren sein. Durch die Aufnahme von automatisch prüfbaren Berechtigungen kann sie außerdem Teil einer Infrastruktur sein, die Möglichkeiten zur elektronischen Kommunikation, zum Zugriff auf Daten und Rechner, zur Vornahme von Handlungen, zum Betreten von Räumen und zu ähnlichen Maßnahmen eröffnet oder verwehrt. Im Rahmen von „Public-Key-Infrastructures“ können Chipkarten außerdem als Träger von geheimen und öffentlichen Schlüsseln und von Zertifikaten die entscheidenden Bestandteile sein, um die Unterschrift ersetzende elektronische Signaturen zu erzeugen und zu prüfen oder um elektronische Daten zu verschlüsseln und zu entschlüsseln.

Chipkarten werden bereits vielfach genutzt, um solche Infrastrukturen aufzubauen. Auch die Bundesrepublik Deutschland will sich ihrer bedienen, um die genannten Funktionen für staatliche Zwecke nutzen zu können. Die wichtigsten Projekte sind in diesem Zusammenhang der digitale Personalausweis, die elektronische Gesundheitskarte und die JobCard. Der digitale Personalausweis soll im Chipkartenformat ausgegeben werden und sowohl einen Chip als auch die bisherigen Aufdrucke enthalten. Im Chip sollen die bisherigen Ausweisdaten als auch weitere biometrische Daten gespeichert sein. Auf Antrag soll er auch die Möglichkeit bieten, zu signieren, sich zu authentifizieren und Daten zu ver- und entschlüsseln. Die elektronische Gesundheitskarte soll den Krankenversicherten ausweisen, als Träger eines elektronischen Rezepts dienen und auf freiwilliger Basis Träger medizinischer Informationen sein. Die JobCard, für die jede qualifizierte Signaturkarte genutzt werden kann, soll bei einem Antrag auf Arbeitslosengeld den Zugriff auf die zentral gespeicherten Daten des Antragstellers frei schalten.

In all diesen Fällen ist die Chipkarte auf einen Bürger oder Versicherten personalisiert. Sie und die in ihr gespeicherten Identitätsdaten repräsentieren diesen im Rahmen der jeweiligen Infrastrukturen. Sie sind Teile umfassender Netzwerke aus Ausgabestellen, Kontrollstellen, Kommunikationsverbindungen, Datenbanken und Verarbeitungsprozessen. Diese technisch gestützten Infrastrukturen sollen die Identifizierung mit Hilfe von Personalausweisen sicherer machen, die medizinische Versorgung verbessern und die Prüfung der Arbeitsgeldberechtigung beschleunigen. Neben diesen qualitativen Verbesserungen sollen sie auch erhebliche finanzielle Einsparungen bewirken. Sie werden jedenfalls im Gesundheitswesen, in der Arbeitsverwaltung und in allen Fällen der Identifizierung von Personen die Informationsverarbeitung und die Arbeitsprozesse für alle Beteiligten erheblich verändern.

Durch die Chipkarten gestützten Identifikations-Infrastrukturen werden die Verwirklichungsbedingungen für Grundrechte und verfassungsrechtliche Ziele wie Sicherheit, Gesundheitsversorgung und soziale Sicherung nachhaltig verändert. Sollen diese Grundrechte und Verfassungsziele auch unter den technisch veränderten Umständen in dem bisher gewährleisteten Umfang gewahrt werden, sind einerseits Anpassungen der technischen und organisatorischen Systeme an rechtliche Vorgaben und andererseits Fortentwicklungen des

Rechts entsprechend den Möglichkeiten und Risiken der neuen Infrastrukturen notwendig. Aus diesem Grund sind rechtswissenschaftliche Untersuchungen der rechtlichen Grundlagen und Anforderungen an Chipkartenausweise und der hinter ihnen stehenden Infrastrukturen sowie rechtswissenschaftliche Vorschläge zur verfassungskonformen Gestaltung dieser Chipkartenprojekte dringend erforderlich.

Daher ist es sehr verdinstvoll, dass Herr Hornung mit seiner Arbeit die rechtlichen Chancen und Risiken künftiger chipkartengestützter Identitätsinfrastrukturen allgemein und in vergleichender Weise insbesondere der drei von der Bundesregierung ins Werk gesetzten oder geplanten Chipkartenprojekte untersucht. Er widmet sich dabei vor allem den Fragen, wie diese Chipkartenprojekte mit Blick auf Grundrechte und Verfassungsziele zu bewerten sind und wie sie durch rechtsverträgliche Technikgestaltung und technikadäquate Rechtsfortbildung beeinflusst werden können.

Indem er die Chipkartenprojekte am Maßstab des geltenden Rechts untersucht, greift Herr Hornung viele bisher offene oder noch umstrittene Fragen des Datenschutzrechts auf und bietet Lösungen für künftige Probleme der Datenschutzpraxis. Indem er die technische und organisatorische Umsetzung der Projekte aus Sicht der Rechtswissenschaften untersucht und rechtlich angeleitete Gestaltungsvorschläge entwirft, bietet er der anwendungsorientierten Forschung und Entwicklung von Chipkartenprojekten allgemein und den für diese Projekte Verantwortlichen insbesondere wertvolle praxisrelevante Hinweise. Durch Vorschläge zur Rechtsfortbildung und durch die Untersuchung von mit diesen Projekten verbundenen Akzeptanzfragen behandelt er für die Rechtspolitik wichtige relevante Fragen.

Für unser Gemeinwesen ist zu hoffen, dass die Entscheidungsträger in Politik, Wirtschaft und Verwaltung die Hiweise dieser Arbeit zur Kenntnis nehmen und ihre Anregungen zu einer verfassungskonformen Gestaltung der ins Werk gesetzten Chipkartenprojekte berücksichtigen.

Kassel, im Mai 2005 *Alexander Roßnagel*

Vorwort des Autors

Die Art und Weise, in der jeder von uns sich gegenüber anderen identifiziert (sei es als Bürger, Arbeitnehmer, Patient, Geschäftspartner oder in sonstigen Rollen), wird sich in naher Zukunft in einigen fundamentalen Punkten ändern. Der Ausweis als hergebrachtes Mittel der Identifizierung bleibt bestehen, wird jedoch technologisch fortentwickelt. Chipkartenausweise erlauben die elektronische Speicherung der bisherigen Angaben und die Erweiterung um zusätzliche Identifizierungsinformationen, insbesondere biometrische Daten. Kontaktlose Schnittstellen ermöglichen den schnellen, aber auch den unmerklichen Abruf dieser Daten durch kontrollierende Instanzen. Freie Speicherbereiche des Chips können Funktionen wie das elektronische Rezept übernehmen, die bislang in papierner Form ausgeführt wurden. Wenn schließlich auf Chipkartenausweisen Verfahren der elektronischen Signatur und Authentisierung ablaufen, so erweitert sich der Identitätsnachweis in eine „virtuelle" Welt, in der der Ausweis als Zugangsinstrument für Anwendungen und Daten in peripheren Netzen dienen kann.

Diese Entwicklung bietet große Chancen für eine höhere Identifizierungssicherheit, Erleichterungen elektronischer Geschäfts- und Verwaltungsprozesse und eine Rationalisierung und damit verbundene Kosteneinsparung, gerade in der öffentlichen Verwaltung und im Gesundheitswesen. Gleichzeitig entstehen jedoch Risiken für die einzelnen Ausweisinhaber und ihre informationelle Selbstbestimmung, denen rechtlich und technisch angemessen zu begegnen ist. Aus diesem Spannungsfeld ergeben sich die Rechtsprobleme des digitalen Personalausweis, der elektronischen Gesundheitskarte und des JobCard-Verfahrens, die Gegenstand dieser Abhandlung sind.

Dass die Bundesregierung die drei Projekte am 9. März 2005 zu einer „eCard-Strategie" zusammenfassen würde, war bei der Konzeption der Arbeit nicht vorhersehbar. Es bestätigt aber den Ansatz, die Vorhaben als Teile einer Identifizierungsinfrastruktur zu sehen, deren Wirkungen auf den Einzelnen nur insgesamt betrachtet werden können.

Die rechtlichen, technischen und organisatorischen Rahmenbedingungen der Einführung von Chipkartenausweisen entwickeln sich kontinuierlich fort. Deshalb bestand die besondere Herausforderung darin, einerseits diese Entwicklungen soweit wie möglich zu berücksichtigen, andererseits grundlegende rechtliche Anforderungen zu formulieren, die nicht von kurzfristigen Umsetzungsentscheidungen abhängig sind. Das gilt insbesondere für den digitalen Personalausweis und das JobCard-Verfahren, für die bei der Fertigstellung des Manuskripts noch keine öffentlichen Gesetzesentwürfe verfügbar waren.

Die Arbeit wurde im Sommersemester 2005 von der Universität Kassel als Dissertation angenommen. Grundlage der Veröffentlichung ist der Literatur- und Gesetzesstand vom Mai 2005.

Mein besonderer Dank gilt Prof. Dr. Alexander Roßnagel für die kontinuierliche und intensive Betreuung während meiner Zeit in Kassel. Seine Anregungen, Ermutigungen und kritischen Bemerkungen haben maßgeblich zum Gelingen der Arbeit beigetragen. Ich danke Herrn Prof. Dr. Alexander Roßnagel gleichzeitig für die Aufnahme der Arbeit in die Schriftenreihe „Der Elektronische Rechtsverkehr".

Die Ausführungen zum digitalen Personalausweis sind überwiegend im Zusammenhang mit der Machbarkeitsstudie „Digitaler Personalausweis" entstanden. In der Arbeit mit unseren Kooperationspartnern habe ich insbesondere von Dr. Dirk Scheuermann (Fraunhofer Institut für Sichere Telekooperation, Darmstadt) und Moritz Strasser (Institut für Informatik und Gesellschaft der Universität Freiburg) viel über die technischen und wirt-

schaftswissenschaftlichen Hintergründe von Chipkarten erfahren. Bei Herrn Prof. Dr. Andreas Hänlein möchte ich mich für die Erstellung des Zweitgutachtens bedanken.

Für die anregenden Diskussionen und die große Unterstützung danke ich meinen Kollegen von der Projektgruppe verfassungsverträgliche Technikgestaltung (provet) der Universität Kassel, Stefanie Fischer-Dieskau, Rotraud Gitter, Florian Hallaschka, Silke Jandt, Michael Knopp, Jürgen Müller, Sandra Paul, Tobias Stadler, Dr. Roland Steidle und Dr. Nuriye Yildrim. Wertvolle Anregungen verdanke ich daneben Frau Dr. Astrid Albrecht (Bundesamt für Sicherheit in der Informationstechnik) und Herrn Dr. Christoph Goetz (Kassenärztliche Vereinigung Bayerns).

Meiner Mutter, Frau Dr. Marianne Hornung-Grove, danke ich ganz herzlich dafür, dass sie die Mühen der kritischen Durchsicht auf sich genommen hat.

Hamburg, im Mai 2005 *Gerrit Hornung*

Übersicht

1 Identität, Identifizierung und die moderne Ausweistechnologie 29

2 Grundlagen 37
- 2.1 Zur Einführung von Chipkartenausweisen 37
- 2.2 Rechtliche Grundlagen 47
- 2.3 Technische Grundlagen 66
- 2.4 Zum Verhältnis von Recht und Technik 87
- 2.5 Methodische Überlegungen 89

3 Internationale Entwicklungen 93

4 Datenschutzrechtliche Anforderungen und Bewertung 131
- 4.1 Regelungssystem und Anwendbarkeit 131
- 4.2 Verfassungsrechtliche Zulässigkeit 152
  - 4.2.1 Verfassungsrechtliche Anforderungen 153
  - 4.2.2 Die verfassungsrechtliche Zulässigkeit des digitalen Personalausweises 165
  - 4.2.3 Die verfassungsrechtliche Zulässigkeit der elektronischen Gesundheitskarte 207
  - 4.2.4 Die verfassungsrechtliche Zulässigkeit des JobCard-Verfahrens 241
- 4.3 Zulässigkeit nach einfachgesetzlichem Datenschutzrecht 246

5 Signaturrechtliche Fragestellungen 313
- 5.1 Das allgemeine Regelungssystem des Signaturgesetzes 313
- 5.2 Spezifische Probleme bei Chipkartenausweisen 319

6 Aspekte der technischen und organisatorischen Umsetzung 337
- 6.1 Allgemeine Umsetzungsstrategien 337
- 6.2 Besonderheiten des digitalen Personalausweises 346
- 6.3 Besonderheiten der elektronischen Gesundheitskarte 362
- 6.4 Die Umsetzung des JobCard-Verfahrens 376

7 Akzeptanzfragen 379
- 7.1 Der Begriff der Akzeptanz 380
- 7.2 Akzeptanz als Rechtsproblem? 383
- 7.3 Einflussfaktoren für die Akzeptanz von Chipkartenausweisen 393
- 7.4 Die Beeinflussbarkeit der Akzeptanz durch den Staat 428

8 Schlussbemerkungen 433

9 Handlungsleitende Thesen 437
- 9.1 Der digitale Personalausweis 437
- 9.2 Die elektronische Gesundheitskarte 439
- 9.3 Das JobCard-Verfahren 442

Stichwortverzeichnis 443

Literaturverzeichnis 455

Inhaltsverzeichnis

Abkürzungsverzeichnis 19

1 Identität, Identifizierung und die moderne Ausweistechnologie 29

2 Grundlagen 37

2.1 Zur Einführung von Chipkartenausweisen 37
2.1.1 Der digitale Personalausweis 37
2.1.2 Die elektronische Gesundheitskarte 41
2.1.3 Das JobCard-Verfahren 46

2.2 Rechtliche Grundlagen 47
2.2.1 Personalausweisrecht 47
2.2.1.1 Entwicklung und gegenwärtiger Inhalt der Personalausweispflicht 47
2.2.1.2 Die Ausgestaltung des Personalausweises 49
2.2.1.3 Das Antrags- und Ausgabeverfahren 50
2.2.1.4 Das Personalausweisregister und seine Verwendung 51
2.2.1.5 Die Verwendung des Ausweises 54
2.2.1.6 Beispiele für den praktischen Einsatz 56
2.2.2 Regelungen für die elektronische Gesundheitskarte 58
2.2.2.1 Allgemeine Regeln für die Datenverwendung im Gesundheitswesen 58
2.2.2.2 Neue Bestimmungen im GKV-Modernisierungsgesetz 60

2.3 Technische Grundlagen 66
2.3.1 Chipkarten und ihre Einsatzumgebungen 66
2.3.2 Verschlüsselung, elektronische Signatur und Authentisierung 70
2.3.3 Biometrische Verfahren 74
2.3.3.1 Begriffsbestimmungen und Arten biometrischer Verfahren 75
2.3.3.2 Funktionsweise 78
2.3.3.3 Einsatz in der Praxis 81
2.3.3.4 Chancen und Problemfelder 85

2.4 Zum Verhältnis von Recht und Technik 87

2.5 Methodische Überlegungen 89

3 Internationale Entwicklungen 93

3.1 Überstaatliche Aktivitäten 94
3.1.1 Die internationale Vereinheitlichung von Reisedokumenten 94
3.1.2 Europäische Initiativen 96

3.2 Staaten mit eingeführten Chipkartenausweisen 98
3.2.1 Europäische Staaten 98
3.2.1.1 Finnland 98
3.2.1.2 Estland 100
3.2.1.3 Belgien 101
3.2.1.4 Frankreich 103
3.2.2 Außereuropäische Staaten 103
3.2.2.1 Brunei 103
3.2.2.2 Oman 104

3.2.2.3 Hongkong 105
3.2.2.4 Macao 107
3.2.2.5 Malaysia 109
3.2.2.6 Taiwan 110
3.3 Staaten mit Pilotprojekten 111
3.3.1 Italien 111
3.3.2 Tschechische Republik 112
3.3.3 Slowenien 112
3.4 Staaten mit grundsätzlichen Entscheidungen für eine Einführung 112
3.4.1 Europäische Staaten 112
3.4.1.1 Großbritannien 112
3.4.1.2 Spanien 115
3.4.1.3 Niederlande 115
3.4.2 Außereuropäische Staaten 116
3.4.2.1 Vereinigte Arabische Emirate 116
3.4.2.2 Bahrain 116
3.4.2.3 Saudi-Arabien 117
3.4.2.4 Thailand 117
3.4.2.5 Japan 117
3.4.2.6 Volksrepublik China 118
3.5 Diskussionsprozesse 118
3.5.1 Diskussionen in europäischen Staaten 118
3.5.1.1 Schweiz 118
3.5.1.2 Österreich 119
3.5.1.3 Schweden 121
3.5.1.4 Russland 121
3.5.2 Diskussionen in außereuropäischen Staaten 122
3.5.2.1 USA 122
3.5.2.2 Kanada 124
3.5.2.3 Indien 125
3.5.2.4 Exkurs: Australien 125
3.6 Staaten mit biometrischen Lösungen ohne Chip; Staaten in der ersten Phase der Überlegungen 125
3.7 Tabellarische Zusammenfassung der wichtigsten Projekte 126
4 Datenschutzrechtliche Anforderungen und Bewertung 131
4.1 Regelungssystem und Anwendbarkeit 131
4.1.1 Normative Grundlagen 131
4.1.1.1 Internationale Grundlagen 132
4.1.1.2 Deutsches Datenschutzrecht 138
4.1.2 Grundsätzliche Anwendbarkeit des Datenschutzrechts: Personenbezug 142
4.1.2.1 Anonyme, pseudonyme und verschlüsselte Daten 142
4.1.2.2 Biometrische Daten 146
4.1.2.2.1 Bisherige Auffassungen zum Personenbezug 146
4.1.2.2.2 Analyse 147
4.1.2.2.2.1 Differenzierung nach Verfahrensschritten 147
4.1.2.2.2.2 Besonderheiten bei Templates 149

4.1.2.2.2.3 Speicherung und Verarbeitung auf Chipkartenausweisen 150
4.1.2.2.2.4 Vermeidung des Personenbezugs durch templatefreie Verfahren? 151
4.1.2.2.3 Zusammenfassung 152
4.2 Verfassungsrechtliche Zulässigkeit 152
4.2.1 Verfassungsrechtliche Anforderungen 153
4.2.1.1 Gesetzesvorbehalt und Bestimmtheitsgrundsatz 153
4.2.1.2 Anforderungen des Grundrechts auf informationelle Selbstbestimmung 155
4.2.1.2.1 Verhältnismäßigkeit 155
4.2.1.2.2 Zweckbindung und Zweckbegrenzung 157
4.2.1.2.3 Informationelle Gewaltenteilung 158
4.2.1.2.4 Profilbildung und allgemeines Personenkennzeichen 159
4.2.1.2.5 Transparenz 162
4.2.1.2.6 Staatliche Schutzpflichten 164
4.2.2 Die verfassungsrechtliche Zulässigkeit des digitalen Personalausweises 165
4.2.2.1 Grundsätzliche Verfassungsmäßigkeit 165
4.2.2.1.1 Verfassungsmäßigkeit der Personalausweispflicht 165
4.2.2.1.2 Grundsätzliche Verfassungsmäßigkeit des Einsatzes von Biometrie 167
4.2.2.2 Gesetzesvorbehalt und Bestimmtheit der Ermächtigungsgrundlage 173
4.2.2.3 Hinlängliche Reichweite der bestehenden Zweckbindung? 177
4.2.2.4 Fragen der Verwendung biometrischer Daten 178
4.2.2.4.1 Rechtliche Kriterien für die Merkmalsauswahl 178
4.2.2.4.1.1 Hinreichend niedrige Fehlerraten 179
4.2.2.4.1.2 Geringstmöglicher Eingriff in Grundrechte 184
4.2.2.4.2 Art der Datenspeicherung: Verwendung von Templates? 188
4.2.2.4.3 Ort der Datenspeicherung 191
4.2.2.4.4 Ort des Matchings 195
4.2.2.4.5 Kontaktlose Schnittstellen 197
4.2.2.4.6 Zugriffsschutz 198
4.2.2.4.7 Einrichtung effektiver Rückfallsysteme 199
4.2.2.5 Einsatz im privaten Bereich 204
4.2.2.6 Schutzpflichten für den Einsatz im Ausland? 206
4.2.3 Die verfassungsrechtliche Zulässigkeit der elektronischen Gesundheitskarte 207
4.2.3.1 Grundsätzliche Verfassungsmäßigkeit 207
4.2.3.2 Gesetzesvorbehalt und Bestimmtheit der Ermächtigungsgrundlage 211
4.2.3.3 Ort der Datenspeicherung 213
4.2.3.4 Zugriffsbefugnisse 218
4.2.3.4.1 Die grundsätzliche Informationshoheit des Versicherten 218

4.2.3.4.2 Zugriffsbefugnisse auf einzelne Anwendungen und technische Absicherung 220
4.2.3.4.2.1 Verpflichtende Anwendungen 220
4.2.3.4.2.2 Freiwillige Anwendungen 223
4.2.3.4.2.3 Protokolldaten 227
4.2.3.5 Normativer Schutz von Zweckbindung und Zugriffsbefugnissen 228
4.2.3.5.1 Gesetzliche Schweigepflicht 229
4.2.3.5.2 Zeugnisverweigerungsrecht, Beschlagnahmeschutz und Überwachung der Telekommunikation 233
4.2.3.5.3 Schutznormen im SGB V 237
4.2.3.6 Eigene technische Zugriffsmöglichkeit des Karteninhabers? 240
4.2.4 Die verfassungsrechtliche Zulässigkeit des JobCard-Verfahrens 241
4.2.4.1 Der geplante Ablauf des Verfahrens 242
4.2.4.2 Zulässigkeit einer verpflichtenden Implementierung von Verfahren der elektronischen Signatur, Verschlüsselung und Authentisierung 243
4.2.4.3 Fragen der Datenspeicherung und der Zugriffsbefugnisse 244
4.3 Zulässigkeit nach einfachgesetzlichem Datenschutzrecht 246
4.3.1 Datenschutzbestimmungen des Signaturrechts 246
4.3.2 Anforderungen an die Systemgestaltung: Datenvermeidung und Datensparsamkeit 247
4.3.2.1 Rechtsnatur von § 3a BDSG 247
4.3.2.2 Anforderungen an Datenverarbeitungssysteme 248
4.3.2.3 Umsetzung bei einzelnen Ausweisen 250
4.3.3 Anforderungen an den Einsatz mobiler personenbezogener Speicher- und Verarbeitungsmedien 253
4.3.3.1 Rechtsnatur von § 6c BDSG 253
4.3.3.2 Anwendungsbereich 256
4.3.3.2.1 Mobile personenbezogene Speicher- und Verarbeitungsmedien 256
4.3.3.2.1.1 Begriff 256
4.3.3.2.1.2 Anwendung auf Chipkartenausweise 257
4.3.3.2.2 Vorrangige Regelungen der Landesdatenschutzgesetze 261
4.3.3.2.3 Abgrenzung zu verwandten Normen 264
4.3.3.3 Unterrichtungspflichten nach § 6c Abs. 1 BDSG 265
4.3.3.3.1 Verpflichtete Stelle 265
4.3.3.3.2 Berechtigter 267
4.3.3.3.3 Umfang der Unterrichtung 267
4.3.3.3.4 Form und Zeitpunkt 270
4.3.3.3.5 Anderweitige Kenntnisnahme 271
4.3.3.4 Sonstige Pflichten (§ 6c Abs. 2 und 3 BDSG) 272
4.3.4 Besondere Arten personenbezogener Daten 274
4.3.4.1 Begriff und besondere Anforderungen 274
4.3.4.2 Anwendung auf Chipkartenausweise 276
4.3.4.2.1 Digitaler Personalausweis 276
4.3.4.2.2 Elektronische Gesundheitskarte 278
4.3.4.2.3 Der Einsatz von Biometrie bei Signaturkarten 282

4.3.5 Automatisierte Einzelentscheidung (§ 6a BDSG) 282
4.3.6 Probleme der Datenübermittlung 283
4.3.6.1 Zulässigkeit nach dem Teledienstedatenschutzrecht 284
4.3.6.2 Datenverarbeitung im Auftrag oder Funktionsübertragung? 286
4.3.6.2.1 Abgrenzung 286
4.3.6.2.2 Anwendung auf Chipkartenausweise 288
4.3.6.2.2.1 Verarbeitung von Gesundheitsdaten im System der Gesundheitskarte 288
4.3.6.2.2.2 Datenerhebungen zu Zwecken der elektronischen Signatur 291
4.3.6.3 Einrichtung automatisierter Abrufverfahren (§ 10 BDSG) 292
4.3.6.3.1 Anwendbarkeit 292
4.3.6.3.2 Angemessenheit der Einrichtung (§ 10 Abs. 1 BDSG) 293
4.3.6.3.3 Anforderungen aus § 10 Abs. 2 und 4 BDSG 295
4.3.7 Besonderheiten der Betroffenenrechte 295
4.3.7.1 Die Rechte des Betroffenen 295
4.3.7.2 Betroffenenrechte beim digitalen Personalausweis 296
4.3.7.3 Betroffenenrechte bei der elektronischen Gesundheitskarte 297
4.3.8 Anforderungen an die Datensicherheit 300
4.3.8.1 Hintergrund und Bedrohungen 300
4.3.8.2 Normative Anforderungen und Anwendung auf Chipkartensysteme 302
4.3.8.2.1 Grundlagen 302
4.3.8.2.2 Anforderungen aus der Anlage zu § 9 Satz 1 BDSG 303
4.3.8.2.3 Verhältnismäßigkeit 309

5 Signaturrechtliche Fragestellungen 313
5.1 Das allgemeine Regelungssystem des Signaturgesetzes 313
5.1.1 Grundlagen und Unterschiede zwischen den Signaturstufen 313
5.1.2 Allgemeine signaturrechtliche Anforderungen an qualifizierte Verfahren 317
5.2 Spezifische Probleme bei Chipkartenausweisen 319
5.2.1 Das Konzept des „elektronischen Ausweises“ als Mittel zur Authentisierung in Online-Verfahren 319
5.2.1.1 Problemstellung 319
5.2.1.2 Lösungswege 320
5.2.2 Das Zusammenwirken unterschiedlicher Instanzen 323
5.2.3 Der kombinierte Einsatz mehrerer Karten 327
5.2.4 Institutionskarten 328
5.2.5 Probleme unterschiedlicher Gültigkeitszeiträume 330
5.2.6 Kartenaktivierung mittels Biometrie? 333

6 Aspekte der technischen und organisatorischen Umsetzung 337
6.1 Allgemeine Umsetzungsstrategien 337
6.1.1 Mechanismen der Datensicherung 337
6.1.2 Standardisierung 340
6.1.3 Evaluierung und Zertifizierung 344

6.2 Besonderheiten des digitalen Personalausweises 346
6.2.1 Sicherung der Daten durch Signatur, Verschlüsselung und Authentisierung 346
6.2.1.1 Signatur der elektronischen Ausweisdaten 346
6.2.1.2 Authentisierung zwischen Ausweis und Lesegerät 348
6.2.1.3 Verschlüsselung der biometrischen Daten 350
6.2.1.4 Verfahren bei Zerstörung des Chips und eintretender Unsicherheit der kryptographischen Sicherungen 351
6.2.2 Biometrische Lebenderkennung 352
6.2.3 Kontaktlose oder kontaktorientierte Schnittstelle 354
6.2.4 Organisationsfragen 355
6.2.4.1 Biometrische Daten 355
6.2.4.2 Signaturfunktion 358
6.2.5 Kosten 359
6.3 Besonderheiten der elektronischen Gesundheitskarte 362
6.3.1 Datensicherheit 363
6.3.2 Anonymisierung und Pseudonymisierung 367
6.3.3 Umsetzbarkeit der Zugriffsrechte 367
6.3.3.1 Absicherung eines abgestuften Zugriffsschutzes 368
6.3.3.2 Verwendung von Biometrie 370
6.3.3.3 Zugriff mittels einer eigenen Signaturkarte des Versicherten 371
6.3.4 Organisationsfragen 372
6.3.5 Kosten 374
6.4 Die Umsetzung des JobCard-Verfahrens 376
7 Akzeptanzfragen 379
7.1 Der Begriff der Akzeptanz 380
7.2 Akzeptanz als Rechtsproblem? 383
7.2.1 Ausgangspunkt 383
7.2.2 Berücksichtigung von Akzeptanz bei der Rechtssetzung und -anwendung? 385
7.2.3 Ergebnis 391
7.3 Einflussfaktoren für die Akzeptanz von Chipkartenausweisen 393
7.3.1 Allgemeine Einflussfaktoren für die Akzeptanz staatlicher Maßnahmen 393
7.3.1.1 Bisherige Kategorisierungen 393
7.3.1.2 Bewertung 396
7.3.2 Frühere Akzeptanzphänomene: Fallstudien aus Deutschland 399
7.3.2.1 Fallstudie 1: Die Volkszählung 399
7.3.2.1.1 Die Geschichte der Volkszählung 399
7.3.2.1.2 Wesentliche Argumentationslinien 402
7.3.2.2 Fallstudie 2: der maschinenlesbare Personalausweis 405
7.3.2.2.1 Die Geschichte des maschinenlesbaren Personalausweises 405
7.3.2.2.2 Wesentliche Argumentationslinien 407
7.3.2.3 Bewertung 410
7.3.2.3.1 Analyse der Fallstudien 410
7.3.2.3.2 Vergleich mit den allgemeinen Akzeptanzfaktoren 412

7.3.2.3.3 Übertragbarkeit auf die derzeitige Akezptanzsituation von Chipkartenausweisen 413
7.3.3 Anwendung auf einzelne Chipkartenausweise und deren Funktionalitäten 414
7.3.3.1 Faktoren im Rahmen der Einführung biometrischer Verfahren 414
7.3.3.2 Faktoren aus dem Bereich des Gesundheitswesens 421
7.3.3.3 Faktoren bei der Einführung elektronischer Signaturverfahren 424
7.3.3.3.1 Die Akzeptanz eines signaturfähigen Ausweises 424
7.3.3.3.2 Potentielle Veränderungen durch das JobCard-Verfahren 426
7.3.3.4 Faktoren aus der Zusammenführung mehrerer Funktionalitäten in einer Karte 428
7.4 Die Beeinflussbarkeit der Akzeptanz durch den Staat 428
8 Schlussbemerkungen 433
9 Handlungsleitende Thesen 437
9.1 Der digitale Personalausweis 437
9.2 Die elektronische Gesundheitskarte 439
9.3 Das JobCard-Verfahren 442
Stichwortverzeichnis 443
Anhang: Fragebogen der internationalen Umfrage 453
Literaturverzeichnis 455

Abkürzungsverzeichnis

a.A.	anderer Ansicht
AAMVA	American Association of Motorvehicle Administration
a.a.O.	am angegebenen Ort
ABDA	Bundesvereinigung Deutscher Apothekerverbände e.V.
ABl. EG	Amtsblatt der Europäischen Gemeinschaften
ABl. EU	Amtsblatt der Europäischen Union
Abs.	Absatz
ABS	Acrylnitril-Butadien-Styrol
ACHR	American Convention on Human Rights
ACLU	American Civil Liberties Union
a.E.	am Ende
a.F.	alte Fassung
AFIS	Automatisches Fingerabdruck-Identifizierungssystem
AG	Amtsgericht / Aktiengesellschaft
AK GG-*Bearbeiter*	*Denninger, E.* / *Hoffmann-Riem, W.* / *Schneider, H.-P.* / *Stein, E.* (Hrsg.), Kommentar zum Grundgesetz für die Bundesrepublik Deutschland, 3. Auflage, Loseblatt, Stand: August 2002; *Wassermann, R.* (Hrsg.), 2. Auflage, 1989, Neuwied
AK StPO-*Bearbeiter*	*Wassermann, R.* (Hrsg.), Kommentar zur Strafprozessordnung, Reihe Alternativkommentare, Band 2, Teilband 1: §§ 94-212b, Neuwied 1992
AKT	Arbeitskreis Technik der Datenschutzbeauftragten des Bundes und der Länder
AKW	Atomkraftwerk
AllER	The All England Law Reports (Entscheidungssammlung)
Alt.	Alternative
AO	Abgabenordnung
AöR	Archiv für öffentliches Recht (Zeitschrift)
AOK	Allgemeine Ortskrankenkasse
ApoBetrO	Verordnung über den Betrieb von Apotheken
ArbG	Arbeitsgericht
ArbGG	Arbeitsgerichtsgesetz
Art.	Artikel
Art. 29 DPWP	Article 29 – Data Protection Working Party
AsylVG	Asylverfahrensgesetz
ATG	Aktionsforum Telematik im Gesundheitswesen
AufenthaltsG	Gesetz über den Aufenthalt, die Erwerbstätigkeit und die Integration von Ausländern im Bundesgebiet
AuR	Arbeit und Recht (Zeitschrift)
BÄK	Bundesärztekammer
BAG	Bundesarbeitsgericht
Banz.	Bundesanzeiger
BayKrankenhausG	Bayerisches Krankenhausgesetz
BayObLG	Bayerisches Oberstes Landesgericht
BayVerfGH	Bayerischer Verfassungsgerichtshof
BB	Betriebsberater (Zeitschrift)
Bbg.	Brandenburg
BbgDSG	Brandenburgisches Datenschutzgesetz
Bd.	Band
BDI	Bundesverband der Deutschen Industrie e.V.

BDSG	Bundesdatenschutzgesetz
BetrVG	Betriebsverfassungsgesetz
BeurkG	Beurkundungsgesetz
BGB	Bürgerliches Gesetzbuch
BGBl.	Bundesgesetzblatt
BGH	Bundesgerichtshof
BGH LM	Das Nachschlagewerk des Bundesgerichtshofes in Zivilsachen, hrsg. von Lindenmaier und Möhring
BGHSt	Entscheidungen des Bundesgerichtshofes in Strafsachen
BGHZ	Entscheidungen des Bundesgerichtshofes in Zivilsachen
BGS	Bundesgrenzschutz
BGSG	Gesetz über den Bundesgrenzschutz
BITKOM	Bundesverband Informationswirtschaft, Telekommunikation und Neue Medien e.V.
BK-*Bearbeiter*	*Dolzer, R.* / *Vogel, K.* / *Graßhof, K.* (Hrsg.), Bonner Kommentar zum Grundgesetz, Loseblatt, Stand: 111. Lieferung, Mai 2004, Heidelberg
BKA	Bundeskriminalamt
BKAG	Gesetz über die Errichtung des Bundeskriminalamts
BKK	Die Betriebskrankenkasse (Zeitschrift)
Bln.	Berlin
BlnDSG	Berliner Datenschutzgesetz
BMGS	Bundesministerium für Gesundheit und Soziale Sicherung
BMI	Bundesministerium des Innern
BND	Bundesnachrichtendienst
BR-Drs.	Bundesrats-Drucksache
BrDSG	Bremisches Datenschutzgesetz
Brem.	Bremen
BSI	Bundesamt für Sicherheit in der Informationstechnik
Bsp.	Beispiel(e)
bspw.	beispielsweise
BT	Bundestag
BT-Drs.	Bundestags-Drucksache
Buchholz	Sammel- und Nachschlagewerk der Rechtsprechung des Bundesverwaltungsgerichts, begründet von *Karl Buchholz*, Köln 1966 ff.
B.U. J. Sci. & Tech. L.	Boston University Journal of Science and Technology Law (Zeitschrift)
Bundesgesundheitsbl.	Bundesgesundheitsblatt (Zeitschrift)
BVerfG	Bundesverfassungsgericht
BVerfGE	Entscheidungen des Bundesverfassungsgerichtes
BVerfGG	Gesetz über das Bundesverfassungsgericht
BVerwG	Bundesverwaltungsgericht
BVerwGE	Entscheidungen des Bundesverwaltungsgerichtes
BWO	Bundeswahlordnung
bzw.	beziehungsweise
C.ACM	Communications of the Association of the Computing Machinery (Zeitschrift)
CAD	Kanadische Dollar
CANPASS	Canadian Passenger Accelerated Service System
CAST	Competence Center for Applied Security Technology
CBEFF	Common Biometric Exchange Formats Framework
CC	Common Criteria for Information Technology Security Evaluation
CCTV	Closed-circuit television
CDU	Christlich Demokratische Union Deutschlands

CEN	European Committee for Standardization
CENELEC	European Committee for Electrotechnical Standardization
cilip	Bürgerrechte & Polizei – cilip (Zeitschrift)
cm	Zentimeter
CMLRev	Common Market Law Review (Zeitschrift)
CR	Computer und Recht (Zeitschrift)
CRi	Computer Law Review International (Zeitschrift)
CSU	Christlich-Soziale Union in Bayern e.V.
c't	Magazin für Computertechnik (Zeitschrift)
DÄ	Deutsches Ärzteblatt (Zeitschrift)
DAR	Deutsches Autorecht (Zeitschrift)
dass.	dasselbe
DB	Der Betrieb (Zeitschrift)
DDR	Deutsche Demokratische Republik
ders.	derselbe
DEÜV	Datenerfassungs- und Übermittlungsverordnung
DFK	Deutsches Forum für Kriminalprävention
d.h.	das heißt
dies.	dieselbe(n)
DIGANT	Digitales Antragsverfahren (der Bundesdruckerei)
DIN	Deutsches Institut für Normung e.V.
DIS	Draft International Standard
DM	Deutsche Mark
DNA	Deoxyribonucleic Acid
DÖV	Die öffentliche Verwaltung (Zeitschrift)
DR	Decisions and Reports (Sammlung der Entscheidungen und Beschlüsse der Europäischen Kommission für Menschenrechte)
DSG BW	Landesdatenschutzgesetz Baden-Württemberg
DSG-LSA	Datenschutzgesetz Sachsen-Anhalt
DSG MV	Datenschutzgesetz Mecklenburg-Vorpommern
DSG NW	Datenschutzgesetz Nordrhein-Westfalen
DSG Rh.-Pf.	Rheinland-pfälzisches Landesdatenschutzgesetz
DSG SH	Datenschutzgesetz Schleswig-Holstein
DSRL	Richtlinie 95/46/EG des Europäischen Parlaments und des Rates v. 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr
DStZ	Deutsche Steuer-Zeitung (Zeitschrift)
DuD	Datenschutz und Datensicherheit, bis 1995: Datenschutz und Datensicherung (Zeitschrift)
DuR	Demokratie und Recht (Zeitschrift)
DVBl.	Deutsches Verwaltungsblatt (Zeitschrift)
DVPassG	Verordnung über die Befreiung von der Passpflicht und zur Bestimmung von amtlichen Ausweisen als Passersatz
DVR	Datenverarbeitung im Recht (Zeitschrift)
ebd.	ebenda
EBF	European Biometric Forum
EC-Karte	Eurocheque-Karte
ECOSOC	Economic and Social Council (der UN)
EDV	Elektronische Datenverarbeitung
EEK	Estnische Kronen
EEPROM	Electrical Erasable Programmable Read Only Memory
EER	Equal Error Rate
eESC/TB11 Health	eEurope Smart Cards Trailblazer 11 Health

EESSI	European Electronic Signature Standardisation Initiative
EG	Europäische Gemeinschaft
EGMR	Europäischer Gerichtshof für Menschenrechte
EGV	Vertrag über die Europäische Gemeinschaft
Einf.	Einführung
Einl.	Einleitung
E.L.Rev.	European Law Review (Zeitschrift)
EMBO reports	European Molecular Biology Organization reports (Zeitschrift)
EMRK	Europäische Menschenrechtskonvention
EMV	Europay, Mastercard, Visa (Chipkartenspezifikation für Kreditkarten)
EN	European Norm
et.al.	et altera
etc.	et cetera
ETSI	European Telecommunications Standards Institute
EU	Europäische Union
EuGH	Gerichtshof der europäischen Gemeinschaften
EuGRZ	Europäische Grundrechtezeitschrift (Zeitschrift)
EuR	Europarecht (Zeitschrift)
EUV	Vertrag über die Europäische Union
EuZW	Europäische Zeitschrift für Wirtschaftsrecht (Zeitschrift)
e.V.	eingetragener Verein
EWG	Europäische Wirtschaftsgemeinschaft
f.	folgend(e)
FAR	False Acceptance Rate
FAZ	Frankfurter Allgemeine Zeitung
FDP	Freie Demokratische Partei Deutschlands
FER	False Enrolment Rate / Failure to Enrol Rate
FeV	Verordnung über die Zulassung von Personen zum Straßenverkehr
ff.	fortfolgende
FGO	Finanzgerichtsordnung
FINEID	Finnish Electronic Identification
Fn.	Fußnote
FoeBuD e.V.	Verein zur Förderung des öffentlichen bewegten und unbewegten Datenverkehrs e.V.
FR	Frankfurter Rundschau
FRR	False Rejection Rate
G8	Gruppe der Acht
G&D	Giesecke & Devrient GmbH
GDD	Gesellschaft für Datenschutz und Datensicherung e.V.
GesR	Gesundheitsrecht (Zeitschrift)
GG	Grundgesetz
GI	Gesellschaft für Informatik e.V.
GKV	Gesetzliche Krankenversicherung
GmbH	Gesellschaft mit beschränkter Haftung
GMD	Gesellschaft für Mathematik und Datenverarbeitung mbH
GMG	Gesetz zur Modernisierung der Gesetzlichen Krankenversicherung
GSM	Global System for mobile Communications
GVBl.	Gesetz- und Verordnungsblatt
GVG	Gesellschaft für Versicherungswissenschaft und -gestaltung
GwG	Gesetz über das Aufspüren von Gewinnen aus schweren Straftaten („Geldwäschegesetz“)
Harv. J. Law & Tec	Harvard Journal of Law & Technology

HdbStR	*Isensee, J.* / *Kirchhof, P.* (Hrsg.), Handbuch des Staatsrechts der Bundesrepublik Deutschland, Heidelberg. Band 1: Grundlagen von Staat und Verfassung, 1987; Band 2, Verfassungsstaat, 3. Auflage 2004; Band 3: Das Handeln des Staates, 2. Auflage 1996; Band 5: Allgemeine Grundrechtslehren, 2. Auflage 2000; Band 6: Freiheitsrechte, 2. Auflage 2001; Band 7: Normativität und Schutz der Verfassung, Internationale Beziehungen, 1992
HDSG	Hessisches Datenschutzgesetz
HeilberufsG	Heilberufsgesetz
Hess.	Hessen
HessStGH	Hessischer Staatsgerichtshof
HKD	Hong Kong Dollar
HKSAR	Hong Kong Special Administrative Region
h.M.	herrschende Meinung
HmbDSG	Hamburgisches Datenschutzgesetz
Hoeren/Sieber-*Bearbeiter*	*Hoeren, T.* / *Sieber, U.*, Handbuch Multimedia-Recht. Rechtsfragen des elektronischen Geschäftsverkehrs, Loseblatt, Stand: Mai 2003, München
HPC	Health Professional Card
HRLJ	Human Rights Law Journal (Zeitschrift)
Hrsg.	Herausgeber
hrsg.	herausgegeben
HSFK	Hessische Stiftung Friedens- und Konfliktforschung
i.a.R.	in aller Regel
IBM	International Business Machines Corporation
ICAO	International Civil Aviation Organisation
i.E.	im Erscheinen
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers, Inc.
IEEE.IT	IEEE Transactions on Information Theory (Zeitschrift)
IETF-PKIX	The Internet Engineering Task Force – Public-Key Infrastructure (X.509)
IfSG	Gesetz zur Verhütung und Bekämpfung von Infektionskrankheiten beim Menschen
IGD	Fraunhofer Institut für Graphische Datenverarbeitung
ILO	International Labour Organisation
INPOL	Informationssystem der Polizei
insbes.	insbesondere
INSPASS	United States Immigration and Naturalization Service Passenger Accelerated Service System
IPbpR	Internationaler Pakt über bürgerliche und politische Rechte
IPTS	Institute for Prospective Technological Studies
ISIS	Industrial Signature Interoperability Specification
ISO	International Organization of Standardization
i.S.v.	im Sinne von
IT	Informationstechnologie
ITG	Informationstechnische Gesellschaft im VDE
ITSG	Informationstechnische Servicestelle der Gesetzlichen Krankenversicherung GmbH
ITU	International Telecommunication Union
IuKDG	Informations- und Kommunikationsdienstegesetz
i.V.m.	in Verbindung mit
JA	Juristische Arbeitsblätter (Zeitschrift)

JAP	Java Anon Proxy
JArbSchG	Gesetz zum Schutz der arbeitenden Jugend
J. Marshall J. Computer & Info. L.	The John Marshall Journal of Computer & Information Law (Zeitschrift)
JPEG	Joint Photographic Experts Group
JR	Juristische Rundschau (Zeitschrift)
JRC	Joint Research Center of the European Commission
Jura	Juristische Ausbildung (Zeitschrift)
JuS	Juristische Schulung (Zeitschrift)
JZ	Juristenzeitung (Zeitschrift)
K&R	Kommunikation und Recht (Zeitschrift)
k.A.	keine Angabe
Kap.	Kapitel
KBV	Kassenärztliche Bundesvereinigung
KGSt	Kommunale Gemeinschaftsstelle für Verwaltungsvereinfachung
KJ	Kritische Justiz (Zeitschrift)
KK-*Bearbeiter*	*Pfeiffer, G.* (Hrsg.), Karlsruher Kommentar zur Strafprozessordnung und zum Gerichtsverfassungsgesetz mit Einführungsgesetz, 5. Auflage, München 2003
Km/h	Kilometer pro Stunde
KMR-*Bearbeiter*	*Heintschel-Heinegg, B.* / *Stöckel, H.* (Hrsg.), KMR. Kommentar zur Strafprozessordnung, Loseblatt, Stand: 37. Lieferung Mai 2004, München
KOM	Europäische Kommission, Dokumente
KORA	Konkretisierung Rechtlicher Anforderungen
KritV	Kritische Vierteljahresschrift (Zeitschrift)
KZfSS	Kölner Zeitschrift für Soziologie und Sozialpsychologie (Zeitschrift)
LAK	Landesärztekammer
LDSG	Landesdatenschutzgesetz
LG	Landgericht
lit.	litera
LK-*Bearbeiter*	Strafgesetzbuch. Leipziger Kommentar, Großkommentar. 10. Auflage hrsg. von *H.-H. Jescheck, W. Ruß, W.* und *G. Willms, G.*; 11. Auflage hrsg. von *B. Jähnke, H. W. Laufhütte* und *W. Odersky*, Berlin
LKA	Landeskriminalamt
LKV	Landes- und Kommunalverwaltung (Zeitschrift)
LPersAuswG	Landespersonalausweisgesetz
LPK-SGB V-*Bearbeiter*	*Kruse, J.* / *Hänlein, A.* (Hrsg.), Gesetzliche Krankenversicherung: Lehr- und Praxiskommentar, 2. Auflage, Baden-Baden 2003
LSE	The London School of Economics & Political Science
LT-Drs.	Landtags-Drucksache
LVerf	Landesverfassung
LVerfG	Landesverfassungsgericht
m	Meter
Macao SAR	Macao Special Administrative Region
MAD	Militärischer Abschirmdienst
Manssen-*Bearbeiter*	*Manssen, G.* (Hrsg.), Telekommunikations- und Medienrecht. Kommentar, Loseblatt, Stand: Juli 2003, Berlin
MBO-Ä 2004	Musterberufsordnung für die deutschen Ärztinnen und Ärzte, zuletzt geändert durch die Beschlüsse des 107. Deutschen Ärztetages 2004 in Bremen
M/D-*Bearbeiter*	*Maunz, T.* / *Dürig, G.* / *Herzog, R.* / *Scholz, R.* / *Lerche, P.* / *Papier, H.-J.* / *Randelzhofer, A.* / *Badura, P.* / *Herdegen, M.* / *di Fabio, U.* /

	Klein, H. M. / *Schmidt-Aßmann, E.*, Grundgesetz. Kommentar, Loseblatt, Stand: 42. Lieferung Februar 2003, München
mdi	Forum der Medizin_Dokumentation und Medizin_Informatik (Zeitschrift)
MDR	Monatsschrift für Deutsches Recht (Zeitschrift)
MDStV	Mediendienste-Staatsvertrag
MedR	Medizinrecht (Zeitschrift)
MEID	Macao Special Administrative Region Electronic Identity Card
MeldeG	Meldegesetz
ME PolG	Musterentwurf eines einheitlichen Polizeigesetzes
Mio.	Million(en)
MJ	Maastricht Journal of European and Comparative Law (Zeitschrift)
MLR	Modern Law Review (Zeitschrift)
mm^2	Quadratmillimeter
MMR	Multimedia und Recht (Zeitschrift)
Mrd.	Milliarde(n)
MRRG	Melderechtsrahmengesetz
MV	Mecklenburg-Vorpommern
m.w.N.	mit weiteren Nachweisen
NADIS	Nachrichtliches Informationssystem
NDSG	Niedersächsisches Datenschutzgesetz
n.F.	neue Fassung
NIST	National Institute for Standards and Technology
NJ	Neue Justiz (Zeitschrift)
NJW	Neue Juristische Wochenschrift (Zeitschrift)
NLJ	New Law Journal (Zeitschrift)
No.	Number
Nr.	Nummer
NS	Nationalsozialismus
NStZ	Neue Zeitschrift für Strafrecht (Zeitschrift)
MTT	MailTrusT (PKI Standard)
NVwZ	Neue Zeitschrift für Verwaltungsrecht (Zeitschrift)
NVwZ-RR	Neue Zeitschrift für Verwaltungsrecht, Rechtsprechungs-Report (Zeitschrift)
NW	Nordrhein-Westfahlen
O.A.S.	Organization of American States
OCG	Österreichische Computer Gesellschaft
OCSP	Online Certificate Service Protocol
OECD	Organization for Economic Cooperation and Development
OLG	Oberlandesgericht
o.V.	ohne Verfasser
OVG	Oberverwaltungsgericht
OWiG	Gesetz über Ordnungswidrigkeiten
PassG	Passgesetz
PC	Personal Computer
PDA	Personal Digital Assistant
PDS	Partei des Demokratischen Sozialismus
PDSV	Verordnung über den Datenschutz für Unternehmen, die Postdienstleistungen erbringen
PersAuswG	Personalausweisgesetz
PersR	Der Personalrat (Zeitschrift)
PersStdGAV	Verordnung zur Ausführung des Personenstandsgesetzes
PET	Polyethylenterephtalat / Privacy Enhancing Technologies

PGP	Pretty Good Privacy
PICAO	Provisional International Civil Aviation Organization
PIN	Persönliche Identifikationsnummer
PIOS	Personen, Institutionen, Objekte und Sachen (Arbeits- und Recherchedatei der Polizei)
PKCS	Public Key Cryptography Standard
PKI	Public-Key-Infrastructure
PKW	Personenkraftwagen
Prot.	Protokoll
provet	Projektgruppe verfassungsverträgliche Technikgestaltung
PUK	Personal Unblocking Key
PVC	Polyvinylchlorid
RAF	Rote Armee Fraktion
RAM	Random Access Memory
RDV	Recht der Datenverarbeitung (Zeitschrift)
RegTP	Regulierungsbehörde für Telekommunikation und Post
RF	Radio Frequency
RFID	Radio Frequency Identification
RGBl.	Reichsgesetzblatt
RGSt	Entscheidungen des Reichsgerichts in Strafsachen
RGZ	Entscheidungen des Reichsgerichts in Zivilsachen
Rh.-Pf.	Rheinland-Pfalz
RLeG	Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates v. 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs
RLeS	Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates v. 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen
RMD-*Bearbeiter*	*Roßnagel, A.* (Hrsg.), Recht der Multimedia-Dienste. Kommentar zum IuKDG und zum MDStV, Loseblatt, Stand: Juni 2004, München
Rn.	Randnummer(n)
RöV	Verordnung über den Schutz vor Schäden durch Röntgenstrahlen
ROM	Read Only Memory
Roßnagel-*Bearbeiter*	*Roßnagel, A.* (Hrsg.), Handbuch zum Datenschutzrecht. Die neuen Grundlagen für Wirtschaft und Verwaltung, München 2003
Rs.	Rechtssache(n)
RSA	Rivest/Shamir/Adleman (Verschlüsselungsalgorithmus)
Rspr.	Rechtsprechung
s.	siehe / section
S.	Seite
s.a.	siehe auch
Saarl.	Saarland
Sachs.	Sachsen
Sachs.-Anh.	Sachsen-Anhalt
SAM	Secure Access Module
SC	Sub-Committee
SDSG	Saarländisches Datenschutzgesetz
SFR	Schweizer Franken
SGB	Sozialgesetzbuch
SGG	Sozialgerichtsgesetz
SigG	Signaturgesetz
SigV	Signaturverordnung

SK StPO-*Bearbeiter*	*Rudolphi, H.-J.* / *Frisch, W.* / *Paeffgen, H.-U.* / *Rogall, K.* / *Schlüchter, E.* / *Wolter, J.*, Systematischer Kommentar zur Strafprozessordnung und zum Gerichtsverfassungsgesetz. Loseblattkommentar, Stand: Juli 2003, Neuwied
Slg.	Sammlung
SM	Secure Messaging
SMC	Security Module Card
s.o.	siehe oben
sog.	so genannte(r/s/n)
SPD	Sozialdemokratische Partei Deutschlands
SSL	Secure Socket Layer
StAG	Staatsangehörigkeitsgesetz
StAnz BW	Staatsanzeiger für Baden-Württemberg
StAnz Hess.	Staatsanzeiger für das Land Hessen
StAZ	Das Standesamt (Zeitschrift)
StGB	Strafgesetzbuch
StPO	Strafprozessordnung
str.	streitig
StrlSchV	Verordnung über den Schutz vor Schäden durch ionisierende Strahlen (Strahlenschutzverordnung)
st. Rspr.	ständige Rechtsprechung
StVO	Straßenverkehrsordnung
s.u.	siehe unten
SÜG	Gesetz über die Voraussetzungen und das Verfahren von Sicherheitsüberprüfungen des Bundes
TAB	Büro für Technikfolgenabschätzung beim Deutschen Bundestag
TDDSG	Teledienstedatenschutzgesetz
TDG	Teledienstegesetz
TeleTrusT	Verein zur Förderung der Vertrauenswürdigkeit von Informations- und Kommunikationstechnik e.V.
Thür.	Thüringen
TKG	Telekommunikationsgesetz
TLS	Transport Security Layer
tlw.	teilweise
TPG	Gesetz über die Spende, Entnahme und Übertragung von Organen (Transplantationsgesetz)
TSG	Transsexuellengesetz
TU	Technische Universität
u.a.	unter anderem
u.ä.	und Ähnliches
ULD	Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein
UN	United Nations
US	United States
USA	United States of America
USB	Universal Serial Bus
USD	US Dollar
u.s.w.	und so weiter
UV	Ultraviolett
v.	von / vom
V&M	Verwaltung und Management (Zeitschrift)
v.a.	vor allem
VAE	Vereinigte Arabische Emirate
Va. J.L. & Tech.	Virginia Journal of Law and Technology (Zeitschrift)

VDAP	Verband deutscher Arztpraxis-Softwarehersteller e.V.
VDE	Verband der Elektronik und Informationstechnik e.V.
Verf.	Verfasser
VerfGH	Verfassungsgerichtshof
VERSA	Verteilte Signatur-Arbeitsplätze
VersammlG	Gesetz über Versammlungen und Aufzüge
VersR	Versicherungsrecht (Zeitschrift)
VerwA	Verwaltungsarchiv (Zeitschrift)
VG	Verwaltungsgericht
VGH	Verwaltungsgerichtshof
vgl.	vergleiche
VHitG	Verband der Hersteller von IT-Lösungen für das Gesundheitswesen e.V.
Vorb.	Vorbemerkung
VwGO	Verwaltungsgerichtsordnung
VwVfG	Verwaltungsverfahrensgesetz
VZBV	Verbraucherzentrale Bundesverband e.V.
WaffenG	Waffengesetz
WI	Wirtschaftsinformatik (Zeitschrift)
wistra	Zeitschrift für Wirtschaft, Steuer, Strafrecht (Zeitschrift)
WPflV	Wehrpflichtverordnung
WSQ	Wavelet Scalar Quantization
XML	Extended markup language
ZaeFQ	Zeitschrift für ärztliche Fortbildung und Qualitätssicherung (Zeitschrift)
z.B.	zum Beispiel
ZBB	Zeitschrift für Bankrecht und Bankwirtschaft (Zeitschrift)
ZBR	Zeitschrift für Beamtenrecht (Zeitschrift)
ZDA	Zertifizierungsdiensteanbieter
ZfRSoz	Zeitschrift für Rechtssoziologie (Zeitschrift)
Ziff.	Ziffer
ZKM	Zeitschrift für Konfliktmanagement (Zeitschrift)
ZM	Zahnärztliche Mitteilungen (Zeitschrift)
ZPO	Zivilprozessordnung
ZRP	Zeitschrift für Rechtspolitik (Zeitschrift)
ZStW	Zeitschrift für die gesamte Strafrechtswissenschaft (Zeitschrift)
zugl.	zugleich
ZVEI	Zentralverband Elektrotechnik und Elektroindustrie e.V.
z.Z.	zurzeit

1 Identität, Identifizierung und die moderne Ausweistechnologie

„Der Mensch muss einen Ausweis haben“[1] – das ist nach § 1 Abs. 1 Satz 1 PersAuswG geltendes Recht für jeden Deutschen ab der Vollendung des 16. Lebensjahres.[2] Ausweise dienen der Identifizierung von Personen, also dem Nachweis ihrer Identität. Aber was ist der eigentliche Sinn der Personalausweispflicht? Mit anderen Worten: „Muss“ der Mensch nur deshalb einen Ausweis haben, um eine Geldbuße nach § 5 Abs. 2 PersAuswG zu vermeiden, oder auch aus anderen, tieferen Gründen?

Schon aus der Anknüpfung der Ausweispflicht an das Alter folgt, dass der Mensch offenbar nicht deshalb eines Ausweises bedarf, um Mensch zu sein und eine Identität zu entwickeln. Auch die historische Entwicklung zeigt, dass Individuen ihr Zusammenleben sehr wohl ohne Ausweiswesen organisieren können. Kleinstgesellschaften kommen ohne dieses aus, weil ihre Mitglieder sich untereinander kennen oder – in etwas größeren Einheiten – auf Dritte zurückgreifen können, die beiden Parteien bekannt sind und so die Identität der jeweils anderen Partei zuverlässig bestätigen können.

Im Grundsatz sind Ausweise also weder eine notwendige Bedingung für Identitäts-, noch für Identifizierungsprozesse. Je mehr sich jedoch Gesellschaftssysteme entwickeln, mobilisieren, ausdifferenzieren und je abstrakter ihre Interaktionsprozesse werden, desto häufiger treten Individuen mit Personen in Kontakt, die ihnen nicht persönlich bekannt sind. Häufig ergibt sich dann die Notwendigkeit, die Identität des Gegenübers sicher festzustellen. In einer derartigen Situation ermöglichen Ausweise den Nachweis der Identität, indem eine allseitig als glaubwürdig anerkannte Autorität in einem Dokument bestätigt, dass einer bestimmten natürlichen Person Merkmale wie Name, Vorname oder Adresse zugeschrieben werden. Diese Bestätigung dient der Versicherung Dritter, wirkt aber auch für den Inhaber des Dokuments, der sich mit ihm aus-weist – schon in dem Wort selbst klingt das „nach außen“ an.

Der Nachweis der Identität ist generell durch die Überprüfung dreier Gruppen von Merkmalen möglich, nämlich Besitz, Wissen und Sein.[3] Besitz kann sich auf ein einfaches Symbol, einen Papierausweis oder eine Chipkarte erstrecken, Wissen auf Informationen wie Name, Adresse, Passwort oder PIN. Sein knüpft demgegenüber an das äußere Erscheinungsbild, Verhaltensmuster oder genetische Informationen an. Diese Form der Identifizierung findet bei jeder alltäglichen Wiedererkennung eines Menschen durch einen anderen Menschen, aber auch bei modernen biometrischen Verfahren statt. Die Merkmale Besitz, Wissen und Sein sind beliebig miteinander kombinierbar. Wenn beispielsweise die Freischaltung einer Chipkarte nur durch die Kombination aus der Eingabe einer PIN und der Präsentation des Fingerabdrucks möglich ist, so werden alle drei Merkmale zugleich verwendet.

Erste Vorläufer der heutigen Ausweise waren Empfehlungsschreiben und andere Zeichen, durch deren (bloßen) Besitz schon in antiker Zeit bei Reisen die Zugehörigkeit zu einer Gemeinschaft oder einer Autorität bezeugt wurde. Für größere Gruppen lassen sich in Europa Papiere zum Nachweis der Identität ab dem 15. Jahrhundert feststellen.[4] Bereits zu Beginn des 18. Jahrhunderts konnte das Betreten eines fremden Hoheitsgebiets ohne derartige Papiere zu empfindlichen Strafen führen.

---

1 Erste Zeile des Gedichts „Der Ausweis“ von *E. Kaiser* (1983, 8).

2 Zu Reichweite und Einschränkungen dieser Pflicht vgl. unten 2.2.1.1.

3 *Schneier* 2000, 136 ff.; *Bolle/Connell/Pankanti/Ratha/Senior* 2004, 4, 20 ff.; *Reid* 2004, 9 ff.

4 S. *Groebner* 2001, 15 ff.; *ders*. 2004, 36 ff., 112 ff., 124 ff. et passim; vgl. zur historischen Entwicklung die Beiträge in *Caplan/Torpey* (Hrsg.) 2001.

Während die Nachfolger dieser ersten Reisepässe nach und nach weltweit gebräuchlich wurden, entwickelte sich nicht in allen Ländern eine allgemeine innerstaatliche Personalausweispflicht. In Deutschland wurde diese in der Zeit des Nationalsozialismus eingeführt und danach beibehalten.[5] Im anglo-amerikanischen Raum gibt es dagegen traditionellerweise keine staatlichen Personalausweise. Auch diese Länder können jedoch in ihren Wirtschafts- und Verwaltungsprozessen nicht auf jede Form von Ausweisen verzichten; auch sie vertrauen nicht (nur) dem Einzelnen, der behauptet, eine bestimmte Identität zu haben, sondern verlangen eine unabhängige Bestätigung, nämlich staatliche, halbstaatliche und private Funktionsäquivalente wie Sozialversicherungsnummern, Führerscheine und Betriebs- und Dienstausweise.[6] Je nach Kontext werden diese Dokumente auch in Staaten akzeptiert, die wie Deutschland über verpflichtende Personalausweise verfügen: Krankenversichertenkarten, Führerscheine, EC- und Kreditkarten oder Bibliotheksausweise verfolgen zwar auch administrative Zwecke, dienen jedoch im Grundsatz der Identifizierung der Inhaber.

Der Begriff des Ausweises kann sich also einerseits – enger – auf zwangsweise ausgegebene staatliche Papiere, oder andererseits – weiter – auf alle Dokumente beziehen, mit denen eine vertrauenswürdige Instanz die Identität des Inhabers bestätigt. Nach diesem weiten Verständnis ist die Existenz von Ausweisen eine Funktionsbedingung moderner Gesellschaften.[7] Alle Menschen, die an den Interaktionsprozessen dieser Gesellschaften teilhaben wollen, müssen also tatsächlich „einen Ausweis haben".

Diese Notwendigkeit führt indes zu einer Reihe von Problemen. Der Identitätsnachweis mittels eines Ausweises wirkt wie jede andere Form der Identifizierung auf denjenigen zurück, der zum Objekt dieses Vorgangs wird. Die Einführung von Ausweisen und ihre technische Fortentwicklung verändern deshalb die Interaktionsprozesse selbst. Die Person des Ausweisinhabers – und damit seine Identität – werden mit früheren Begebenheiten und Verhaltensweisen verbunden, die Tatsache der Identifizierung oder ihre Begleitumstände aktenkundig gemacht. Schließlich folgen, unmittelbar oder später, Reaktionen der identifizierenden Instanz oder einer anderen Stelle, die von dieser Informationen bezieht. Die Identifizierung (insbesondere mittels Ausweisen) wirkt so auf Prozesse der Identitätsbildung zurück. Dies vermag erhebliche individuelle und soziale Auswirkungen hervorzurufen.

Um sich diese Auswirkungen zu verdeutlichen, ist eine – kursorische – Verdeutlichung der Zusammenhänge zwischen Identität und Identifizierung hilfreich. Identität ist eine Antwort auf die Frage „wer bin ich?"[8] und bildet einen Gegenstand verschiedener For-

---

5 S. näher unten 2.2.1.1; erste Bsp. für sektorielle Ausweispflichten bei Boten und Soldaten lassen sich dagegen bereits im 15. Jahrhundert feststellen, s. *Groebner* 2004, 124 f.

6 Allerdings wird in sicherheitsrelevanten Bereichen regelmäßig nur ein staatliches Dokument akzeptiert. In den USA wurde bspw. nach den Anschlägen des 11.9.2001 die bis dahin übliche Praxis geändert, im Rahmen von innerstaatlichen Flugreisen Betriebsausweise zum Identitätsnachweis ausreichen zu lassen. Erforderlich ist nunmehr eine „government-issued photo ID", s. *Kent/Millet* 2003, 155 f.

7 *Caplan/Torpey* (2001, 1) sprechen von einem „Meilenstein in der Bildung des modernen Staates wie einer Bedingung privatwirtschaftlicher Betätigung"; s.a. *Torpey* 2000, 14 ff.; *IPTS* 2003, 40 f. („Indeed, in today's society it is no longer the individual who is trusted to justify his/her identity but instead it is the identity support/platform that he/she will present that is trusted. Therefore the crucial point of identity will be focused on the definition, the design and the value of these identity supports which will be the result of the identity building process and which will be the main tool of the identification process.").

8 *A. Blasi*, zitiert nach *Keupp/Höfer* 1997, 7; s.a. *Ellis* 2003, 43 („At its most basic level, 'identity' is about who we are"); zur Geschichte des Begriffs der Identität vgl. *Barkhaus* 1999, 55 ff. Jenseits seiner einzelnen Facetten beinhaltet er jedenfalls drei Elemente: die Einheit der verschiedenen Merkmale

schungsdisziplinen. Der Begriff wird in den Sozialwissenschaften in zwei Varianten verwendet: Als „personale Identität" bezeichnet er das Bewusstsein eines Menschen von seiner eigenen Kontinuität über die Zeit hinweg und die Vorstellung einer gewissen Kohärenz seiner Person, als „kollektive Identität" die Vorstellung von Gleichheit oder Gleichartigkeit mit anderen, die zum Zugehörigkeitsgefühl der Gruppenmitglieder beiträgt.[9]

Das Kernproblem der personalen Identität hat der Psychologe *Erikson* als „die Fähigkeit des Ichs" beschrieben, „angesichts des wechselnden Schicksals Gleichheit und Kontinuität aufrechtzuerhalten".[10] Das Mittel zur Herstellung dieser Kontinuität ist das „Gefühl der Ich-Identität", nämlich „das angesammelte Vertrauen darauf, dass der Einheitlichkeit und Kontinuität, die man in den Augen anderer hat, eine Fähigkeit entspricht, eine innere Einheit und Kontinuität (also das Ich im Sinne der Psychologie) aufrechtzuerhalten".[11]

In diesem Prozess sind Identität und Identifizierung untrennbar miteinander verbunden: Ein Individuum kann in den Augen Anderer nur dann Einheitlichkeit und Kontinuität besitzen, wenn es von diesen wiedererkannt wird; je nach der Form des Wiedererkennens und der Informationen, über die die Anderen bereits verfügen, verändert sich auch die Identität des Individuums. Identität ist damit der Weg, auf dem der Einzelne mit der Gesellschaft interagiert.[12] Sie wird auch als eine Konstruktion verstanden, die auf wechselseitige soziale Anerkennung angewiesen ist.[13]

Genau die gesellschaftlichen Entwicklungsprozesse, die die Notwendigkeit von Ausweisen (im weiteren Sinne) begründen, erschweren es dem Individuum zunehmend, das zur Identitätsbildung unabdingbare Maß an Kontinuität und Kohärenz herzustellen.[14] Der Einzelne kann in einer Gesellschaft, die durch immer stärker globalisierte, deregulierte und fragmentarisierte Wirtschafts- und Wertesysteme gekennzeichnet ist, immer weniger auf festgefügte Rollen- und Verhaltenskonzepte zurückgreifen.[15] Er ist deshalb gezwungen, diese selbst zu wählen, zu gestalten und das Verbindende, Konsistente in ihnen zu finden – mit der Chance der Selbstverwirklichung, aber auch der Gefahr der Überforderung.[16] Am Ende dieses Prozesses – der sich plastisch als „Identitätsarbeit"[17] bezeichnen lässt – steht

---

und Ausprägungen, die zu einer Person gehören (Kohärenz), deren zeitliche Beständigkeit (Kontinuität) und die Verankerung in physischen Charakteristika, s. *Bogdanowicz/Beslay* 2001; *IPTS* 2003, 39.

9 *Wagner* 1999, 45 m.w.N.; *Straub* 1999, 73 ff.; *Barkhaus* 1999, 57. Die beiden Perspektiven schließen sich nicht aus, sondern sind aufeinander bezogen.

10 *Erikson* 1964, 87, s. näher *Mey* 1999, 24 ff.; *Barkhaus* 1999, 61 ff.; zur Kritik am Konzept *Eriksons* s. *Keupp/Ahbe/Gmür/Höfer/Mitzscherlich/Kraus/Straus* 1999, 25 ff.; *Straub* 1999, 76 f. m.w.N.; *Mey* 1999, 37 ff. m.w.N.

11 *Erikson* 1973, 107.

12 *IPTS* 2003, 39.

13 *Keupp/Ahbe/Gmür/Höfer/Mitzscherlich/Kraus/Straus* 1999, 27 unter Verweis auf die modernen Identitätstheoretiker „von Hegel bis Mead"; s. zu dieser Dimension der Identität auch *Barkhaus* 1999, 60 f.; *Storch* 1999, 78 f. m.w.N.

14 Vgl. *Keupp/Ahbe/Gmür/Höfer/Mitzscherlich/Kraus/Straus* 1999, 33 ff.; *Keupp* 1997, 11 ff.; *Wagner* 1999, 50 ff.; *Storch* 1999, 70 ff.; s.a. *Mey* 1999, 67 ff., 73 ff.

15 Diese bildeten etwa den Kern des Personenmodells *Max Webers* im Sinne eines „stahlharten Gehäuses der Hörigkeit", s. *Keupp* 2001, 9; *Keupp/Ahbe/Gmür/Höfer/Mitzscherlich/Kraus/Straus* 1999, 22 f.

16 Dieser Doppelcharakter der „reflexiven Moderne" ist beschrieben bei *Beck* (1986 und 1993). Für den Einzelnen ergibt sich aus dieser ein ausfüllungsfähiger (aber auch -bedürftiger) „Möglichkeitsraum" (*Straub* 1999, 89).

17 *Keupp/Ahbe/Gmür/Höfer/Mitzscherlich/Kraus/Straus* 1999, 107 ff., 190 ff.; *Keupp* 2001, 11; *Straub* 1999, 87; ähnlich *Ellis* 2003, 35 ff. m.w.N.

die „multiple Identität“,[18] die nicht mehr ein gesichertes Endergebnis, sondern ein „passagerer Identitätszustand“ ist.[19]

In diese Prozesse der Identitätsbildung greifen Identifizierungsverfahren ein. Das gilt zunächst allgemein, im Besonderen jedoch für die Identifizierung durch Ausweise, deren vornehmliche Bedeutung in ihrer situations- und rollenübergreifenden Verwendbarkeit liegt. Das garantiert dem Inhaber die Möglichkeit, trotz wechselnder Sozialbeziehungen beständig über sich selbst Auskunft geben zu können. Es birgt jedoch die Gefahr, in unterschiedlichen gesellschaftlichen Zusammenhängen nicht mehr selbstbestimmt Rollen entwickeln und definieren zu können, weil die jeweiligen Interaktionspartner bereits über detaillierte Persönlichkeitsprofile verfügen oder den Einzelnen anhand abstrakter Kriterien typisierend einordnen. Ausweise sind ein hochgradig effektives Instrument zum Sammeln und Abrufen personenbezogener Daten. Bereits heute erfolgen mittels des maschinenlesbaren Personalausweises Abgleiche mit Fahndungsdatenbanken und Zugriffe auf Behördenakten. Wenn Identität hingegen die gesellschaftsvermittelte Möglichkeit eines Menschen ist, seine eigene Vergangenheit der Gesellschaft oder einzelnen Personen gegenüber so darzustellen, dass er diese Darstellung in der Gegenwart bejahen kann und die Chance erhält, für sie soziale Anerkennung und Bestätigung zu gewinnen,[20] so gefährden derartige mit Hilfe von Ausweisen hergestellte Datensammlungen die Chance des Einzelnen zur Eigendarstellung – mit der Gefahr, dass dabei Verhaltensmodelle aufoktroyiert und Identitäten beschädigt werden.[21]

Die rechtswissenschaftliche Perspektive fasst diese Frage als Teil der Problematik des Grundrechts auf informationelle Selbstbestimmung.[22] Diese „aus dem Gedanken der Selbstbestimmung folgende Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen“[23] wird verfassungsrechtlich garantiert, um dem Individuum „individuelle Entfaltungschancen“[24] zu erhalten, die es zur Herausbildung und Bewahrung seiner Identität benötigt.[25] Aus diesem Grund verbietet das Grundrecht dem Staat auch, „den Menschen zwangsweise in seiner ganzen Persönlichkeit zu registrieren und zu katalogisieren“.[26] Individuelle Gefahren für die Identität des Einzelnen bestehen dabei nur dann, wenn dieser erkannt wird. Die informationelle Selbstbestimmung schützt deshalb immer nur den identifizierten oder identifizierbaren Menschen; das Grundrecht ist in seinem Anwendungsbereich auf personenbezogene Daten beschränkt.

Der Zusammenhang zwischen Identität und Identifizierung ist also aus rechtswissenschaftlicher und sozialwissenschaftlicher Sicht gleichermaßen stark ausgeprägt. Die Wechselwirkungen zwischen Identitätsbildung und Identifizierung (mittels Ausweisen) sind

---

18 *Keupp* 2001, 7. Diese ist nicht zu verwechseln mit der multiplen Persönlichkeit (die ein Persönlichkeitsmodell ist, in dem die Teileinheiten – als Folge eines unverarbeiteten Traumas – keine Verbindung mehr miteinander haben), vgl. ebd.; s.a. *Ellis* 2003, 34; *Storch* 1999, 73 ff.

19 *Keupp/Ahbe/Gmür/Höfer/Mitzscherlich/Kraus/Straus* 1999, 85.

20 Vgl. *Luhmann* 1965, 60 ff.; ähnlich AK GG-*Podlech*, Art. 1 Abs. 1 Rn. 34 ff.; s.a. *Bernstein*, CRi 2005, 1 f. m.w.N. Private Lebensbereiche und -dimensionen sind unabdingbare Voraussetzung autonomer Lebensführung, s. dazu *Rössler* 2001, 127 ff., 136 ff., 201 ff. et passim.

21 S. zu diesem Aspekt näher unten 4.2.1.2.4.

22 In Extremfällen kann auch die Menschenwürdegarantie einschlägig sein. Der Schutz der physischen und psychischen Identität (und Integrität) bildet eine Fallgruppe von Art. 1 Abs. 1 GG, s. AK GG-*Podlech*, Art. 1 Abs. 1, Rn. 23 ff.; *Maihofer* 1968, 56 ff.; *Häberle*, HdbStR II (2004), § 22 Rn. 45 ff.; *Pieroth/Schlink* 2003, Rn. 361 (vgl. auch 12. Auflage 1996, Rn. 389 ff.).

23 BVerfGE 65, 1 (42); s. ausführlich unten 4.1.1.2.

24 BVerfGE 65, 1 (43).

25 Zur weitergehenden Komponente der informationellen Selbstbestimmung als „strukturelle[r] Komponente jeder demokratischen Gesellschaft“ (*Simitis*, DuD 2000, 714, 719) vgl. unten 4.1.1.2.

26 So bereits BVerfGE 27, 1 (6); damals als Verstoß gegen die Menschenwürdegarantie gefasst.

immer dann zu überprüfen, wenn eine neue Ausweisgeneration neue Formen der Datensammlung, Profilbildung und Zuschreibung ermöglicht. Das wird beispielsweise an der Diskussion deutlich, die in Deutschland im Jahre 1987 durch den Übergang vom papiernen Personalausweis zur maschinenlesbaren Karte ausgelöst wurde, die derzeit im Einsatz ist.[27]

Als nächste Ausweistechnologie steht – in unterschiedlichen technischen Ausprägungen – die Chipkarte bereit. Aufgrund ihrer vielfältigen Einsatzmöglichkeiten werden die Auswirkungen ihrer Einführung die Folgen der Einführung des maschinenlesbaren Personalausweises bei weitem übertreffen; es fällt deshalb auf, dass – verglichen mit der Vehemenz der damals geführten Auseinandersetzung – derzeit praktisch kaum eine öffentliche Diskussion um Chipkartenausweise stattfindet.

Chipkarten finden bereits in einer Vielzahl von Lebensbereichen Verwendung und werden teilweise auch schon als Ausweise eingesetzt. Beispiele sind Krankenversichertenkarten, Betriebs- und Studentenausweise.[28] In der Diskussion sind zurzeit vor allem zwei allgemeine Ausweise, die als leistungsfähige Mikroprozessorkarten ausgestattet werden könnten. Ein zukünftiger „digitaler Personalausweis" wird biometrische Daten zur sicheren Identifikation des Inhabers enthalten und könnte darüber hinaus Zusatzapplikationen wie die Erstellung qualifizierter elektronischer Signaturen bieten. Die vom Gesetzgeber bereits vorgeschriebene „elektronische Gesundheitskarte"[29] (vorgesehener Starttermin 1. Januar 2006) soll nicht nur den Nachweis der Identität und der Mitgliedschaft in der gesetzlichen Krankenversicherung ermöglichen, sondern auch in großem Umfang medizinische Informationen aufnehmen oder den Zugriff auf sie vermitteln. Beide Chipkartenausweise werden die Identifikationsmechanismen und -umgebungen ihrer Vorgänger grundlegend erweitern und verändern:

- Wenn auf Chipkarten biometrische Daten gespeichert und dort oder in den zugehörigen Lesegeräten automatisiert verarbeitet werden,[30] so ermöglicht dies – die Zuverlässigkeit der Verfahren vorausgesetzt – eine sichere Verbindung zwischen Person und Identitätsdokument: Der Prozess der Identifizierung wird unmittelbar an das „Sein" dieser Person geknüpft, auch wenn diese der identifizierenden Instanz nicht selbst bekannt ist.
- Die Verfahren der elektronischen Signatur und Authentisierung erweitern den Identitätsnachweis in eine „virtuelle" Welt. Chipkartenausweise werden so zum Zugangsinstrument für Anwendungen und Daten (beispielsweise aus dem Gesundheitsbereich), die in peripheren Netzen gespeichert sind; gleichzeitig können sie ihre Funktion des Identitätsnachweises gegenüber unbekannten Interaktionspartnern (zumindest potentiell) global erfüllen, ohne dass sich der Ausweisinhaber physisch bewegen muss.
- Schließlich ist es denkbar, diese beiden Dimensionen miteinander zu verknüpfen. Wenn der Einsatz des Ausweises in der „virtuellen" Welt an die Authentisierung mittels biometrischer Merkmale geknüpft wird, kann auch eine Identifikation in

27 Vgl. hierzu näher unten 7.3.2.2.

28 S. zu diesen und anderen Beispielen unten 2.3.1.

29 Im Rahmen der Arbeit wird durchgängig die deutsche Gesetzesterminologie verwendet (vgl. die Regelung in § 291a SGB V), also elektronische Gesundheitskarte, elektronischer Heilberufsausweis und elektronische Patientenakte. In den medizinischen und technischen Fachdiskussionen finden stattdessen häufig die Begriffe Patient Data Card (oder Electronic Health Card), Health Professional Card (HPC) und Electronic Health Record Verwendung.

30 Personalausweis und Reisepass enthalten auch heute schon Angaben über körperliche Merkmale. Da diese nicht automatisiert geprüft werden, handelt es sich jedoch nicht um biometrische Daten im eigentlichen Sinne, s.u. 2.3.3.1.

weltweiten Netzen fest mit der Person des Ausweisinhabers selbst – im Unterschied zu seinem Besitz (des Ausweises) und Wissen (einer PIN oder eines Passworts) – verbunden werden.

Man muss nicht (wie teilweise in der US-amerikanischen Diskussion vertreten)[31] bereits die Existenz von Ausweisen als Gefahr für die Identitätsbildung begreifen, um zu erkennen, dass diese Funktionserweiterungen grundlegende rechtliche, technische und soziale Fragen aufwerfen.[32] Identifikationsmechanismen gewährleisten die Interaktionsfähigkeit der handelnden Personen in der Privatwirtschaft und sind unabdingbare Voraussetzung für eine Vielzahl von Rechten gegenüber dem Staat und anderen Autoritäten.[33] Hoheitliche und private Akteure können Ausweise jedoch rechtswidrig zweckfremd verwenden, die gewonnenen Daten missbrauchen und so die Ansprüche des Einzelnen auf Selbstbestimmung und Privatheit beschneiden.

Auch der rechtmäßige Gebrauch der Ausweise ist keineswegs unproblematisch. Zunächst sind die gesetzlich bestimmten Verwendungszwecke, und damit die Grenze zwischen Gebrauch und Missbrauch eines Ausweises, innerhalb der verfassungsrechtlichen Grenzen veränderbar und damit bis zu einem bestimmten Grad willkürlich. Außerdem können Ausweise, auch wenn sich ihr Einsatz im Rahmen der gesetzlich definierten Grenzen bewegt, durch ihre weitreichende Verwendbarkeit zur Sammlung und Nutzung von Daten das Selbstverständnis und die Interaktion der beteiligten Personen verändern – die individuelle Eigendefinition des Inhabers stößt auf ein „behördliches" Verständnis von Identität und wird dabei auf eine Sammlung formeller Merkmale reduziert, die eine für soziale und wirtschaftliche Beziehungen sowie für den Umgang mit Behörden notwendige Identifizierung und Authentifizierung ermöglicht.[34] Den neuen Möglichkeiten, die die ständige Verfügbarkeit von Daten bietet, stehen also Risiken gegenüber, die durch die Intransparenz der Dateninhalte und Verarbeitungsmechanismen, die Masse der Daten, deren Sensibilität und die Möglichkeit der Zusammenführung bisher verteilt gespeicherter Informationen verursacht werden.

Diese Ambivalenz des Prozesses der Identifizierung mittels Ausweisen ist nichts Neues; neu sind aber die Methoden, die bei diesem Prozess angewandt werden, die Chancen, die sich für Individuum und Gesellschaft ergeben und die Gefährdungslagen, die für den Ausweisinhaber und seine Identität entstehen.

Art und Gewicht sowohl der Chancen als auch der Risiken hängen von der konkreten technischen Ausprägung der jeweiligen Chipkarte und der mit ihr interagierenden Umgebung ab. Beide können das Recht des Inhabers auf informationelle Selbstbestimmung schützen, umgekehrt aber auch verletzten: Der Erfinder der Chipkarte, *Jürgen Dethloff*, spricht vom Konflikt zwischen der Chipkarte „als Schild des Bürgers zur Bewahrung, ja

---

31 S. z.B. *Sobel*, 8 B.U. J. Sci. & Tech. L. 37, 40: „Databanks and other identification schemes imply that society and government have the legitimate power to define and derive individual identities separate from the inherent nature of personhood."

32 Diese sind Teil des allgemeinen Einflusses der Entwicklung der Informationsgesellschaft auf den Prozess der Identitätsbildung (*IPTS* 2003, 40) und bestehende Partizipationsmöglichkeiten (ebd., 12: „The digitisation of identity may be regarded as a bottleneck to the engagement of citizens with Information Society services because without it there is effective exclusion."); s.a. den Literaturüberblick von *Ellis* 2003, insbes. 14 ff.; „Identitäten im Internet" werden untersucht von *Breidenbach/Zukrigl*, Aus Politik und Zeitgeschichte, B 49-50/2003, 29 ff.; s. dazu auch *Bernstein*, CRi 2005, 1, 2 ff.; s.a. *Rejman-Greene* 2003b, 14 ff.

33 *Caplan/Torpey* 2001, 6; *Rössler* 2001, 228 f.

34 Zu dieser Perspektive *Bogdanowicz/Beslay* 2001.

möglichen Herstellung seiner Anonymität“ und der Chipkarte „als einem Instrument der Herrschenden“.[35]

Vor diesem Hintergrund untersucht die vorliegende Abhandlung anhand der Beispiele des digitalen Personalausweises und der elektronischen Gesundheitskarte rechtliche, technische und soziale Aspekte der Verwendung von Chipkarten als Ausweise. Der Gegenstand der Arbeit kann wie folgt umrissen werden:

- Die Erarbeitung der rechtlichen Anforderungen an die Ausgestaltung und den Einsatz von Chipkartenausweisen, die Bewertung der technischen Umsetzungsmöglichkeiten und die Abschätzung der zu erwartenden Akzeptanz. Der Schwerpunkt der rechtlichen Untersuchung liegt im Bereich des Datenschutzrechts, wobei verfassungs- und einfachrechtliche Aspekte in den Blick genommen werden.
- Die Betrachtung der Chipkarte nicht als solche, sondern im Zusammenhang mit der technischen Infrastruktur, mit der sie interagiert. Dementsprechend werden der Aufbau und die Funktionsweise dieser Infrastruktur an den entsprechenden Stellen behandelt. Allgemeine Aspekte des Personalausweisrechts,[36] des Einsatzes von Telematik[37] im Gesundheitswesen[38] und des „Identitätsmanagements“[39] bleiben jedoch außen vor.
- Die Berücksichtigung einer absehbaren großen Anwendung für den Einsatz von Chipkartenausweisen als sichere Signaturerstellungseinheiten. Das größte Projekt im Bereich qualifizierter elektronischer Signaturen könnte in Zukunft das so genannte „JobCard“-Verfahren werden. Deshalb werden die politischen Hintergründe, die rechtlichen Rahmenbedingungen, die verfassungsrechtlichen Anforderungen, die technische Umsetzung und die zu erwartende Akzeptanz dieses Verfahrens betrachtet. Da noch keine gesetzliche Regelung besteht und das System keine Chipkarte einführt, sondern voraussetzt, erfolgt aber nur eine knappe Analyse.

Die Ausführungen gliedern sich im Folgenden in sechs Abschnitte. Der nächste Teil behandelt die politischen Rahmenbedingungen des Einsatzes von Chipkartenausweisen, ihre rechtlichen und technischen Grundlagen sowie methodische Überlegungen (2). Danach gibt das Kapitel zur internationalen Entwicklung Aufschluss über den Fortschritt von Ausweisprojekten im Ausland (3). Der datenschutzrechtliche Abschnitt beinhaltet verfassungsrechtliche Anforderungen des Grundrechts auf informationelle Selbstbestimmung und Vorgaben des einfachgesetzlichen Datenschutzrechts (4). Im Anschluss werden die

35 *Dethloff* 1992, 3 (zitiert nach *Elkeles/Rosenbrock* 1995, 1).

36 Vgl. dazu *Medert/Süßmuth* 1998; aus datenschutzrechtlicher Sicht Roßnagel-*Wollweber*, Kap. 8.5.

37 Der Begriff Telematik bezeichnet Anwendungen im Bereich von *Tele*kommunikation und Infor*matik*, s. *Berger & Partner* 1997, 20 m.w.N. Telematik ist nicht identisch mit Telemedizin. Diese umfasst die Erbringung konkreter medizinischer Leistungen mit den Mitteln der Telematik (*Goetz* 2001, 10); s. näher *Grätzel v. Grätz* 2004c, 69 ff.

38 Dazu *Hermeler* 2000; *Kraft* 2003; *Dierks/Nitz/Grau* 2003; *Ulsenheimer/Heinemann*, MedR 1999, 197 ff. und die Beiträge in *Grätzel v. Grätz* 2004c; zur Rechtslage der elektronischen Patientenakte vor dem GKV-Modernisierungsgesetz *Laskaridis* 2003; zum elektronischen Rezept aus technischer Sicht *Warda/Noelle* 2002, 112 ff.

39 Darunter ist die Aufgabe zu verstehen, verschiedene „virtuelle“ Teilidentitäten einer Person zu verwalten und den Benutzer bei der Auswahl dieser Identitäten für verschiedene Zwecke zu unterstützen. Hierzu besteht eine Verbindung, da Chipkartenausweise in bestimmten technischen Ausprägungen als Identitätsnachweis in „virtuellen“ (d.h. durch offene Netze gebildeten) Welten dienen. Dieser Aspekt liegt jedoch jenseits des Themas dieser Arbeit, s. näher *Hansen/Krasemann/Rost/Genghini*, DuD 2003, 551 ff.; *Scholz* 2003, 398 ff. m.w.N.; *Köhntopp/Pfitzmann* 2000, 316 ff.; Roßnagel-*Hansen*, Kap. 3.3, Rn. 88 ff.; zu den sicherheitstechnischen und datenschutzrechtlichen Aspekten auch *Liberty Alliance* 2003.

Anforderungen des Rechts der elektronischen Signatur betrachtet, die besondere Bedeutung für Ausweiskarten erlangen (5). Der darauf folgende Teil setzt sich mit der technischen und organisatorischen Umsetzbarkeit der Ausweisprojekte auseinander (6). Abschließend erfolgt eine Abschätzung der zu erwartenden Akzeptanz dieser Projekte (7).

Die gefundenen Ergebnisse sind – unter dem Vorbehalt der Anpassung an die Besonderheiten der jeweiligen Einsatzumgebung – auf eine Reihe anderer, zukünftig zu erwartender Chipkartenausweise übertragbar. Beispiele könnten Dienstausweise, Truppenausweise und Betriebsausweise sein, die weithin vergleichbare Chancen und Problemfelder mit sich bringen. Das gilt im besonderen Maße für die Einführung biometrischer Daten auf dem Reisepass, die voraussichtlich vor der Einführung des digitalen Personalausweises erfolgen wird.[40] Ein Pass im Chipkartenformat ist zwar solange nicht realistisch, wie Visa-Aufkleber und Stempel bei der Ein- und Ausreise verwendet werden.[41] Auf absehbare Zeit wird es deshalb hier bei einer papiernen, um einen kontaktlosen Chip erweiterten Form bleiben. Diese ist jedoch auch für den digitalen Personalausweis eine Umsetzungsvariante. Aufgrund dieser Parallelität sind die Ausführungen zu den rechtlichen Anforderungen und der technische Umsetzbarkeit der Biometrie von wenigen Ausnahmen abgesehen auf den Reisepass übertragbar, zumal die entsprechenden Normen von Personalausweis- und Reisepassgesetz wortgleich sind.[42] Um Wiederholungen zu vermeiden, wird darauf nicht jeweils gesondert hingewiesen.

40 Durch die Verordnung (EG) Nr. 2252 v. 13.12.2004 (ABl. EG 2004 L 385/1) wird den Mitgliedstaaten der EU sowohl die Speicherung von Gesichts- als auch von Fingerabdrucksdaten verbindlich vorgeschrieben; s. näher *Roßnagel/Hornung*, DÖV 2005, i.E. und unten 3.1.2.

41 Beides ließe sich theoretisch auch elektronisch umsetzen; dies ist jedoch für eine Vielzahl von Staaten kurzfristig kaum durchführbar.

42 § 1 Abs. 4 und 5 PersAuswG entsprechen § 4 Abs. 3 und 4 PassG, § 3 Abs. 5 PersAuswG entspricht § 16 Abs. 6 PassG. Allerdings werden die Normen des PassG verdrängt, soweit sie der Verordnung (EG) Nr. 2252 v. 13.12.2004 (Fn. 40) widersprechen, s.u. 3.1.2.

2 Grundlagen

2.1 Zur Einführung von Chipkartenausweisen

Die Motive zur Einführung von Chipkartenausweisen sind bis zu einem gewissen Grad verallgemeinerbar. Angestrebt werden meist eine Erhöhung der Sicherheit, eine Reduzierung von Kosten, die Vereinfachung von Prozessabläufen, die dezentrale Verfügbarkeit von Daten und die Kontrollierbarkeit von Zugriffen durch den Karteninhaber. Diese Ziele werden allerdings nicht durchgängig verfolgt und sind teilweise auch nicht miteinander vereinbar. Die Erhöhung des Sicherheitsniveaus der jeweiligen Anwendung spielt allerdings durchweg eine Rolle: Bezweckt wird die Verbesserung der Sicherheit des elektronischen Rechtsverkehrs, der Personenkontrollen durch die staatlichen Gefahrenabwehr- und Strafverfolgungsbehörden oder der Datenströme in einem Gesundheitswesen, das über eine Telematikstruktur verfügt.

Jenseits dieses Beweggrunds sind die Motive teilweise unterschiedlich. So spielen etwa im Gesundheitswesen und beim JobCard-Verfahren Fragen der Effizienz und Kostenersparnis eine erhebliche Rolle. Der digitale Personalausweis wird dagegen sowohl in der Herstellung als auch in der Anwendung erheblich teurer als das bisherige Modell werden, sodass es hier nur darum gehen kann, die zusätzlichen Kosten möglichst gering zu halten. Im Gesundheitsbereich besteht ein wesentliches Motiv in der Stärkung der Patientenautonomie und der Datenhoheit der Betroffenen; beides spielt beim digitalen Personalausweis keine Rolle. Bei der Beantragung des Personalausweises werden in Zukunft neuartige Daten erhoben, während es bei der elektronischen Gesundheitskarte und dem JobCard-Verfahren um den Umgang mit Daten geht, die auch im bisherigen System verwendet werden.

Trotz dieser Unterschiede weisen die drei im Folgenden erläuterten Vorhaben vielfältige Gemeinsamkeiten auf und sind teilweise aufeinander bezogen. Dies dürfte das wesentliche Motiv der Bundesregierung gewesen sein, die Projekte am 9. März 2005 zu einer gemeinsamen „eCard-Strategie“ zusammenzufassen.[43]

2.1.1 Der digitale Personalausweis

Hinter der in Deutschland (und vielen andere Staaten)[44] verfolgten Idee eines digitalen Personalausweises stehen zwei grundsätzlich verschiedene, jedoch miteinander vereinbare Konzepte: Einerseits soll die hergebrachte Identifizierungsfunktion mittels biometrischer Daten verbessert, andererseits die möglichst weite Verbreitung von Chipkarten, die zur Erstellung qualifizierter elektronischer Signaturen im Sinne von § 2 Nr. 3 SigG geeignet sind, erreicht werden.[45]

Die Anschläge des 11. September 2001 auf das World Trade Center und das Pentagon und die nachfolgende sicherheitspolitische Diskussion haben Forderungen nach einer Neukonzeption des deutschen Personalausweises laut werden lassen. Diese fanden ihren Niederschlag im Terrorismusbekämpfungsgesetz vom 9. Januar 2002.[46] Durch dieses Artikelgesetz wurde unter anderem in § 1 Abs. 4 und 5 PersAuswG eine „Ankündigung“

43 Vgl. http://www.bundesregierung.de/-,413.799497/artikel/eCard-Strategie-der-Bundesregi.htm.
44 S. dazu unten 3.
45 Vgl. zum Folgenden *Roßnagel*, in: Reichl/Roßnagel/Müller 2005, 3 ff.; *ders*., DuD 2005, 59 ff.
46 Gesetz zur Bekämpfung des internationalen Terrorismus, BGBl. I, 361.

der Aufnahme weiterer biometrischer Merkmale in den Ausweis aufgenommen.[47] Nach der Gesetzesbegründung soll dadurch die computergestützte Prüfung des Ausweises ermöglicht und so dessen Fälschungssicherheit und die zweifelsfreie Identifikation des Inhabers sichergestellt werden.[48]

Die Entwicklung in Deutschland ist massiv durch außenpolitische Einflüsse geprägt. Sicherheitsexperten in einer Vielzahl von Ländern forderten nach den Anschlägen des 11. September die Einführung biometrischer Daten in Reisedokumente. Unter diesem Eindruck verabschiedete die Vollversammlung der Vereinten Nationen am 28. September 2001 die Resolution 1373 „Zur Verhütung und Bekämpfung des Terrorismus", in der „Maßnahmen zur Verhütung der Nachahmung, Fälschung und betrügerischen Nutzung von Ausweisen und Reisedokumenten" gefordert werden, um Bewegungen von Terroristen zu verhindern.[49] In der Folge setzten internationale Bestrebungen der International Civil Aviation Organisation (ICAO)[50] und der Gruppe der Acht (G8)[51] ein. Der stärkste Impuls zur Verwendung von Biometrie in Reisedokumenten ging allerdings von den USA aus,[52] die einerseits maßgeblich die Maßnahmen der ICAO zur globalen Einführung von Biometrie in Reisedokumenten beeinflussten,[53] andererseits unabhängig von der internationalen Entwicklung nationale Maßnahmen beschlossen. Durch neue Gesetze (Enhanced Border Security and Visa Entry Reform Act[54] und Provide Appropriate Tools Required to Intercept and Obstruct Terrorism (PATRIOT) Act[55]) wurde die Grundlage dafür geschaffen, dass seit Anfang des Jahres 2004 von allen visumpflichtigen Einreisenden digitale Photos und Fingerabdrucksdaten erhoben werden.[56] Die Staaten, die Partner des Visa-Waiver-Abkommens sind,[57] wurden unter Androhung der Kündigung des Abkommens dazu verpflichtet, ab dem 26. Oktober 2004 biometrische Daten in ihren Reisepässen einzuführen.[58] Nachdem sich abzeichnete, dass dieser Termin weder von diesen Staaten noch

47 S. näher unten 2.2.1. Weitere Änderungen zu Identitätspapieren betreffen den Reisepass und Dokumente für Ausländer; s. hierzu unten 4.2.2.2 a.E. (Fn. 1044).

48 S. BT-Drs. 14/7368, 48; kritisch zur Möglichkeit, durch biometrische Merkmale die Fälschungssicherheit zu erhöhen, *Petermann*, TAB-Brief Nr. 24 (2003), 19; in der Tat dürfte es im Wesentlichen um die Herstellung einer festen Verbindung zwischen Person und Personalausweis gehen.

49 Resolution Nr. 1373 v. 28.9.2001 (UN-Doc. S/RES/1373(2001), unter 2 g); die Gesetzesbegründung zur Änderung des PersAuswG nimmt ausdrücklich hierauf Bezug, s. BT-Drs. 14/7386, 48.

50 Ausführlich zur Rolle der ICAO s.u. 3.1.1.

51 Diese Staaten (Deutschland, Frankreich, Großbritannien, Italien, Japan, Kanada, Russland und die USA) haben eine Arbeitsgruppe für Biometrie in Reisedokumente gebildet, vgl. http://www.heise.de/newsticker/meldung/32991.

52 Zur Entwicklung etwa *TAB* 2004, 13 ff.; *Petermann*, TAB-Brief Nr. 24 (2003), 19.

53 S. zu den Beratungen der ICAO und der Position der USA *ACLU* 2004, 3 ff. m.w.N.

54 Abrufbar unter http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_public_laws&docid=f:publ173.107.pdf.

55 Abrufbar unter http://thomas.loc.gov/cgi-bin/query/D?c107:1:./temp/~c107zZlrN6::.

56 S. http://www.heise.de/newsticker/meldung/43295; Sec. 303 (b) (1) und (2) des Enhanced Border Security and Visa Entry Reform Act sahen als letzte Frist hierfür den 26.10.2004 vor. Derzeit werden an den US-Grenzen bei visapflichtigen Einreisenden zwei Finger (flach) und ein Webcam-Bild aufgenommen. Letzteres wird allerdings nicht biometrisch verarbeitet.

57 Die Angehörigen dieser Staaten dürfen mit ihrem Reisepass ohne Visum in die USA einreisen. Die USA entscheiden von Fall zu Fall über die Aufnahme in das Abkommen, das im Mai 2005 27 Partner hatte (Andorra, Australien, Belgien, Brunei, Dänemark, Deutschland, Finnland, Frankreich, Großbritannien, Irland, Island, Italien, Japan, Liechtenstein, Luxemburg, Monaco, Neuseeland, die Niederlande, Norwegen, Österreich, Portugal, San Marino, Schweden, die Schweiz, Slowenien, Singapur und Spanien).

58 Die Rechtslage ist in sich widersprüchlich. Einerseits heißt es in Sec. 303 (c) (1) des Enhanced Border Security and Visa Entry Reform Acts, die Staaten müssten bis zum 26.10.2004 ein „Programm" zur Einführung biometrischer Daten (und nicht etwa diese Daten selbst) implementieren. Das hätte einen

von den USA selbst eingehalten werden konnte, wurde die Frist durch den Kongress um zunächst ein Jahr verlängert. Eine weitere Verlängerung erscheint einerseits wahrscheinlich, da die US-Administration selbst davon ausgeht, innerhalb dieses Jahres keine Pässe mit biometrischen Daten ausstellen zu können.[59] Andererseits zeigte sich der Vorsitzende des Justizausschusses des US-Repräsentantenhauses im Frühjahr des Jahres 2005 ablehnend gegenüber einer entsprechenden Anfrage des zuständigen EU-Kommissars *Frattini*.[60] Während der Übergangszeit sind auch Reisende, die Angehörige von Staaten des Visa-Waiver-Abkommens sind, bei der Einreise zur Abgabe von Fingerabdrücken und digitalen Gesichtsbildern verpflichtet.

Die Vorgaben der USA sind für den deutschen Personalausweis zunächst nur von untergeordneter Bedeutung, weil mit diesem dort ohnehin keine Einreise möglich ist. Innerhalb Europas ist der Personalausweis jedoch ein vollwertiges Reisedokument,[61] sodass er die Vorgaben der ICAO einhalten muss. Überdies enthält der Personalausweis zwar zum Teil andere Daten als der Reisepass.[62] Er entspricht aber in Herstellungsprozess, Aufbau und Sicherheitsmerkmalen der Plastikkarte, die in den Reisepass eingenäht ist. Diese Kongruenz ist nicht zwingend, eine Trennung könnte jedoch zu höheren Kosten und unterschiedlichen Prüfanforderungen bei Kontrollen führen. Am 18. Januar 2005 trat die Verordnung (EG) Nr. 2252/2004 in Kraft, die die Mitgliedstaaten zur Einführung biometrischer Daten des Gesichts und des Fingers in ihre Reisepässe verpflichtet.[63] Deshalb steht zu erwarten, dass sich die technische Umsetzung zunächst auf den Pass konzentrieren und der Personalausweis erst im nächsten Schritt folgen wird.

Neben der Verbesserung der Fälschungs- und Identifikationssicherheit eröffnet die Weiterentwicklung des Personalausweises zu einem digitalen Personalausweis die Perspektive einer Stärkung der Sicherheit des elektronischen Rechtsverkehrs durch die Verbreitung elektronischer Signaturverfahren. Deshalb gibt es auch entsprechende Forderungen nach der Einführung eines signaturfähigen Personalausweises.[64] Beweggrund ist insbesondere die Möglichkeit der Kostenreduzierung, die ein flächendeckender Einsatz elektronischer Signaturen ermöglichen könnte. Allein das Einsparungspotential in der Verwaltung wird auf 400 Millionen Euro geschätzt.[65]

---

relativ weiten Spielraum ermöglicht. Gleichzeitig bestimmt jedoch Sec. 303 (c) (2), dass Reisedokumente, die ab dem 26. 10.2004 ausgestellt werden, nur dann akzeptiert werden sollten, wenn sie biometrische Daten enthalten. Daraus folgt, dass de facto bis zu diesem Zeitpunkt das Format des Reisepasses umgestellt werden musste.

59 Das liegt v.a. an immer noch bestehenden Standardisierungsproblemen, s. http://www.cardtechnology.com/cgi-bin/readstory.pl?story=20050114CTDN800.xml. Offenbar werden auch nicht an allen US-amerikanischen Grenzübergängen Kartenlesegeräte verfügbar sein, s. http://www.cardtechnology.com/cgi-bin/readstory.pl?story=20050425CTDN467.xml

60 S. http://europa.eu.int/idabc/en/document/4068/194; http://europa.eu.int/idabc/en/document/3317/194.

61 Grenzübertrittspapier ist der Reisepass, der nach § 2 Abs. 1 Nr. 1 DVPassG aber grundsätzlich durch den Personalausweis ersetzt werden kann, sofern sich nicht aus dem Passersatz, aus Rechtsvorschriften oder aus zwischenstaatlichen Vereinbarungen etwa anderes ergibt (§ 2 Abs. 2 DVPassG).

62 Der Reisepass enthält nach § 4 Abs. 1 Satz 2 Nr. 6 PassG – anders als der Personalausweis – eine Angabe über das Geschlecht des Inhabers. Anstatt der gegenwärtigen Anschrift (vgl. § 1 Abs. 2 Satz 2 Nr. 8 PersAuswG) wird gemäß § 4 Abs. 1 Satz 2 Nr. 9 PassG der Wohnort eingetragen. Die übrigen Angaben sind identisch.

63 Abl. EG 2004, L 385/1; s. näher *Roßnagel/Hornung*, DÖV 2005, i.E. und unten 3.1.2.

64 S. etwa *Initiative D21* 2002; *BITKOM* 2002, 22; s.a. *Roßnagel*, in: Reichl/Roßnagel/Müller 2005, 7 f.; *ders*., DuD 2005, 59.

65 Aussage des Staatssekretärs im Bundesministerium des Innern *Wewer*, vgl. *Schulzki-Haddouti* 2003.

Für den Einsatz rechtsverbindlicher elektronischer Signaturen sind in Deutschland in den letzten Jahren die notwendigen Rechtsgrundlagen geschaffen worden.[66] Auch im technischen Bereich ist inzwischen die entsprechende Infrastruktur vorhanden.[67] Dennoch werden die vorhandenen Signaturverfahren bislang nicht in weitem Umfang eingesetzt. Das liegt an zwei Problemen, die einen circulus vitiosus bilden.[68] Da es bislang weder attraktive Anwendungen für die elektronische Signatur noch eine hinreichende Zahl von Kommunikationspartnern gibt, die ebenfalls über die Möglichkeit der Signaturerstellung verfügen, besteht kein Anreiz für den Bürger, sich eine – Kosten verursachende – Signaturkarte nebst Hard- und Softwareausrüstung zuzulegen.[69] Solange umgekehrt die Zahl der Nutzer die kritische Masse nicht erreicht, die für einen profitablen Betrieb von Anwendungen erforderlich ist, besteht auf Anbieterseite kein Anreiz, in derartige Anwendungen zu investieren.

Ein signaturfähiger Personalausweis könnte im Ergebnis 60 Millionen Deutschen eine sichere Signaturerstellungseinheit verschaffen und für Entwickler und Systemintegratoren die Sicherheit bieten, dass eine hinreichende Zahl von Personen in der Lage wäre, qualifizierte elektronische Signaturen zu erstellen.[70] Überdies sind durch Kostendegressionseffekte erheblich preiswertere Signaturkarten, Lesegeräte und Anwendungen zu erwarten. Auch die Standardisierung der Verfahren und Komponenten könnte durch das Projekt befördert werden. Der Personalausweis könnte eine Alternative zu Plänen im Rahmen des „Signaturbündnisses“ sein, Signaturverfahren auf den EC-Karten der Banken anzubieten.[71] Ein so konzipierter Personalausweis bietet erhebliche Vorteile:[72]

- Er weist gegenüber anderen Signaturkarten eine deutlich höhere Identifizierungssicherheit auf, die unmittelbar zu einem Zugewinn an Rechtssicherheit führt.[73]
- Für die Verbindung von Signaturfunktion und Personalausweis spricht ein höheres Vertrauen in staatliche Ausweisdokumente, die der Akzeptanz der elektronischen Signatur zugute kommen würde.
- Außerdem verfügt der Ausweis über einen sehr hohen Verbreitungsgrad, während etwa die Inhaberschaft einer EC-Karte nicht nur von der Entscheidung des Bürgers, sondern auch der Bank abhängig ist, die nicht verpflichtet ist, jedem ihrer aktuellen oder potentiellen Kunden eine solche auszustellen. Selbst eine elektronische Gesundheitskarte mit qualifizierter Signaturfunktion würde nur die Mitglieder der gesetzlichen Krankenversicherung, also nur einen Teil der Bevölkerung erfassen.

---

66 S.u. 5.1.

67 Im Mai 2005 gab es 28 akkreditierte Anbieter elektronischer Signaturen, vgl. die Übersicht der RegTP unter http://www.regtp.de → elektronische Signatur → Zertifizierungsdiensteanbieter.

68 S. z.B. *Roßnagel*, MMR 2003, 1 f.; *GI/ITG*, DuD 2003, 763 ff.; *Strasser/Müller/Roßnagel/Gitter*, in: Reichl/Roßnagel/Müller 2005, 248 ff.; *Gitter/Strasser*, DuD 2005, 74 f. Neben dem im Folgenden erläuterten Hauptproblem behindert auch die Infrastrukturpolitik der Bundesregierung die Verbreitung, da diese intern ein alternatives Verfahren verwendet, das nicht signaturgesetzkonform ist; s. näher *Roßnagel*, MMR 2002, 215, 221.

69 Das Starterpaket der Signtrust (Signaturkarte, Kartenleser und Software in der Minimalversion) kostete bspw. im Mai 2005 103,24 Euro; in den Folgejahren betrug die Gebühr jeweils 45,24 Euro; zu den Anwendungen, die im Test- und Pilotbetrieb laufen, s. z.B. *Viefhues/Scherf*, K&R 2002, 170, 171.

70 S. zum digitalen Personalausweis als Infrastrukturelement *Roßnagel*, in: Reichl/Roßnagel/Müller 2005, 4 f., *ders*., DuD 2005, 59 f.

71 Zum Signaturbündnis (aus Sicht der Banken) vgl. *Büger/Esslinger/Koy*, DuD 2004, 133 ff.; s.a. http://www.signaturbuendnis.de.

72 S. näher *Roßnagel/Gitter/Hornung/Strasser*, in: Reichl/Roßnagel/Müller 2005, 319 ff.

73 S. ausführlich unten 5.2.2.

- Anders als bei einer Einführung über die Banken- oder Gesundheitskarte besteht beim digitalen Personalausweis nicht die Gefahr einer Einstellung des Projekts durch den Betreiber unter betriebswirtschaftlichen Gesichtspunkten.
- Schließlich sind beim Wechsel des Kreditinstituts oder der Krankenkasse die entsprechenden Karten zurückzugeben. Mit der Karte des neuen Vertragspartners müsste jedes Mal ein neuer Signaturschlüssel generiert und ein neues Zertifikat ausgestellt werden. Damit sind unnötige Kosten verbunden. Werden diese auf den Bürger abgewälzt, könnten sie ihn von einem Wechsel der Bank oder Versicherung abhalten. Daraus könnten sich wettbewerbsrechtliche Probleme ergeben.

Die Signaturfunktion ließe sich (wie bei den bisher angebotenen Signaturkarten) problemlos um Verschlüsselungs- und Authentisierungsverfahren ergänzen. In diesem Fall wäre auch ein Einsatz des Ausweises überall dort denkbar, wo es um den Zugang zu Rechnern und Netzen, die Zeiterfassung und den Zugriffs- und Zutrittsschutz geht. Damit wäre eine weite Verbreitung der Basistechnologien für einen sicheren und rechtsverbindlichen Geschäftsverkehr erreichbar.[74] Die Verbindung aus der Aufnahme biometrischer Daten und der für die elektronische Signatur, Verschlüsselung und Authentisierung benötigten Schlüssel und Zertifikate würde sich zu einer völligen Neukonzeption des Personalausweises zusammenfügen. Nach dem Aktionsprogramm „Informationsgesellschaft Deutschland 2006“ der Bundesregierung sollte im Lauf des Jahres 2004 ein Gesetzgebungsverfahren zu einem so konzipierten digitalen Personalausweis durchgeführt werden.[75] Dies ist zwar nicht erfolgt, die Bundesregierung hält jedoch an dem Vorhaben fest und nennt nunmehr das Jahr 2007 als Starttermin.[76] Die „eCard-Strategie“ der Bundesregierung vom 9. März 2005 sieht vor, den Ausweis so auszugestalten, dass er „auf Wunsch der nutzenden Person auch für qualifizierte Signaturen zu verwenden“ ist.[77]

2.1.2 Die elektronische Gesundheitskarte

Die elektronische Gesundheitskarte ist Teil der Bemühungen zur Schaffung einer umfassenden „Telematikinfrastruktur“[78] im deutschen Gesundheitswesen. Aus rechtlicher Sicht wurden die Weichen im Gesetz zur Modernisierung der Gesetzlichen Krankenversicherung (GKV-Modernisierungsgesetz – GMG) gestellt, das vom Bundestag am 26. September 2003 mit breiter Mehrheit beschlossen wurde.[79] Nach § 291a SGB V (neu) soll die elektronische Gesundheitskarte zum 1. Januar 2006 an alle Mitglieder der gesetzlichen Krankenversicherung ausgegeben werden. Es ist allerdings bereits deutlich, dass zu diesem

74 Vgl. *Roßnagel*, in: Reichl/Roßnagel/Müller 2005, 10 ff.

75 S. *Bundesregierung* 2003, 9; s. zum Inhalt (Trägermedium für die elektronische Signatur und für biometrische Daten) ebd. 6, 72, 83.

76 Vgl. die Antwort auf die Kleinen Anfrage der FDP-Fraktion im Januar 2005, BT-Drs. 15/4616, 4.

77 Vgl. http://www.bundesregierung.de/-,413.799497/artikel/eCard-Strategie-der-Bundesregi.htm.

78 Zum Begriff der Telematik s.o. Fn. 38 (S. 35). Eine Telematikinfrastruktur ist demgegenüber die Gesamtheit aller Hard- und Software, die nötig ist, um in einem Gesamtsystem (z.B. dem Gesundheitswesen) elektronisch zu kommunizieren, s. *Grätzel v. Grätz* 2004c, 114. Bei dem Gesamtvorhaben handelt es sich um eines der anspruchsvollsten IT-Projekte der Welt. Die medizinische Versorgung in Deutschland umfasst pro Jahr etwa 11 Mrd. Transaktionen mit einem Datenaufkommen von mindestens 23,6 Terabyte (ohne Bilddaten), s. http://www.heise.de/newsticker/meldung/48370.

79 BGBl. I, 2190. Basis waren Entwürfe der Koalitionsfraktionen v. 16.6.2003 (BT-Drs. 15/1170) und der Koalition mit der Fraktion der CDU/CSU v. 8.9.2003 (BT-Drs. 15/1525); zur Entwicklung etwa *Sendatzki*, BKK 2002, 207 ff.; kritisch zum Prozess der Gesetzgebungsvorbereitung *Devigne*, ZM 2003, 18 ff.; zur fehlenden Einbindung der Patienten *Pitschas* 2002, 107 ff.; s. bereits *Stark*, DuD 1997, 575 ff.

Zeitpunkt keine allgemeine Verteilung der Karten erfolgt sein wird.[80] Ein Konsortium der Industrie verfasste parallel zum Gesetzgebungsverfahren eine Expertise zur Einführung einer Telematik-Architektur im deutschen Gesundheitswesen.[81] Das Projekt fügt sich in den Plan einer europäischen Krankenversichertenkarte ein. Im Rahmen der Fortschreibung des europäischen Aktionsprogramms eEurope plante die Kommission zu Beginn des Jahres 2003 ein dreistufiges Vorgehen:[82]

- Zum 1. Juni 2004 sollte eine europäische Krankenversichertenkarte eingeführt werden, die den Vordruck E 111 ersetzen und dessen Angaben in sichtbarer Form enthalten sollte.
- Bis Ende des Jahres 2005 soll es zur Ersetzung der weiteren, bei einem Aufenthalt in einem Mitgliedstaat verwendeten Vordrucke kommen.
- Im dritten Schritt ist Ende des Jahres 2008 die Speicherung aller Vordrucke auf einem elektronischen Träger geplant.

Anfang Juni des Jahres 2004 wurde der Start des Projekts in zwölf Mitgliedstaaten offiziell bekannt gegeben.[83] Allerdings waren die Karten ab diesem Zeitpunkt nicht durchweg verfügbar. Auch wenn der Zeitplan damit bereits in seiner ersten Stufe nicht vollständig eingehalten wurde, orientieren sich die deutschen Vorhaben an dem durch die Europäische Union geplanten Ablauf. Dementsprechend wird die elektronische Gesundheitskarte im ersten Schritt auf der Rückseite die europäischen Berechtigungsscheine als Sichtausweis abbilden und darüber hinaus die aktuelle Krankenversichertenkarte ersetzen. Diese wird seit dem Jahre 1995 flächendeckend eingesetzt[84] und ermöglicht seitdem bei den gesetzlich Versicherten die automatisierte Übertragung der Versicherungsstammdaten in das Datenverarbeitungssystem des Arztes. Dieser Vorgang war bis dahin manuell mittels eines Krankenscheins vonstatten gegangen.[85] Bei der Krankenversichertenkarte handelt sich um einen einfachen Speicherchip ohne Prozessor. Schutzmechanismen wie eine PIN werden nicht verwendet und es existiert kein Schreibschutz.[86] Im Unterschied hierzu soll der neue Prozessorchip eine Vielzahl von Funktionen ermöglichen: neben der Ablage der Stammdaten auch das elektronische Rezept, die Speicherung von Notfalldaten, den elektronischen Arztbrief, die elektronische Patientenakte, den Medikamentenpass, selbst zur Verfügung gestellte Daten und die so genannte „Patientenquittung“.[87] Die elektronische Gesundheits-

---

80 Bundesgesundheitsministerin *Schmidt* ging im Januar 2005 davon aus, dass im Laufe des Jahres 2006 zunächst lediglich ca. 100.000 Versicherte die Karte erhalten werden, s. *Rabbata*, DÄ 2005, A 96.

81 *BITKOM/VDAP/VHitG/ZVEI* 2003. Ein früheres Gutachten wurde von *Berger & Partner* (1997) erstellt; s. zu dieser Studie auch *Grätzel v. Grätz* 2004c, 121 f.

82 Vgl. *Europäische Kommission*, KOM(2003) 73; *Dierks/Nitz/Grau* 2003, 116 f.; *Bales/Holland* 2004, 15 f. und unten 3.1.2.

83 Vgl. http://europa.eu.int/idabc/document/2589/194.

84 Ursprünglich sollte sie nach dem 1988 verabschiedeten § 291 SGB V bis zum 1.1.1992 verfügbar sein. Dieser Termin wurde von Krankenkassen allerdings nicht eingehalten, s. *Kilian*, NJW 1992, 2313, 2314; *Fuest* 1999, 4 f.; zur Entwicklung der Krankenversichertenkarte vgl. *Fuest* 1999, 2 ff.; *Berger & Partner* 1997, 40 f.; *Kraft* 2003, 5 f. m.w.N.; s.a. *Wellbrock*, DuD 1994, 70; *Schaefer*, DuD 1993, 685 ff.; *Betrand/Kuhlmann/Stark* 1995, 133 ff.; *Der Bundesbeauftragte für den Datenschutz* 1993, unter 12.1.

85 Näher LPK-SGB V-*Roß*, § 291 Rn. 1 ff. Das System war weltweit die erste flächendeckende Chipkartenanwendung im Gesundheitswesen, s. *Fuest* 1999, 6.

86 Zu den technischen Einzelheiten *Fox*, DuD 1997, 600. Danach sind Manipulationen technisch und finanziell ohne besonderen Aufwand möglich. Unzutreffend ist deshalb, aus der Funktionsweise der üblicherweise verwendeten Software von Praxen und Krankenkassen zu folgern, nur die entsprechenden Stellen könnten auf die Karte zugreifen (so aber *Rankl/Effing* 2002, 823).

87 S. *Hornung* 2004a, 226 ff.; *Hornung/Goetz/Goldschmidt*, WI 2005, 171 ff.; ausführlich unten 2.2.2.2.

karte wird ein Bindeglied im deutschen Gesundheitswesen sein, das über 80 Millionen Versicherte (einschließlich privat Versicherte), 270.000 Ärzte, 77.000 Zahnärzte, 2.000 Krankenhäuser, 22.000 Apotheken und über 300 Krankenkassen umfasst.[88]

Die Potentiale der Verwendung von Informationstechnologie im Gesundheitswesen wurden bereits früh erkannt.[89] Die Motive für den Einsatz waren von Beginn an die Verbesserung der Versorgung, die Verstärkung des Informationsflusses, die Kosteneinsparung durch Rationalisierungen, die Verbesserung der Forschung und der Einfluss hin zu einer gesunden Lebensweise.[90] Diese Gründe spielen auch bei der elektronischen Gesundheitskarte eine tragende Rolle: Diese soll gemäß § 291a Abs. 1 SGB V der „Verbesserung von Wirtschaftlichkeit, Qualität und Transparenz der Behandlung" dienen.

Auf Seiten des Staates und der Krankenkassen sind die Pläne zweifach motiviert. Vor dem Hintergrund des Skandals um das Arzneimittel Lipobay[91] wird einerseits eine Verbesserung der Versorgung insbesondere im Bereich der Arzneimittelverschreibung angestrebt. Andererseits erhofft man sich mittelfristig Einsparungen im Gesundheitssystem von bis zu 1 Milliarde Euro pro Jahr.[92] Die Anlaufinvestitionen – im Gespräch sind 1,2 bis 1,5 Milliarden Euro[93] – sollen sich bereits innerhalb von ein bis zwei Jahren amortisieren. Der Zeitraum wäre damit vergleichbar mit dem bei der Einführung der Krankenversichertenkarte.[94] Ermöglicht werden diese Einsparungen durch eine straffere Verwaltung, eine stärkere Verzahnung der Beteiligten, eine dezentrale Verfügbarkeit von Expertenwissen und eine Konzentration auf die eigentlichen Aufgaben der Krankenkassen und Leistungserbringer.[95] Die Zahl der Mehrfachuntersuchungen soll abgebaut und Leistungsmissbrauch eingedämmt werden. Außerdem werden eine standardisierte Dokumentation und eine erleichterte Archivierung angestrebt. Darüber hinaus sollen anonymisierte Strukturdaten

88 Diese Zahlen sind im Einzelnen umstritten (die Angabe erfolgt nach *Schröder*, Gesundheits- und Sozialpolitik, Ausgabe 15-16/2004; *Bales/Holland* 2004, 18; *Grätzel v. Grätz* 2004c, 115), geben aber zumindest die Größenordnung an.

89 Zu den ersten Beispielen für die Verwendung von EDV im Gesundheitswesen vgl. *Beier* 1979, 9 ff., aus datenschutzrechtlicher Sicht insbes. *Steinmüller/Ermer/Schimmel* 1978; eine Übersicht für Chipkartenprojekte in Deutschland bis 1998 findet sich bei *Iwansky* 1999, 40 ff.; s.a. *Stark/Wohlmacher*, DuD 1997, 595; *Elkeles/Rosenbrock* 1995, 7 ff.; *Rienhoff*, ZaeFQ 2001, 642 ff.

90 So schon *Schaefer* 1979, 21; s.a. *Lilie* 1980, 26 f.; *Roßnagel/Wedde/Hammer/Pordesch* 1990, 182.

91 Das Medikament Lipobay (ein Cholesterinsenker) der *Bayer AG* geriet im Sommer 2001 wegen massiver Nebenwirkungen in die Schlagzeilen und wurde vom Anbieter am 8.8.2001 vom Markt genommen. Die elektronische Arzneimitteldokumentation als Teil der elektronischen Gesundheitskarte ist eine der politischen Reaktionen auf den Vorfall, s. *Grätzel v. Grätz* 2004c, 120 f. Es gibt in Deutschland bislang keine belastbaren Erkenntnisse über arzneimittelbedingte Komplikationen, vgl. *Grätzel v. Grätz* 2004b m.w.N. Genannt wird regelmäßig eine Größenordnung von ca. 10.000 Todesfällen durch Neben- und Wechselwirkungen, s. *Bales/Holland* 2004, 14; nach anderen Angaben sollen es bis zu 58.000 Fälle sein, s. *Grätzel v. Grätz* 2004c, 163.

92 So die Begründung des Gesetzesentwurfs, BT-Drs. 15/1525, 173; s. näher unten 6.3.5.

93 Vgl. *Goldschmidt/Goetz/Hornung*, mdi 2/2004, 61, 67 f.

94 S. *Berger & Partner* 1997, 40; *Bizer* 2002, 36; zum Motiv der Kostenersparnis vgl. auch *Dierks/Nitz/Grau* 2003, 16 m.w.N.; zur Gemengelage der Motive Rationalisierungsdruck und Qualitätsverbesserung s. schon *Hammer/Roßnagel* 1989, 121 ff.; *BSI* 1995, 11 f.; *Iwansky* 1999, 51 ff. Die gesetzlichen Krankenkassen sind nach § 12 SGB V auf Wirtschaftlichkeit verpflichtet.

95 *BITKOM/VDAP/VHitG/ZVEI* 2003, 5, 14 ff.; zur Motivation s.a. *Dietzel*, Bundesgesundheitsbl. 2003, 267 ff.; *ders*., DÄ 2002, A 1417 ff.; *Dierks/Nitz/Grau* 2003, 17 ff. m.w.N.; *Kartte* 2004, 212 f.; *Weichert*, DuD 2004, 391; *Wellbrock*, DuD 1994, 70, 71; *Elkeles/Rosenbrock* 1995, 6 ff.; *Kruse/Peuckert*, DuD 1995, 142, 149; *Fuest* 1999, 83 ff.; BSI 1995, 34 ff.; allgemeiner für die Telematik *Hermeler* 2000, 12 ff.; *Goetz* 2001, 21 f. m.w.N.; *Laskaridis* 2003, 144 ff.; *Warda/Noelle* 2002, 23 ff.; *Orlowski*, MedR 2004, 202 ff.

gewonnen werden.[96] Schließlich erhofft man sich eine Stärkung der Eigenverantwortung und Mitwirkungsbereitschaft der Patienten.[97] All dies soll zu mehr Effizienz im deutschen Gesundheitswesen führen, das nach Meinung von Experten insbesondere im Verhältnis von Kosten und Nutzen international schlecht abschneidet.[98]

Auch für die Versicherten sollen sich Vorteile ergeben. Die elektronische Gesundheitskarte eröffnet die Aussicht auf eine verbesserte Versorgung durch eine höhere Verfügbarkeit von Daten für den behandelnden Arzt (etwa zum Erkennen von Kontraindikationen), eine verbesserte Arzneimittelsicherheit und eine geringere Eingriffsintensität, wenn zum Beispiel auf erneute Untersuchungen verzichtet werden kann[99] oder erkannt wird, dass eine bestimmte Behandlung (beispielsweise eine Tetanus-Impfung)[100] überflüssig ist. Mit der Gesundheitskarte könnte auch dem Problem des Vergessens der eigenen Krankengeschichte abgeholfen werden. Denkbar ist daneben ein Einsatz zur Prävention.[101] Die Bekämpfung von Missbrauch führt außerdem zu mehr Beitragsgerechtigkeit.

Die Ablage der europäischen Berechtigungsnachweise auf der Gesundheitskarte entbindet den Versicherten davon, vor jedem vorübergehenden Aufenthalt in einem anderen Mitgliedstaat bei seinem Versicherungsträger einen neuen Vordruck zu besorgen.[102] Die Karte könnte daneben neue Möglichkeiten für eine selbstbestimmte Datenhoheit und Patientenautonomie bieten. Eine Speicherung auf oder mittels einer Chipkarte könnte dem Versicherten – je nach der technischen Ausgestaltung der Zugriffsbefugnisse – die Möglichkeit geben, über die Verwendung seiner Daten selbstbestimmt zu entscheiden und in größerem Maße als bisher Auskunft über Behandlungen und Abrechnungen zu erhalten.[103]

Der Nutzen für die Leistungserbringer liegt vor allem in der Erhöhung des Behandlungsniveaus.[104] Untersuchungsergebnisse und sonstige Daten könnten schneller, einfacher und vollständiger verfügbar sein. Außerdem ergeben sich weitere Möglichkeiten im Bereich (tele-)konsiliarischer Leistungen und der Zusammenarbeit mit den Krankenhäusern. Die Verminderung des administrativen Aufwands spart Kosten. Apotheker könnten mehr als bisher beratend tätig werden. Schließlich erleichtert und beschleunigt die Ersetzung der europäischen Vordrucke die Behandlung und Abrechnung, weil anstelle von schlecht lesbar ausgefüllten Papiervordrucken ein standardisierter Sichtausweis eingeführt wird.[105]

Die zuständigen Stellen arbeiteten von Anfang an mit Nachdruck an der Erarbeitung und Umsetzung eines Konzepts für die elektronische Gesundheitskarte. Dennoch wird

---

96 Zum Aspekt der Gesundheitssystemforschung s. *Dierks/Nitz/Grau* 2003, 20 f. m.w.N.; *Warda/Noelle* 2002, 180 ff.; vgl. schon *Wellbrock*, DuD 1994, 70, 71.

97 In diese Richtung gehen auch parallele Bemühungen zur Einrichtung effektiver Patienteninformationssysteme, s. *ATG/GVG* 2004b, insbes. die Evaluierungsmöglichkeiten auf S. 11 ff.

98 S. ausführlich *Sachverständigenrate für die konzertierte Aktion im Gesundheitswesen* 2003; diese Ansicht ist allerdings nicht unwidersprochen, s. *Richter-Kuhlmann*, DÄ 2004, A 1215 und ausführlich *Beske/Drabinski/Zöllner* 2004; zur EDV-Situation im Deutschen Gesundheitswesen zum Zeitpunkt des Jahres 2002 vgl. *Warda/Noelle* 2002, 36 ff.

99 *BITKOM/VDAP/VHitG/ZVEI* 2003, 5; *Kartte* 2004, 213; *Dierks/Nitz/Grau* 2003, 94 f.; *Berger & Partner* 1997, 27, 69 f.; *Wellbrock*, DuD 1994, 70, 71; *Fuest* 1999, 84, 87 m.w.N.

100 Derzeit werden eine Vielzahl dieser Impfungen nach Unfällen allein deshalb durchgeführt, weil im Rahmen der Notfallbehandlung der Impfausweis nicht verfügbar ist, s. *Warda/Noelle* 2002, 107.

101 *BSI* 1995, 36; zur Verwendung von Chipkarten zur Prävention und Gesundheitsförderung s. *Elkeles/Rosenbrock* 1995, insbes. 15 ff. und die kritische Einschätzung auf S. 43 ff.

102 *Europäischen Kommission*, KOM(2003) 73, 10.

103 *BITKOM/VDAP/VHitG/ZVEI* 2003, 15; *Warda/Noelle* 2002, 24 f.; *Wellbrock*, DuD 1994, 70, 72 f.; *BSI* 1995, XI, 35 f.

104 S. zum Folgenden *BITKOM/VDAP/VHitG/ZVEI* 2003, 15 ff.; *Berger & Partner* 1997, 27, 70 ff.

105 *Europäische Kommission*, KOM(2003) 73, 12.

diese im Jahre 2006 zunächst lediglich in Testregionen verfügbar sein.[106] Mitte des Jahres 2003 wurde ein Auftrag für die Entwicklung einer Rahmenarchitektur und Sicherheitsinfrastruktur an das Industrie-Konsortium „biT4health“ vergeben.[107] Die Ergebnisse wurden der Ministerin *Schmidt* auf der CeBIT 2004 übergeben.[108] Modellprojekte laufen beispielsweise in Schleswig-Holstein,[109] Bochum und Essen,[110] Sachsen[111] und Bremen.[112] Das Ministerium möchte im Juli des Jahres 2005 offizielle Testregionen auswählen.[113]

Ein Konsortium aus mehreren Fraunhofer-Instituten und der TU Wien erarbeitete im Frühjahr des Jahres 2005 auf der Basis der Ergebnisse des biT4health-Projekts eine Lösungsarchitektur, die zur CeBIT 2005 fertiggestellt wurde[114] aber offenbar noch unvollständig ist.[115]

Am 11. Januar 2005 unterzeichneten insgesamt 15 Verbände der Ärzteschaft, der Krankenkassen und der Apotheker einen Gesellschaftervertrag zur Gründung einer neuen Betriebsorganisation. An der „gematik Gesellschaft für Telematikanwendungen der Gesundheitskarte GmbH“ beteiligen sich unter anderem die Bundesärztekammer, die Kassenärztliche Bundesvereinigung, die Deutsche Krankenhausgesellschaft und der Deutsche Apothekerverband.[116] Die Gesellschaft soll für die Einführung der Gesundheitskarte und des elektronischen Rezeptes sowie für die Entwicklung der elektronischen Patientenakte zuständig sein. Anders als bei ihrem Vorgänger, dem Koordinationsbüro „protego.net“, können Entscheidungen mit 2/3-Stimmenmehrheit gefällt werden. Die Hoffnung ist, dass diese Abkehr vom Einstimmigkeitsprinzip die Handlungsfähigkeit der Gesellschaft erhöhen wird. Am 15. April 2005 verabschiedete der Bundestag die rechtlichen Grundlagen für die gematik GmbH und ihre Kompetenzen,[117] die sich nunmehr in § 291b SGB V finden.

In das System der elektronischen Gesundheitskarte wird auch der so genannte elektronische Heilberufsausweis integriert werden, der in den meisten Fällen zum Zugriff auf die Daten erforderlich ist. Dieser wird über die Möglichkeit verfügen, qualifizierte elektroni-

---

106 BITKOM und BDI verlangten bereits Ende 2003 zusätzliche Anstrengungen, um die Umsetzung zum 1.1. 2006 tatsächlich bewerkstelligen zu können, s. http://www.heise.de/newsticker/meldung/42117; s.a. die Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten *Sehling*, *Storm*, *Widmann-Mauz*, weiterer Abgeordneter und der Fraktion der CDU/CSU v. 30.3.2004 (BT-Drs 15/2810). Die Verantwortlichen der BÄK rechneten im Frühjahr 2005 mit einem Projektstart frühestens im Jahre 2007, s. http://www.heise.de/newsticker/meldung/57024.

107 S. den Bericht in DuD 2003, 654 f.; vgl. zum Projekt bit4Health auch *Grätzel v. Grätz* 2004c, 116 ff.

108 Vgl. http://www.heise.de/newsticker/meldung/45879.

109 Näher *ULD* 2003a, 47 f.; *dass*. 2005, 55 ff.; http://landesregierung.schleswig-holstein.de/coremedia/generator/Aktueller_20Bestand/MSGV/Information/Gesundheit/Gesundheitskarte.html. Das Projekt in Schleswig-Holstein ist bundesweit am weitesten fortgeschritten.

110 http://www.heise.de/newsticker/meldung/43635; OMNICARD-Newsletter Januar 2004/2.

111 S. den Bericht in DuD 2004, 376 f.

112 S. OMNICARD-newsletter März 2004; zu frühen Feldversuchen mit sektoriellen Karten vgl. *BSI* 1995, 21 f. Die Durchführung der Projekte für die Telematik-Infrastruktur stützt sich auf § 63 Abs. 3a SGB V; s.a. *Schneider* 2004, 141.

113 Vgl. http://www.heise.de/newsticker/meldung/59473.

114 S. http://www.heise.de/newsticker/meldung/57490; die Ergebnisse sind unter http://www.dimdi.de/static/de/ehealth/karte/technik/loesungsarchitektur/ergebnisse/index.htm abrufbar. Zu den jeweils neuesten Entwicklungen s. http://www.dimdi.de.

115 S. http://www.heise.de/newsticker/meldung/58820; http://www.aerztezeitung.de/docs/2005/04/12/065a0103.asp?cat=/politik/gesundheitssystem_uns; http://www.aerztezeitung.de/docs/2005/04/18/069a0401.asp?cat=/politik/gesundheitssystem_uns; s.a. das Interview mit dem KBV-Vorsitzenden *Köhler*, http://www.aerztezeitung.de/docs/2005/04/12/065a0601.asp?cat=/politik/gesundheitssystem_uns.

116 Vgl. *Rabatta*, DÄ 2005, A 96; s.a. *Hornung/Goetz/Goldschmidt*, WI 2005, 171, 175, 178.

117 Gesetz zur Organisationsstruktur der Telematik im Gesundheitswesen, noch nicht im BGBl. veröffentlicht; s. BT-Drs. 15/4924 und 15/5272.

sche Signaturen zu erzeugen.[118] Die Gesundheitskarte benötigt demgegenüber diese Fähigkeit für die Anwendungen im Gesundheitswesen nicht.[119] Dennoch ist schon länger geplant, sie als sichere Signaturerstellungseinheit auszugestalten.[120] Das wurde im März des Jahres 2005 in der „eCard-Strategie" der Bundesregierung erneut bekräftigte.[121] Damit ergibt sich auch hier ein weit verbreitetes potentielles Trägermedium für qualifizierte Signaturverfahren.

2.1.3 Das JobCard-Verfahren

Im Jahre 2002 entwickelte die Kommission zum Abbau der Arbeitslosigkeit und zur Umstrukturierung der Bundesanstalt für Arbeit („Hartz-Kommission") die Idee des so genannten JobCard-Verfahrens.[122] Die Bezeichnung des Projekts als „JobCard" ist allerdings irreführend: Es handelt sich nicht um ein Karten-, sondern um ein Anwendungsprojekt.[123] Die Hartz-Kommission schlug vor, ein neues System für den Abruf von Arbeits- und Verdienstbescheinigungen zu entwickeln. Diese sollten nicht mehr – wie bislang – durch den Arbeitgeber ausgegeben, sondern zentral so gespeichert werden, dass ein Zugriff im Leistungsfall unmittelbar möglich ist, jedoch nur durch den kombinierten Einsatz der Signaturkarte des „Job-Centers" (heute Arbeitsagentur) und der Signaturkarte des Arbeitnehmers erfolgen kann.[124] Angesichts von ca. 60 Millionen Bescheinigungen in Papierform, die zurzeit von 2,8 Millionen Arbeitgebern jährlich ausgestellt werden[125] erwartete die Kommission von der medienbruchfreien Verarbeitung vor allem zwei Vorteile:

- Zum einen könnten sich erhebliche Einsparungen bei den Arbeitsagenturen und den Arbeitgebern ergeben. Diese Tätigkeit soll ca. 5 % der Personalverwaltungskosten verursachen.
- Zum anderen würde die Leistungsauszahlung im Versicherungsfall beschleunigt.

Die Bundesregierung hat den Vorschlag im Aktionsprogramm „Informationsgesellschaft Deutschland 2006" aufgenommen.[126] Sie verspricht sich von der Einführung des JobCard-Verfahrens nicht nur die genannten Effizienzeffekte, sondern auch eine breite Einführung von Chipkarten, die zur Erstellung qualifizierter elektronischer Signaturen in der Lage sind.[127] Mit dieser Initiative wird ein anderer Weg beschritten als mit der Einführung allgemeiner signaturfähiger Ausweise (beispielsweise des digitalen Personalausweises oder der elektronischen Gesundheitskarte). Statt die Verbreitung von Signaturkarten zu fördern, wird eine zwangsweise Massenanwendung geplant, die jeden Antragsteller in der gesetzlichen Arbeitslosenversicherung verpflichten würde, eine – allerdings beliebige – Signaturkarte zu besitzen. In einem zweiten Schritt könnten alle sozialversicherungspflichtigen Personen, insgesamt etwa 35 Millionen Menschen in Deutschland, betroffen sein.

---

118 Näher unten 5.2.2, 5.2.3.
119 Erforderlich ist nach § 291 Abs. 2a Satz 3 SGB V zwar die Eignung zur Erstellung elektronischer, nicht aber *qualifizierter* elektronischer Signaturen; s. zu den Unterschieden unten 5.1.1.
120 *Bundesregierung* 2003, 6, 86 ff.; s.a. *BITKOM/VDAP/VHitG/ZVEI* 2003, 46; *Krüger-Brand*, DÄ 2002, A 3304.
121 Vgl. http://www.bundesregierung.de/-,413.799497/artikel/eCard-Strategie-der-Bundesregi.htm.
122 *Kommission zum Abbau der Arbeitslosigkeit und zur Umstrukturierung der Bundesanstalt für Arbeit* 2002, 123 ff., 130 ff.
123 *Hornung/Roßnagel*, K&R 2004, 263, 265.
124 S. zum Ablauf näher unten 4.2.4.1.
125 S. *Leistenschneider*, DuD 2004, 175; *Ernestus*, DuD 2004, 404.
126 *Bundesregierung* 2003, 9, 72 f.
127 S. *Hornung/Roßnagel*, K&R 2004, 263 f.

Die Menge von 35 Millionen Nutzern würde weit jenseits der kritischen Masse liegen, die es Anbietern ermöglicht, mit einer hinreichenden Gewinnerwartung neue Anwendungen zu entwickeln. Entsprechend der Attraktivität dieser Anwendungen könnten die Nutzer die – dann ohnehin vorhandene – Signaturkarte vielfältig nutzen. Werden Signaturverfahren von vielen genutzt, werden sie auch für diejenigen interessant, die nicht durch das JobCard-Verfahren zum Besitz einer Signaturkarte verpflichtet sind. Dieses Verfahren könnte also den entscheidenden Anstoß geben, um aus dem bisherigen Dilemma der Signatureinführung heraus zu kommen.[128]

Ein Gesetzentwurf zum JobCard-Verfahren wird derzeit vorbereitet. Das Projekt ist auch Teil der „eCard-Strategie" der Bundesregierung.[129] In einem Versuch wurde das Konzept seit dem Herbst des Jahres 2002 zunächst in Bezug auf die zentrale Speicherung von Arbeitsbescheinigungen und danach ab dem 1. September 2003 mit mehreren Arbeitsämtern im Modellbetrieb getestet.[130] Die flächendeckende Speicherung aller Bescheinigungen könnte ab dem Jahre 2007 erfolgen.[131] Da für die Berechnung des Leistungsanspruchs zumindest die Daten der letzten zwölf Monate in der Zentralen Speicherstelle vorliegen müssen, kann der Abruf durch die Arbeitsagenturen frühestens ein Jahr später beginnen.

2.2 Rechtliche Grundlagen

Im Personalausweis- und Sozialrecht existieren – anders als für das JobCard-Verfahren – bereits Normen für den digitalen Personalausweis und die elektronische Gesundheitskarte. Diese sind nur vor dem Hintergrund der allgemeinen Regeln über die Datenverarbeitung im Personalausweis- und Gesundheitswesen verständlich.

2.2.1 Personalausweisrecht

Das gegenwärtige Personalausweisgesetz enthält die Rechtsgrundlagen für den bisherigen Personalausweis. Durch das Terrorismusbekämpfungsgesetz wurden aber auch bereits Regelungen für den künftigen digitalen Personalausweis eingefügt.

2.2.1.1 Entwicklung und gegenwärtiger Inhalt der Personalausweispflicht

Eine allgemeine Personalausweispflicht besteht in Deutschland erst seit der Zeit des Nationalsozialismus. Ziel der Einführung war einerseits die effektive Registrierung und Kontrolle der Bevölkerung im Rahmen der Kriegsvorbereitungen, andererseits die Erfassung und Aussonderung der jüdischen Mitbürger.[132] § 2 des Gesetzes über das Pass-, das Ausländerpolizei- und das Meldewesen sowie über das Ausweiswesen vom 11. Mai 1937[133] ermächtigte den Reichsminister des Innern, die erforderlichen Maßnahmen zur Vereinheit-

128 Vgl. hierzu *Hornung/Roßnagel*, K&R 2004, 263, 265 f.

129 Vgl. http://www.bundesregierung.de/-,413.799497/artikel/eCard-Strategie-der-Bundesregi.htm.

130 In Helmstedt, Bamberg und Offenbach, s. *Bundesregierung* 2003, 72 f.; *Ernestus*, DuD 2004, 404, 405. Zuvor wurde eine Abstimmung mit dem Bundesbeauftragten für den Datenschutz durchgeführt; s.a. *Leistenschneider*, DuD 2004, 175; *Schulzki-Haddouti*, c't 13/2004, 46 f.; *Der Bundesbeauftragte für den Datenschutz* 2005, 153 ff.

131 In diese Richtung gehen Äußerungen der Bundesagentur für Arbeit vom Januar 2005, s. http://www.heise.de/newsticker/meldung/55064.

132 Zum Missbrauch von Ausweisen und staatlichen Registern durch die Nationalsozialisten in Deutschland vgl. *Torpey* 2000, 131 ff.; *Sobel*, B.U. J. Sci. & Tech. L. 2002, 37, 48 ff. m.w.N.; *ders*., Harv. J. Law & Tec 2002, 319, 343 ff.

133 RGBl I, 589; s. näher *Medert/Süßmuth* 1998, Einf. Rn. 1.

lichung und Vereinfachung des Ausweiswesens zu treffen, insbesondere entsprechende Muster zu bestimmen. Auf dieser Grundlage wurde am 22. Juli 1938 die Verordnung über Kennkarten erlassen.[134] Diese wurden als allgemeine polizeiliche Inlandsausweise eingeführt, die gemäß § 3 Abs. 2 a) und b) der Verordnung das Lichtbild und den Fingerabdruck der Inhaber enthielten. Nach § 1 Abs. 2 der Verordnung konnten alle deutschen Staatsangehörigen ab dem vollendeten 15. Lebensjahr die Kennkarte erhalten, es bestand also noch keine allgemeine Ausweispflicht. Diese wurde kurz nach Ausbruch des Zweiten Weltkrieges durch § 2 Abs. 1 der Verordnung über den Pass- und Sichtvermerkszwang sowie über den Ausweiszwang vom 10. September 1939 begründet.[135] Danach mussten alle deutschen Staatsangehörigen sich auf amtliches Erfordern „jederzeit" ausweisen. Der Ausweis war also ständig bei sich zu führen.

Nach einer Übergangszeit, in der das Ausweiswesen durch Anordnungen der Militärregierungen der einzelnen Besatzungsgebiete bestimmt wurde, trat am 1. Januar 1951 das neue Personalausweisgesetz in Kraft.[136] Bis zur Einführung des heutigen maschinenlesbaren Personalausweises im Jahre 1987[137] blieb das Gesetz nahezu unverändert.

Gegenwärtig besteht gemäß § 1 Abs. 1 Satz 1 PersAuswG für alle Deutschen im Sinne des Art. 116 Abs. 1 GG, die der allgemeinen Meldepflicht nach den Landesmeldegesetzen unterliegen, mit der Vollendung des 16. Lebensjahres eine Personalausweispflicht.[138] Die Ausführungsgesetze der Länder[139] gestalten diese näher aus und beinhalten (bei Unterschieden im Einzelnen) Ausnahmen für betreute und solche Personen, die sich nicht nur kurz in Krankenhäusern, Pflegeheimen oder ähnlichen Anstalten sowie in einer Einrichtung aufhalten, die dem Vollzug einer richterlichen Entscheidung über eine Freiheitsentziehung dient.[140] Einige Ausführungsgesetze gestatten, dass auch nicht ausweispflichtige Personen auf Antrag einen Personalausweis erhalten können.[141]

Die Personalausweispflicht gebietet, einen Personalausweis zu besitzen und ihn auf Verlangen einer zur Prüfung der Personalien ermächtigten Behörde vorzulegen. Demgegenüber gibt es keine Pflicht, das Papier ständig bei sich zu führen.[142] Der Personalausweispflicht kann auch durch den Besitz eines gültigen Passes (§ 1 Abs. 1 Satz 1, 2. Halbsatz PersAuswG) und eines vorläufigen Personalausweises (§ 1 Abs. 1 Satz 2 PersAuswG) genügt werden.

Für die Personalausweisbehörden bestimmt § 2b Abs. 1 PersAuswG eine grundsätzliche Verwendungssperre für personenbezogene Daten, die nur auf der Basis von Gesetzen (insbesondere des Personalausweisgesetzes selbst) oder Rechtsverordnungen erhoben, verarbeitet und genutzt werden dürfen. Dies stellt insofern eine Einschränkung des allge-

---

134 RGBl. I, 913.
135 RGBl. I, 1739.
136 PersAuswG v. 21.12.1950, BGBl. S. 807.
137 S. eingehend unten 7.3.2.2.
138 Der Ausweispflicht korrespondiert ein durchsetzbarer Rechtsanspruch auf Ausstellung eines Ausweises, s. BVerwG, Urteil v. 29.9.1992 – Buchholz 402.02 Nr. 5.
139 Abgedruckt (Stand 1998) bei *Medert/Süßmuth* 1998, 25 ff.; s.a. die Übersicht ebd., Einf. Rn. 33.
140 *Medert/Süßmuth* 1998, § 1 Rn. 11; s. z.B. § 1 Abs. 2 LPersAuswG Rh.-Pf.; § 1 Abs. 2 und 3 LPersAuswG Bln.; § 1 Abs. 2 und 3 LPersAuswG Bbg.
141 Etwa Kinder vor Vollendung des 16. Lebensjahres, s. *Medert/Süßmuth* 1998, § 1 Rn. 15.
142 § 111 OWiG ahndet nur falsche Angaben zur Identität und das Unterlassen der Angabe gegenüber zuständigen Behörde, Amtsträgern und Soldaten, nicht hingegen das Unterlassen des Mitführens von Ausweisen, s. *Gusy* 2003, Rn. 231. Tlw. bestimmen die Ausführungsgesetze zum PersAuswG ausdrücklich, dass keine Pflicht zum ständigen Beisichführen besteht, so § 1 Abs. 6 Satz 2 LPAuswG Bbg. Allerdings muss die Vorlage bei einer Behörde in angemessener Frist erfolgen, s. *Medert/Süßmuth* 1998, § 1 Rn. 17.

meinen Grundsatzes des § 4 Abs. 1 BDSG dar, als damit eine Datenverwendung auf Basis einer Einwilligung (beispielsweise zusätzliche Daten im Ausweis[143] oder Verwendung über die im Gesetz normierten Verwendungszwecke hinaus) unzulässig ist.

2.2.1.2 Die Ausgestaltung des Personalausweises

Nach § 1 Abs. 2 PersAuswG enthält der Personalausweis neben dem Lichtbild und der Unterschrift ausschließlich folgende Angaben: Familienname und gegebenenfalls Geburtsname, Vornamen, Doktorgrad, Ordensname/Künstlername, Tag und Ort der Geburt, Größe, Farbe der Augen, gegenwärtige Anschrift und Staatsangehörigkeit. Der durch das Gesetz zur Bekämpfung des internationalen Terrorismus vom 11. Januar 2002[144] neu aufgenommene § 1 Abs. 4 Satz 1 PersAuswG regelt, dass der Personalausweis künftig „neben dem Lichtbild und der Unterschrift auch weitere biometrische Merkmale von Fingern oder Händen oder Gesicht des Personalausweisinhabers enthalten [darf]".[145] Damit sollen die computergestützte Identifizierung des Ausweisinhabers ermöglicht und die maschinelle Echtheitsprüfung des Ausweises verbessert werden.[146] § 1 Abs. 4 Satz 2 PersAuswG ordnet an, dass das Lichtbild, die Unterschrift und die weiteren biometrischen Daten auch in mit Sicherheitsverfahren verschlüsselter Form im Personalausweis eingebracht werden dürfen.[147] Dies gilt nach § 1 Abs. 4 Satz 3 PersAuswG auch für die übrigen im Ausweis enthaltenen Angaben zur Person.

Bis zur Neufassung des Gesetzes verbot dagegen § 3 Abs. 1 Satz 1 PersAuswG a.F. ausdrücklich die Speicherung von Fingerabdrücken im Personalausweis.[148] Überdies war die Aufnahme verschlüsselter Merkmale untersagt, um zu verdeutlichen, „dass der Personalausweis keinerlei Informationen enthalten darf, die nicht für jeden Inhaber lesbar und verständlich sind".[149] Die neue Regelung ist unter Transparenzgesichtspunkten problematisch, weil sie eben dies zulässt.[150]

Die Bestimmungen zu möglicherweise neu aufzunehmenden biometrischen Merkmalen sind nach dem ausdrücklichen Gesetzeswortlaut noch nicht abschließend: § 1 Abs. 5 Satz 1 PersAuswG bestimmt, dass „die Arten der biometrischen Merkmale, ihre Einzelheiten und die Einbringung von Merkmalen und Angaben in verschlüsselter Form nach Absatz 4 sowie die Art ihrer Speicherung, ihrer sonstigen Verarbeitung und ihrer Nutzung...durch Bundesgesetz geregelt" werden.

Jeder Personalausweis erhält eine Seriennummer, die sich aus der Behördenkennzahl der Personalausweisbehörde und einer fortlaufend zu vergebenden Ausweisnummer zusammensetzt. Seriennummern und Prüfziffern, die Daten über die Person des Ausweisinhabers oder Hinweise auf solche Daten enthalten, sind nach § 3 Abs. 1 PersAuswG unzulässig, um eine Verwendung als Personenkennziffer zu verhindern.[151] Aus demselben Grund ist die Seriennummer nicht inhaber- sondern ausweisbezogen. Bei der Ausstellung eines neuen Personalausweises wird also eine neue Seriennummer vergeben und nicht etwa die alte weiterverwendet. Eine zentrale, alle Seriennummern umfassende Speicherung lässt

143 Dies ist auch auf freiwilliger Basis nicht möglich, s. *Medert/Süßmuth* 1998, § 1 Rn. 21.
144 BGBl. I 2002, 361.
145 Zur Unbestimmtheit dieser Regelung s.u. 4.2.2.2.
146 S. die Gesetzesbegründung, BT-Drs. 14/7386, 48.
147 Zum Erfordernis der Verschlüsselung der biometrischen Merkmale s.u. 4.2.2.4.6 und 6.2.1.3.
148 Dieses Verbot fand sich bereits in § 1 Abs. 2 Satz 3 des PersAuswG von 1950 (BGBl S. 807).
149 So der Bericht des BT-Innenausschusses, BT-Drs. 8/3498, 9.
150 Zu den Folgen für das Auskunftsrecht s.u. 4.3.7.2.
151 Bericht des BT-Innenausschusses, BT-Drs. 8/3498, 9; *Medert/Süßmuth* 1998, § 3 Rn. 4.

§ 3 Abs. 3 Satz 1 PersAuswG nur bei der Bundesdruckerei GmbH und nur zum Nachweis über den Verbleib der Ausweise zu. Andere personenbezogene Daten dürfen dabei nicht gespeichert werden. Nach § 3 Abs. 3 Satz 2 PersAuswG ist eine Speicherung der übrigen Ausweisdaten ausschließlich und vorübergehend zur Herstellung des Personalausweises, das heißt zweckgebunden, zulässig. Die Angaben sind anschließend zu löschen. Mithin existiert in Deutschland kein zentrales Bevölkerungsregister mit den Daten aller Ausweisinhaber.

In technischer Hinsicht sind die Personalausweise nach einheitlichen Mustern mit Lichtbild auszustellen (§ 1 Abs. 2 Satz 1 PersAuswG) und enthalten eine maschinenlesbare Zone (§ 1 Abs. 3 PersAuswG).[152] Ihr Inhalt ist genau geregelt und beschränkt sich auf die Abkürzung "IDD" für "Identitätskarte der Bundesrepublik Deutschland", den Familiennamen, den oder die Vornamen, die Seriennummer, die Abkürzung "D" für die Eigenschaft als Deutscher, den Geburtstag, die Gültigkeitsdauer des Personalausweises, die Prüfziffern und Leerstellen.[153] § 1 Abs. 7 PersAuswG sieht im Übrigen die Bestimmung der Muster durch Rechtsverordnung vor, die das Bundesministerium des Innern mit Zustimmung des Bundesrates erlässt. Die erste Musterverordnung für den aktuellen Ausweis datiert vom 2. Juli 1986.[154] Sie wurde am 20. Januar 1997 sprachlich in eine geschlechtsneutrale Form geändert[155] und seitdem mehrmals novelliert.[156] In ihr ist lediglich die äußere Form des Ausweises geregelt (die etwa für die Sichtkontrolle wichtig ist); es erfolgt keine Anordnung der Sicherheitsmerkmale. Diese werden in Abstimmung mit dem Bundesministerium des Innern und dem Bundeskriminalamt durch die Bundesdruckerei GmbH bestimmt, die dabei im Auftrag des Kunden, des Bundesministeriums, handelt.[157]

2.2.1.3 Das Antrags- und Ausgabeverfahren

Die im Personalausweisgesetz genannten Personalausweisbehörden werden durch die Ausführungsgesetze der Länder bestimmt,[158] die auch Durchführungsbestimmungen für das weitere Verfahren erlassen haben.[159] Dieses beginnt mit einem förmlichen Antrag auf

---

152 Letzteres war einer der Hauptkritikpunkte bei der Einführung im Jahre 1987, s.u. 7.3.2.2.2.

153 Näher *Medert/Süßmuth* 1998, § 1 Rn. 26 ff.

154 Verordnung zur Bestimmung der Muster der Personalausweise der Bundesrepublik Deutschland, BGBl. I 1986, 1009 und BGBl. I 1987, 1160.

155 1. Verordnung zur Änderung der Verordnung zur Bestimmung der Muster der Personalausweise der Bundesrepublik Deutschland, BGBl I, 33.

156 Zuletzt durch Art. 4 V des Gesetzes v. 3.12.2001, BGBl. I, 3274.

157 Zu den aktuellen Sicherheitsmerkmalen s.u. 4.2.2.2, dort auch zur Frage, ob ein Übergang auf eine Chipkarte im Wege der Rechtsverordnung vorgenommen werden kann.

158 Vgl. ausführlich *Medert/Süßmuth* 1998, Teil C Rn. 4. Im Überblick sind zuständig die Gemeinden in Bayern, Niedersachsen, Nordrhein-Westfalen (als örtliche Ordnungsbehörde), im Saarland, in Sachsen, Sachsen-Anhalt (soweit keine Verwaltungsgemeinschaften bestehen) und Thüringen (in Landkreisen die Landratsämter), die Ortspolizeibehörden in Baden-Württemberg (bzw. die Verwaltungsgemeinschaften), Brandenburg (kreisfreie Städte, Ämter und amtsfreie Gemeinden), Bremen, Hessen (Bürgermeister), Mecklenburg-Vorpommern (Bürgermeister der kreisfreien Städte und der amtsfreien Gemeinden, Amtsvorsteher), Rheinland-Pfalz und Schleswig-Holstein (Bürgermeister der amtsfreien Gemeinden und Amtsvorsteher). Personalausweisbehörde in Berlin ist das Landeseinwohneramt, in Hamburg die Behörde für Inneres bzw. die Bezirksämter. Örtlich zuständig sind normalerweise die Ämter am Sitz der Hauptwohnung oder dort, wo der Ausweisinhaber meldepflichtig oder gemeldet ist. Ausnahmen bestehen regelmäßig aus wichtigen Gründen.

159 S. etwa für Hessen die Durchführungsbestimmungen v. 26.8.2002, StAnz Hess. Nr. 34, S. 3171 (die folgenden Ausführungen orientieren sich an diesem Bsp.); s.a. *Medert/Süßmuth* 1998, Teil C Rn. 10 ff.

einem einheitlichen Vordruck.[160] Für die erstmalige Ausstellung des Personalausweises sowie für die Neuausstellung nach Ablauf der Gültigkeitsdauer ist gemäß § 1 Abs. 6 Satz 1 PersAuswG eine Gebühr von acht Euro zu erheben.[161] Pro Jahr werden je nach Zyklussituation zwischen 5 und 10 Millionen neue Personalausweise ausgegeben.

Der Ausweisbewerber hat grundsätzlich persönlich zu erscheinen. Ausnahmen aus wichtigem Grund sind möglich.[162] Der Antrag wird sodann nach Maßgabe des Leitfadens zum Ausfüllen eines Antrags auf Ausstellung eines Personalausweises, der vom Bundesministerium des Innern erstellt wird und als Anlage Bestandteil der Verwaltungsvorschriften der Länder ist, von der Behörde (das heißt nicht vom Antragsteller) ausgefüllt.[163] Die Verwaltungsvorschriften schreiben den Personalausweisbehörden auch die Verwendung von Antragsvordrucken und Versandtaschen der Bundesdruckerei GmbH vor. Wird ein elektronisches Verfahren verwendet, so ist den Behörden ein Verfahren vorgegeben, das den Anforderungen der Bundesdruckerei GmbH genügt. Dabei handelt es sich zurzeit um das so genannte DIGANT-Verfahren, das im März des Jahres 2005 in 3.000 Personalausweisbehörden eingesetzt wurde.[164] Den Behörden steht es bislang frei, sich für dieses zu entscheiden, die Bundesdruckerei GmbH gewährt hierfür allerdings Rabatte beim Entgelt für die Ausweise. Geplant ist, die Verwendung des DIGANT-Verfahrens in Zukunft verbindlich vorzuschreiben.

Die Bundesdruckerei GmbH weist den Personalausweisbehörden auch die Kennzahlen für den Ausweis zu. Nach der Herstellung werden die Personalausweise an die Behörden übersandt, von diesen auf Richtigkeit und Vollständigkeit der Eintragungen überprüft und danach persönlich ausgehändigt. Ist dies aus wichtigem Grund nicht möglich, kann der Ausweis auch einer bevollmächtigten Person übergeben werden.

Weitere Anforderungen in den Verwaltungsvorschriften betreffen die sichere Aufbewahrung der auszugebenden Ausweise und der Vordrucke für die vorläufigen Papiere und die Pflicht zu Verwendung von Adressaufklebern der Bundesdruckerei GmbH bei Adressänderungen. Die übrigen Organisationsfragen werden von den Trägern der Personalausweisbehörden (regelmäßig den Gemeinden) unterschiedlich geregelt, da sie in deren Organisationshoheit fallen.

2.2.1.4 Das Personalausweisregister und seine Verwendung

Außer auf dem Personalausweis selbst werden personenbezogene Daten auch im Personalausweisregister geführt, das bei den Personalausweisbehörden angesiedelt ist.[165] Das Register enthält gemäß § 2a Abs. 1 Satz 2 PersAuswG das Lichtbild, die Unterschrift, verfahrensbedingte Bearbeitungsvermerke, die Daten des Ausweises nach § 1 Abs. 2 Pers-

160 Eine Ausnahme besteht für vorläufige Personalausweise.

161 Nach § 1 Abs. 6 Satz 2 PersAuswG ist die erstmalige Ausstellung des Personalausweises an Personen, die das 21. Lebensjahr noch nicht vollendet haben, gebührenfrei, während nach § 1 Abs. 6 Satz 3 PersAuswG von der Erhebung einer Gebühr abgesehen werden kann, wenn der Gebührenpflichtige bedürftig ist; zur Rechtmäßigkeit der Gebühr vgl. VGH Mannheim, NVwZ-RR 2003, 712 f.

162 In diesem Fall wird der Antrag von einem Mitarbeiter der Behörde in der Wohnung des Antragstellers, einem Krankenhaus oder einer Justizvollzugsanstalt aufgenommen.

163 Zu einzelnen Fragen bezüglich des Namens, Doktorgrads, Wohnorts etc. s. *Medert/Süßmuth* 1998, Teil C Rn. 20 ff. m.w.N.

164 Der jeweils aktuelle Stand ist unter http://www.bundesdruckerei.de/de/behoerde/3_1/index.html abrufbar; s.a. *Yildirim* 2004, 25 f.

165 Zum Ursprung der Entwicklung allgemeiner Personenregister im 15. Jahrhundert s. *Groebner* 2004, 48 ff.

AuswG, Vermerke über Anordnungen nach § 2 Abs. 2 PersAuswG,[166] Daten von gesetzlichen Vertretern (Familiennamen, Vornamen, Tag der Geburt und Unterschrift), die Seriennummer und das Gültigkeitsdatum des Personalausweises, die ausstellende Behörde und Angaben zur Erklärungspflicht des Ausweisinhabers nach § 29 StAG.[167] Die Daten des Personalausweisregisters sind nach § 2a Abs. 3 PersAuswG spätestens fünf Jahren nach Ablauf der Gültigkeit des Ausweises zu löschen.

Die Personalausweisbehörden gehören in aller Regel derselben Verwaltungseinheit wie die Meldebehörden an. Sie sind mit diesen organisatorisch zusammengefasst und nur funktional getrennt.[168] Die Trennung zwischen Personalausweis- und Melderegister ist (im Sinne des Grundsatzes der „informationellen Gewaltenteilung")[169] dennoch von Bedeutung, weil der Datenbestand unterschiedlich und das Auskunftsrecht des Personalausweisregisters enger ist als das des Melderegisters. Einige Länder schließen hier explizit Auskünfte an Dritte aus.[170]

§ 3 Abs. 2 PersAuswG bestimmt, dass die Vorgänge der Beantragung, Ausstellung und Ausgabe von Personalausweisen nicht zum Anlass genommen werden dürfen, die dafür erforderlichen Angaben außer bei den nach Landesrecht zuständigen örtlichen Personalausweisbehörden zu speichern. Damit ist der Aufbau paralleler bundes- wie landesweiter Register unzulässig.[171]

§ 1 Abs. 5 Satz 2 PersAuswG untersagt überdies die Einrichtung einer bundesweiten Datei für die biometrischen Merkmale. Neben § 3 Abs. 2 PersAuswG ist die Norm an sich überflüssig. Sie drückt jedoch den Willen des Gesetzgebers aus, ein System zu verhindern, in dem der Abruf individueller biometrischer Daten eines Betroffenen oder die Bestimmung eines Merkmalsträgers anhand eines anderweitig erhobenen Datensatzes möglich wären. Das ist bei der Auslegung des § 1 Abs. 5 Satz 2 PersAuswG zu berücksichtigen. Dem Wortlaut nach wären nämlich sowohl landesweite Dateien als auch eine Vernetzung der dezentral gespeicherten Merkmalsdateien zulässig. Eine solche Auslegung wird dem Sinn und Zweck der Vorschrift jedoch nicht gerecht. Für die Grundrechtsbeeinträchtigungen, die die Norm verhindern soll, macht es keinen Unterschied, ob eine räumlich zentralisierte Datensammlung oder ein – wie auch immer organisiertes – dezentral-vernetztes System zur Abfrage verwendet wird, wenn letzteres in gleicher Weise das Auffinden des gesuchten Datensatzes garantiert. Unter den heutigen Bedingungen der automatisierten Datenverarbeitung besteht zwischen beiden Systemen weder auf der Ebene der Effektivität noch auf der des datenschutzrechtlichen Bedrohungspotentials ein Unterschied. Das Verbot in § 1 Abs. 5 Satz 2 PersAuswG ist deshalb weit zu verstehen. Es erfasst jedes Speichersystem, das ein funktionelles Äquivalent zur räumlich zentralisierten Speicherung darstellt.[172]

Nach der aktuellen Gesetzeslage wäre überdies eine Speicherung biometrischer Daten - abgesehen von Gesichtsdaten – auch in nicht vernetzen Personalausweisregistern rechts-

166 Das betrifft Nutzungseinschränkungen im Reiseverkehr entsprechend den Passversagungsgründen nach § 7 Abs. 1 PassG; s. dazu *Medert/Süßmuth* 1998, § 2 Rn. 7 ff.

167 Letzteres betrifft die Erklärung bei Erreichen der Volljährigkeit über die Wahl zwischen der deutschen und einer ausländischen Staatsangehörigkeit, wenn die erstere nach § 4 Abs. 3 oder § 40b StAG erworben wurde.

168 *Medert/Süßmuth* 1998, § 2b Rn. 38; Roßnagel-*Wollweber*, Kap. 8.5, Rn. 6.

169 S.u. 4.2.1.2.3.

170 *Medert/Süßmuth* 1998, § 2a Rn. 6; vgl. auch *Golembiewski/Probst* 2003, 40 f.; darin liegt eine höhere Zugangsbeschränkung des Personalausweisregisters, s. BT-Innenausschuss, BT-Drs. 10/5129, 5.

171 *Medert/Süßmuth* 1998, § 3 Rn. 5 f.

172 Dieses Verbot ist verfassungsrechtlich abgesichert, vgl. unten 4.2.2.4.3.

widrig. Die Aufzählung der im Register enthaltenen Daten in § 2a Abs. 1 Satz 2 PersAuswG ist abschließend und erwähnt biometrische Daten nicht.

Das Personalausweisregister darf des Weiteren nicht beliebig eingesetzt werden. Sein Zweck ist nach § 2a Abs. 2 PersAuswG ausschließlich die Ausstellung und Feststellung der Echtheit der Ausweise, die Identitätsfeststellung des Inhabers (etwa bei Abhandenkommen oder Unbenutzbarkeit des Ausweises) und die Durchführung des Personalausweisgesetzes und der Ausführungsgesetze der Länder. Eine andere Nutzung ist aufgrund des verfassungsrechtlichen Erfordernisses der Zweckbestimmung und -bindung[173] unzulässig.

Die nähere Verwendung der Daten im Personalausweisregister wird in § 2b PersAuswG geregelt. Eine Übermittlung an andere Behörden ist nach § 2b Abs. 2 PersAuswG zulässig, wenn diese durch Gesetz oder Rechtsverordnung zum Erhalt berechtigt sind und ohne Kenntnis der Daten nicht in der Lage wären, eine ihnen obliegende Aufgabe zu erfüllen.[174] Formelle Voraussetzung ist ein Ersuchen der anfragenden Behörde. Damit sind automatisierte Abrufverfahren unzulässig.[175] Außerdem ist erforderlich, dass die Daten nicht oder nur mit unverhältnismäßigem Aufwand beim Betroffenen selbst erhoben werden können, beziehungsweise, dass aufgrund der Art der Aufgabe von einer solchen Erhebung abgesehen werden muss. Die Verantwortung für das Vorliegen dieser Voraussetzungen liegt nach § 2b Abs. 3 PersAuswG bei der ersuchenden Behörde.[176] Der Anlass des Ersuchens und die Herkunft der übermittelten Daten sind bei der ersuchenden Behörde aktenkundig zu machen.[177] Bei Anfragen von Sicherheits- und Strafverfolgungsbehörden des Bundes besteht eine Sonderregelung, wonach stattdessen Name und Anschrift des Betroffenen sowie Anlass der Übermittlung zu dokumentieren sind. Die Aufzeichnungen sind gesondert (das heißt listenmäßig) aufzubewahren, zu sichern und nach einem Jahr zu löschen.

Von wenigen Ausnahmen abgesehen haben die Länder für Anfragen ihrer Behörden Regelungen getroffen, die § 2b Abs. 3 Satz 4 und 5 PersAuswG entsprechen, sodass auch diese Behörden ihre Anfragen dokumentieren müssen.[178] Von einer Dokumentation der Anfragen bei den Personalausweisbehörden hat der Bundesgesetzgeber mit Absicht abgesehen, weil dadurch eine umfassende Aufzeichnung aller Anfragen entstehen würde, die gerade bei Übermittlungen an Gefahrenabwehr- und Strafverfolgungsbehörden unabhängig vom Ergebnis der weiteren Datenverarbeitung bei diesen Stellen für den Betroffenen belastend wäre.[179]

Ein Hauptbeispiel für die Übermittlung von Daten aus dem Personalausweisregister ist die Lichtbildanforderung der Strafverfolgungsbehörden im Rahmen der Ermittlung bei Straßenverkehrsdelikten.[180] In der Praxis kommt es immer wieder zur Verstößen gegen die in § 2b Abs. 2 Nr. 3 PersAuswG festgelegten Übermittlungsvoraussetzungen, weil die Behörden teilweise standardmäßig das Lichtbild anfordern, anstatt zunächst andere Ermitt-

---

173 S.u. 4.2.1.2.2.

174 Zu Gegenstand und Umfang des Übermittlungsvorgangs vgl. *Medert/Süßmuth* 1998, § 2b Rn. 13 ff.

175 AG Stuttgart, DuD 2003, 649, 651 (zur gleichlautenden Norm des § 22 PassG); zu automatisierten Abrufverfahren s.u. 4.3.6.3.

176 Die Personalausweisbehörde hat dennoch die Plausibilität des Ersuchens zu prüfen, s. *Medert/Süßmuth* 1998, § 2b Rn. 24. Die Verantwortungsverteilung gilt auch für Anfragen einer funktional anderen Behörde derselben organisatorischen Verwaltungseinheit (z.B. Gemeinde), s. AG Stuttgart, DuD 2003, 649, 651.

177 Damit ist die konkrete Verfahrensakte gemeint, s. zur entsprechenden Norm im PassG (§ 22 Abs. 3 Satz 3) AG Stuttgart, DuD 2003, 649, 650.

178 S. *Medert/Süßmuth* 1998, § 2b Rn. 39 ff.

179 S.a. den Bericht des BT-Innenausschusses, BT-Drs. 10/5129, 5.

180 S. *Pätzel*, DuD 1998, 188 f.; Roßnagel-*Wollweber*, Kap. 8.5, Rn. 33 f.

lungsmittel durchzuführen. Dieses Verhalten ist wegen des Verstoßes gegen das Erforderlichkeitsprinzip rechtswidrig, führt allerdings nach der (problematischen) obergerichtlichen Rechtsprechung nicht zu einem Beweisverwertungsverbot in einem späteren Straf- oder Ordnungswidrigkeitsverfahren.[181]

Eine Verwendung der Registerdaten ist nach § 2b Abs. 4 PersAuswG außerdem zur Berichtigung des Melderegisters zulässig. Diese Übermittlung erfolgt von Amts wegen, das heißt unabhängig vom Vorliegen der Voraussetzungen der § 2b Abs. 2 und 3 PersAuswG. Übermittelt werden dürfen allerdings nur die zur Berichtigung erforderlichen Daten. Dies sind nur diejenigen, die in beiden Registern vorhanden sind, also insbesondere nicht das Lichtbild, die Unterschrift, die Größe und die Augenfarbe, die ausschließlich Inhalt des Personalausweisregisters sind.

2.2.1.5 Die Verwendung des Ausweises

Das Personalausweisgesetz enthält auch Bestimmungen zur Verwendung des Personalausweises und der auf ihm gespeicherten Angaben.[182] Ein Einsatz der Seriennummern zum Abruf personenbezogener Daten aus Dateien oder zur Verknüpfung von Dateien ist nach § 3 Abs. 4 Satz 1 PersAuswG prinzipiell unzulässig. Abweichend davon dürfen die Seriennummern von den Personalausweisbehörden für den Abruf personenbezogener Daten aus ihren Dateien und von den Polizeibehörden und -dienststellen des Bundes und der Länder für den Abruf[183] der in Dateien gespeicherten Seriennummern solcher Personalausweise eingesetzt werden, die für ungültig erklärt worden oder abhanden gekommen sind oder bei denen der Verdacht einer Benutzung durch Nichtberechtigte besteht.

§ 3 Abs. 5 Satz 1 PersAuswG bestimmt den Verwendungszweck der künftigen verschlüsselten Merkmale und Angaben. Diese dürfen nur „zur Überprüfung der Echtheit des Dokuments und zur Identitätsprüfung ausgelesen und verwendet werden". Für die biometrischen Merkmale bedeutet dies, dass sowohl eine Identifikation als auch eine Verifikation[184] möglich wären. Wegen des Verbots einer bundesweiten Datei in § 1 Abs. 5 Satz 2 PersAuswG, das sich auf funktionale Äquivalente erstreckt, beschränkt sich der Einsatz jedoch auf Verfahren der Verifikation, da Verfahren der Identifikation eine zentrale Datenbank voraussetzen. Die Beschränkung auf den Zweck der Identitätsprüfung ist nach geltendem Recht abschließend.[185]

§ 3a PersAuswG regelt den automatischen Abruf aus Dateien und die automatische Speicherung für den öffentlichen Bereich.[186] Nach § 3a Abs. 1 PersAuswG ist der Abruf für Behörden und sonstige öffentliche Stellen im Grundsatz unzulässig. Es bestehen jedoch Ausnahmen für Polizeibehörden und -dienststellen des Bundes und der Länder sowie für

---

181 S. z.B. OLG Frankfurt, NJW 1997, 2963; OLG Hamm, Beschluss v. 3.4.1997, 3 Ss OWi 248/97; BayObLG, JZ 2003, 1124; DAR 1999, 79; ebenso *Pätzel*, DuD 1998, 188, 189; nach OLG Stuttgart, DAR 2002, 566; AG Schleiden, DAR 2001, 232 liegt bereits keine unzulässige Datenerhebung vor; ein Verwertungsverbot nehmen dagegen an *Nobis*, DAR 2002, 299, 300 f.; *Schäpe*, DAR 2002, 568 (anders noch *Schäpe*, DAR 1999, 186 f.); kritisch zu den Übermittlungsregeln schon *Bäumler*, CR 1986, 284, 285.

182 Vgl. zum Folgenden bereits *Roßnagel/Hornung*, in: Reichl/Roßnagel/Müller 2005, 127.

183 Hierunter ist nicht nur ein automatisiertes Abrufverfahren, sondern jede Form des Zugangs auch zu herkömmlich geführten Dateien zu verstehen, vgl. *Medert/Süßmuth* 1998, § 3 Rn. 12.

184 Zu diesen Begriffen vgl. unten 2.3.3.2.

185 S. dazu unten 4.2.2.3.

186 Werden Daten unter Verstoß gegen diese Norm gespeichert, so ist dies nach § 202a StGB strafbewehrt, s. *Medert/Süßmuth* 1998, § 3a Rn. 5.

Zollbehörden.[187] Diese Behörden dürfen im Rahmen ihrer Aufgaben und Befugnisse mittels des Personalausweises automatisch Daten aus Dateien des polizeilichen Fahndungsbestandes abrufen, die der Grenzkontrolle, der Fahndung oder Aufenthaltsfeststellung aus Gründen der Strafverfolgung, Strafvollstreckung oder der Abwehr von Gefahren für die öffentliche Sicherheit dienen.[188] Beim automatischen Abruf dürfen vorbehaltlich gesetzlicher Regelungen nach § 3a Abs. 1 Satz 3 PersAuswG keinerlei (das heißt auch keine handschriftlichen) Aufzeichnungen über solche Abrufe angefertigt werden, die zu keiner Feststellung geführt haben. Erfolgt eine Feststellung, dürfen personenbezogene Daten gemäß § 3a Abs. 2 PersAuswG ohne explizite gesetzliche Grundlage[189] nicht in einer Datei gespeichert werden; eine Speicherung außerhalb von Dateien ist dagegen nach dem Personalausweisgesetz nicht untersagt. Nach beiden Regelungen ist damit die Bildung von dateimäßigen Bewegungsprofilen bei Kontrollen unzulässig. Die zurzeit einzige gesetzliche Ausnahme zu diesem Verbot findet sich in § 163d StPO.[190]

Für den nichtöffentlichen Bereich sind die Verwendungsmöglichkeiten des Personalausweises demgegenüber erheblich enger. Zwar kann der Ausweis nach § 4 Abs. 1 PersAuswG auch im privaten Bereich als Ausweis- und Legitimationspapier benutzt werden. Das betrifft eine Vielzahl von Alltagssituationen, wie zum Beispiel die Eröffnung eines Bankkontos, Altersnachweise im Bereich des Jugendschutzes oder ganz allgemein den Vertragsschluss zwischen bislang unbekannten Vertragspartnern, insbesondere bei wichtigen oder betrugsanfälligen Geschäften. Nach § 4 Abs. 2 und 3 PersAuswG ist im nichtöffentlichen Bereich jedoch die Verwendung der Seriennummer zum Abruf aus Dateien oder zu deren Verknüpfung sowie der Einsatz des Ausweis allgemein zum automatischen Abruf und zur automatischen Speicherung unzulässig. Ein Verstoß ist nach § 5 Abs. 1 Nr. 3 PersAuswG bußgeldbewehrt. Ausnahmen von diesen Verboten bestehen im privaten Bereich nicht. Deshalb dürfen sich Fluggesellschaften, Kreditinstitute, Versicherungs- oder Versandunternehmen und vergleichbare Einrichtungen keiner ausweis- oder passgerechten Lesegeräte zur schnelleren oder eindeutigeren Identifizierung von Kunden bedienen.[191]

Hintergrund der Regelung war die Gefahr der Entstehung eines einheitlichen Personenkennzeichens, das die Zusammenführung bislang verteilt gespeicherter Angaben erleichtern würde.[192] Diese Gefahr besteht zwar im öffentlichen wie im nichtöffentlichen Bereich. Im Gegensatz zum Bereich der hoheitlichen Datenverarbeitung, in dem das Allgemeininteresse an Gefahrenabwehr und Strafverfolgung automatische Abruf- und Speicherungsverfahren rechtfertigt, besteht im privaten Bereich aber kein vergleichbares Bedürfnis. Die automatische Datensammlung und -zusammenführung wird vielmehr regelmäßig im Interesse des Vertragspartners des Ausweisinhabers erfolgen. Um den Inhaber zu schützen, hat der Gesetzgeber diese Verwendungsart untersagt. Im Rahmen des denkbaren Einsatzes der biometrischen Merkmale des digitalen Personalausweises zur Identitätsprüfung auch im

187 S. näher *Medert/Süßmuth* 1998, § 3a Rn. 11 ff. Es handelt sich im Wesentlichen um Zollbehörden, den BGS, das BKA, den Polizeivollzugsdienst des Bundestages und die Schutz- und Kriminalpolizeien der Länder, nicht jedoch um Nachrichtendienste, Verfassungsschutzbehörden und Staatsanwaltschaften.

188 Das betrifft v.a. das beim BKA geführte INPOL-System (§§ 7, 8 BKAG), s. *Medert/Süßmuth* 1998, § 3a Rn. 18; ausführlich dazu Rublack, DuD 1999, 437 ff.; Roßnagel-*Bäumler*, Kap. 8.3, Rn. 61 ff.

189 Hierunter ist nicht jedes Gesetz im materiellen Sinn, sondern ausschließlich ein Parlamentsgesetz zu verstehen, s. *Medert/Süßmuth* 1998, § 3a Rn. 24.

190 *Medert/Süßmuth* 1998, § 3a Rn. 3 ff., 23; s. näher unten 2.2.1.6.

191 *Medert/Süßmuth* 1998, § 4 Rn. 9; Roßnagel-*Wollweber*, Kap. 8.5, Rn. 32.

192 S. näher unten 4.2.1.2.4.

nichtöffentlichen Umfeld stellt sich allerdings die Frage, ob dieses Verbot auch verfassungsrechtlich geboten ist.[193]

2.2.1.6 Beispiele für den praktischen Einsatz

Der digitale Personalausweis wird – wie der derzeit gültige – in einer Vielzahl von hoheitlichen Einsatzfeldern zur Identitätsprüfung Verwendung finden, insbesondere im präventiven Bereich des Polizeirechts und bei der Strafverfolgung.[194]

Die Polizei ist im Rahmen der Gefahrenabwehr zu einer Reihe von Maßnahmen zur Identitätsfeststellung befugt. Die Prüfung freiwillig[195] mitgeführter Ausweispapiere ist hierbei das zentrale Mittel.[196] Sistierung und erkennungsdienstliche Maßnahmen sind regelmäßig nur zulässig, wenn die Identifizierung auf andere Weise nicht oder nur unter erheblichen Schwierigkeiten möglich ist.[197] Damit entfällt bei Vorlage eines Personalausweises regelmäßig die Zulässigkeit weiterer Maßnahmen. Das gilt selbst dann, wenn dieser abgelaufen ist.[198]

Die Personenfeststellung ist eine der häufigsten polizeilichen Standardmaßnahmen, weil polizeiliches Einschreiten regelmäßig die vorherige Identifizierung des Betroffenen erfordert.[199] In Anlehnung an § 9 Abs. 1 ME PolG[200] finden sich heute in allen Bundesländern mehr oder weniger identische Rechtsgrundlagen für die Identitätsfeststellung. Zulässig ist diese danach zur Abwehr einer Gefahr,[201] an gefährlichen Orten[202] und gefährdeten Objekten, teilweise auch zum Schutz gefährdeter Personen wie Führungskräfte aus Wirtschaft, Politiker und Staatsgäste.[203] Dabei wird nicht zwischen Störern und Nichtstörern unterschieden, sodass auch routinemäßige Kontrollen zulässig sind.[204] Außerdem können Identitätsüberprüfungen an so genannten Kontrollstellen zur Abwehr einer konkreten Gefahr (etwa der Verhinderung von Straftaten nach § 27 VersammlG) und zum Zweck einer ereignisunabhängigen und allgemeinen Fahndung durchgeführt werden.[205] Weitere Ermächtigungsgrundlagen, die vor allem nach Wegfall der innereuropäischen Grenzkontrollen

193 Dazu unten 4.2.2.5.

194 Vgl. zum Folgenden bereits *Roßnagel/Gitter/Hornung*, in: Reichl/Roßnagel/Müller 2005, 146 f.

195 In Deutschland besteht keine allgemeine Pflicht zum Mitführen von Ausweispapieren, s.o. 2.2.1.1.

196 Daneben kommen die Polizeibekanntheit des Betroffenen, Erkundigungen bei Dritten, Gegenüberstellung und erkennungsdienstliche Behandlung in Betracht, s. Lisken/Denninger-*Rachor*, Kap. F, Rn. 312; *Pieroth/Schlink/Kniesel* 2002, 246 ff.

197 Vgl. § 10 ME PolG (s. *Kniesel/Vahle* 1990, 12), *Gusy* 2003, Rn. 233 f., 240 ff. m.w.N.; *Pieroth/Schlink/Kniesel* 2002, 245 f.; *Schoch* 2003, Rn. 202; Lisken/Denninger-*Rachor*, Kap. F, Rn. 406.

198 *Gusy* 2003, Rn. 233.

199 Vgl. Lisken/Denninger-*Rachor*, Kap. F, Rn. 309.

200 S. *Kniesel/Vahle* 1990, 11.

201 In wieweit die Feststellung der Identität *selbst* eine präventive Wirkung entfalten kann, ist allerdings umstritten (bejahend *Pieroth/Schlink/Kniesel* 2002, 239, zweifelnd *Gusy* 2003, Rn. 227; *Benfer* 2001, Rn. 198). Eine mögliche abschreckende Wirkung, die z.B. *Würtenberger/Heckmann/Riggert* (2002, Rn. 324) und *Mußmann* (1994, Rn. 180) annehmen („Zipperlein-Effekt") wird tlw. auch dem Straf- oder Strafverfahrensrecht zugeordnet, s. Lisken/Denninger-*Rachor*, Kap. F, Rn. 321.

202 S. *Gusy* 2003, Rn. 228; *Pieroth/Schlink/Kniesel* 2002, 239 f.; Lisken/Denninger-*Rachor*, Kap. F, Rn. 325 ff. Die Polizeigesetze verwenden nicht diesen Begriff, sondern konkretisieren ihn durchweg weiter, etwa als Orte, an denen typischerweise Straftaten verübt werden, an denen sich Straftäter verbergen, u.a.

203 Lisken/Denninger-*Rachor*, Kap. F, Rn. 337 ff.

204 Vgl. *Benfer* 2001, Rn. 216, 220. Sofern die Ermächtigungsgrundlage hier ein „Aufhalten" am Ort voraussetzt, zählt dazu nicht das bloße Passieren, s. OVG Hamburg, NVwZ-RR 2003, 276, 277.

205 *Pieroth/Schlink/Kniesel* 2002, 241 ff.; die Verfassungsmäßigkeit dieser Kontrollstellen wird tlw. bestritten, s. z.B. Lisken/Denninger-*Rachor*, Kap. F, Rn. 348 ff.

zwischen den Mitgliedstaaten des Schengen-Acquis eingerichtet worden sind, finden sich in einigen Bundesländern inzwischen für den Bereich des Grenzgebietes, der Durchgangsstraßen und öffentlichen Einrichtungen des internationalen Verkehrs.[206] Wegen ihres weiten Tatbestands begegnen diese Bestimmungen allerdings verfassungsrechtliche Bedenken.[207]

Der Bundesgrenzschutz verfügt über ähnliche Befugnisse. Nach § 2 Abs. 1 BGSG obliegt ihm insbesondere der grenzpolizeiliche Schutz des Bundesgebiets, der nach § 2 Abs. 2 Nr. 2 a) BGSG die Überprüfung von Grenzübertrittspapieren umfasst. Dazu zählt gemäß § 2 Abs. 2 DVPassG auch der Personalausweis. Die Befugnisse zur Identitätsfeststellung richten sich nach § 23 BGSG und umfassen die Gefahrenabwehr, die polizeiliche Kontrolle des grenzüberschreitenden Verkehrs, die Verhinderung oder Unterbindung unerlaubter Einreise (im Grenzgebiet bis zu einer Tiefe von 30 Kilometern) und den Schutz privater Rechte und gefährdeter Objekte.[208] Deren Bestimmung in § 23 Abs. 1 Nr. 4 BGSG orientiert sich an den für den Bundesgrenzschutz typischen Objekten und nennt seine eigenen Einrichtungen, Eisenbahnen des Bundes, Verkehrsflughäfen, Amtssitze eines Verfassungsorgans oder Bundesministeriums und Grenzübergangsstellen.

Wenn jemand einer Straftat verdächtig ist, können im Strafprozessrecht die Staatsanwaltschaft und die Beamten des Polizeidienstes nach § 163b Abs. 1 StPO die zur Feststellung der Identität erforderlichen Maßnahmen treffen. Darunter fällt vor allem die Identifizierung durch amtlichen Ausweis.[209] Der Verdächtige darf festgehalten werden, wenn die Identität sonst nicht oder nur unter erheblichen Schwierigkeiten festgestellt werden kann.[210] Unter dieser Voraussetzung sind auch Durchsuchung und Durchführung erkennungsdienstlicher Maßnahmen zulässig. § 163b Abs. 2 StPO lässt die Identitätsfeststellung bei anderen als verdächtigen Personen zu, wenn es zur Aufklärung einer Straftat geboten ist; Durchsuchung und erkennungsdienstliche Maßnahmen sind jedoch in diesem Fall gegen den Willen des Betroffenen nicht gestattet.

§ 111 StPO ermöglicht die Einrichtung von Kontrollstellen auf öffentlichen Straßen und Plätzen.[211] Voraussetzung ist, dass Tatsachen den Verdacht begründen, es sei eine der genannten Straftaten begangen worden.[212] Gemäß § 111 Abs. 1 Satz 2 StPO ist an einer Kontrollstelle jedermann verpflichtet, seine Identität feststellen zu lassen. Zu erwähnen ist auch noch die computergestützte Fahndungsmaßnahme nach § 163d StPO. Danach dürfen beim Verdacht einer Straftat nach § 111 und § 100a Satz 1 Nr. 3 und 4 StPO Daten, die anlässlich von Kontrollen erfasst werden, in einer Datei gespeichert werden, wenn Tatsachen die Annahme rechtfertigen, dass ihre Auswertung zur Ergreifung des Täters oder zur Aufklärung der Straftat führen kann und die Maßnahme nicht außer Verhältnis zur Bedeutung der Sache steht.[213] Die Daten dürfen nur an Strafverfolgungsbehörden übermittelt

---

206 S. *Schoch* 2003, Rn. 201 m.w.N.

207 Etwa Lisken/Denninger-*Rachor*, Kap. F, Rn. 325 ff.; *Lisken*, NVwZ 1998, 22 ff.; nicht ganz so weitgehend *Gusy* 2003, Rn. 213, der den entsprechenden Normen bei der gebotenen restriktiven Auslegung allerdings jede Nützlichkeit abspricht (noch deutlicher die Vorauflage, Rn. 202).

208 S. näher *Fischer/Hitz/Laskowski/Walter* 1996, § 23 BGSG Rn. 6 ff.

209 *Benfer* 2001, Rn. 245; *Meyer-Goßner*, § 163b Rn. 6.

210 Das nähere Verfahren hierzu bestimmt sich nach § 163c StPO, vgl. *Meyer-Goßner*, § 163c Rn. 2 ff.

211 Näher *Benfer* 2001, Rn. 1325 ff. Der Charakter der Norm als repressives oder präventives Instrument ist umstritten, vgl. die Nachweise bei *Meyer-Goßner*, § 111 Rn. 1.

212 Die Effektivität von Kontrollstellen zur Aufklärung der genannten Taten wird allerdings als gering eingestuft; s. *Gusy* 2003, Rn. 215, wonach Zufallsfunde hinsichtlich anderer Straftaten überwiegen.

213 Sog. „Schleppnetzfahndung". Die Weiterverwendbarkeit der an der Kontrollstelle angefallenen Daten geht erheblich über die Polizeigesetze der Länder hinaus, s. Lisken/Denninger-*Rachor*, Kap. F, Rn. 351.

werden. Nach § 163d Abs. 2 StPO darf die Maßnahme nur durch den Richter, bei Gefahr im Verzug auch durch die Staatsanwaltschaft und ihre Hilfsbeamten angeordnet werden. Sie darf höchstens drei Monate andauern und nur einmal um nicht mehr als drei Monate verlängert werden. Werden die erlangten Daten nicht mehr benötigt, so sind sie nach § 163d Abs. 4 Satz 2 StPO unverzüglich zu löschen. Ihr Zweck ist auf die Verwendung im Strafverfahren begrenzt, wenn sich nicht weitere Erkenntnisse zur Aufklärung einer anderen Straftat oder Ermittlung einer Person ergeben, die zur Fahndung oder Aufenthaltsfeststellung ausgeschrieben ist. Schließlich ist gemäß § 163d Abs. 5 StPO der Betroffene von der Maßnahme zu benachrichtigen, wenn dies nicht den Untersuchungszweck oder die öffentliche Sicherheit beeinträchtigt.

Neben diesen selbständigen Maßnahmen ist die Identitätsfeststellung auch als „unselbständiger Begleiteingriff" gestattet, wenn etwa eine Durchsuchung oder sonstige strafprozessuale Maßnahme gegen einen Verdächtigen oder Beschuldigten zulässig ist, und zu ihrer Durchführung zunächst die Identität des Betroffenen bestimmt werden muss.[214] Für dieses Vorgehen enthält die Strafprozessordnung keine eigene Ermächtigungsgrundlage. Es genügt die Rechtmäßigkeit der Grundmaßnahme.

Darüber hinaus kennen das öffentliche und private Recht eine Vielzahl von Verwendungen des Personalausweises. Beispiele enthalten § 56 Abs. 3 Satz 2 BWO (Bundestagswahl), § 10 Abs. 2 BeurkG (notarielle Beurkundung von Erklärungen), § 1 Abs. 5 Nr. 1 WPflV (Musterung), § 13 Abs. 1 SÜG (Sicherheitsüberprüfung),[215] § 38 Nr. 1 WaffenG (Ausweispflicht beim Führen einer Schusswaffe), § 12 Abs. 2 Satz 3 FeV (Durchführung des Sehtests), § 16 Abs. 3 Satz 3 und § 17 Abs. 5 Satz 2 FeV (theoretische und praktische Fahrprüfung), § 3 Nr. 3 PersStdGAV (Eintragung ins Heiratsbuch),[216] § 154 Abs. 2 AO (Kontoeröffnung),[217] § 1 Abs. 5 GwG (Identifizierung nach dem Geldwäschegesetz), § 6 Abs. 1 PDSV (Ausweispflicht am Postverkehr Beteiligter) und § 3 Abs. 1 Satz 1 SigV (Vergabe von qualifizierten Zertifikaten).

2.2.2 Regelungen für die elektronische Gesundheitskarte

Im Unterschied zum digitalen Personalausweis besteht für die elektronische Gesundheitskarte eine von ihrer Idee her umfassende gesetzliche Regelung. Allerdings hat der Gesetzgeber darauf verzichtet, technische Aspekte im Detail zu regeln. Die Bestimmungen bedürfen also der technischen Umsetzung.

2.2.2.1 Allgemeine Regeln für die Datenverwendung im Gesundheitswesen

Das GKV-Modernisierungsgesetz regelt die Verwendung von Daten, die auch bislang, jedoch teilweise in anderer Form, bei den Beteiligten im Gesundheitswesen erhoben, verarbeitet und genutzt werden. Die allgemeinen Regeln, die im Gesundheitswesen für diese Verwendung gelten, sind im Grundsatz auch auf das System der Gesundheitskarte anwendbar.

---

214 *Gusy* 2003, Rn. 236.

215 Bei der sog. Sicherheitserklärung muss der Betroffene u.a. seine Personalausweisnummer angeben.

216 Hier kann auch ein abgelaufener Ausweis ausreichen, vgl. Entscheidung des Fachausschusses Nr. 3338, StAZ 1994, 324.

217 Diese erfordert nach h.M. die Identifizierung des Antragstellers mittels Personalausweis oder Reisepass, vgl. III Ziff. 7 ff. der Verlautbarungen des Bundesaufsichtsamtes für das Kreditwesen über Maßnahmen der Finanzdienstleistungsinstitute zur Bekämpfung und Verhinderung der Geldwäsche v. 30.3.1998 (http://www.bakred.de/texte/verlautb/gwg34fin.htm); *Carl/Klos*, DStZ 1995, 296, 302 ff.

Zu unterscheiden ist zwischen den Versicherungsstammdaten und gesundheitsbezogenen Daten.[218] Die Stammdaten werden bei der Begründung des Versicherungsverhältnisses erhoben. Grundlage für die Erhebung von Gesundheitsdaten durch Leistungserbringer ist demgegenüber immer der Behandlungsvertrag.[219] Für den praktisch wichtigsten Fall der nicht öffentlichen Stellen (hierunter fallen insbesondere Vertragsärzte)[220] lässt § 28 Abs. 7 BDSG die Datenerhebung zum Zweck der Gesundheitsvorsorge, der medizinischen Diagnostik, der Gesundheitsversorgung oder Behandlung und für die Verwaltung von Gesundheitsdiensten zu, sofern die Verarbeitung durch eine Personen erfolgt, die einer Geheimhaltungspflicht unterliegt. Neben dieser Regelung ist so gut wie kein Raum mehr für § 28 Abs. 1 Nr. 1 BDSG.[221]

Nach § 1 Abs. 3 BDSG gehen sowohl andere Rechtsvorschriften des Bundes als auch gesetzliche Geheimhaltungspflichten und Berufsgeheimnisse dem Bundesdatenschutzgesetz vor. Im Gesundheitswesen betrifft das insbesondere:

- bereichsspezifische Regelungen des Sozialgesetzbuches und Sonderbestimmungen für Krankenhäuser (Landeskrankenhausgesetze, Gesundheitsdatenschutzgesetze),[222]
- die ärztliche Schweigepflicht,[223] die sich aus § 203 Abs. 1 Nr. 1 StGB, der standesrechtlichen Norm des § 9 MBO-Ä 2004[224] und dem Behandlungsvertrag ergibt und
- Dokumentationspflichten für Ärzte.[225] Dabei handelt es sich einerseits um eine standesrechtliche Berufspflicht, die auf den Berufsordnungen analog § 10 MBO-Ä 2004 beruht. Andererseits ist die Dokumentationspflicht auch im Persönlichkeitsrecht des Patienten begründet und bildet eine vertragliche Nebenpflicht zum Arztvertrag.[226] Außerdem bestehen weitere gesetzliche Pflichten zur Dokumentation des Behandlungsprozesses.[227]

---

218 Die folgende Darstellung beschränkt sich auf den für die elektronische Gesundheitskarte relevanten Kontext. Die Datenverwendung durch die gesetzlichen Krankenkassen (insbesondere bei der Abrechnung) wird deshalb nur am Rande behandelt.

219 *Bultmann/Wellbrock/Biermann/Engels/Ernestus/Höhn/Wehrmann/Schurig* 2002, 4. Dieser wird durch schriftliche und mündliche Absprachen zwischen Patient und Arzt weiter konkretisiert, s. *Wehrmann/Wellbrock*, CR 1997, 754, 755.

220 Unzutreffend insoweit Laufs/Uhlenbruck-*Schlund* 2002, 588, wonach für die Datenerhebung § 13 BDSG anwendbar sein soll. Bei Krankenhäusern ist nach Trägern zu differenzieren, wobei aber im Ergebnis i.a.R. entweder die Normen des BDSG für nicht öffentliche Stellen oder bereichsspezifische Landesregelungen Anwendung finden, s. *Hermeler* 2000, 69 ff., insbes. die Übersicht auf S. 76. Die Landesregeln können durchaus erheblich differieren, s. für das Bsp. Einwilligung ebd., 80 f.

221 Simitis-*Simitis*, § 28 Rn. 114. Das wird übersehen von Roßnagel-*Schirmer*, Kap. 7.12, Rn. 78; s.a. unten 4.3.4.2.2.

222 S. die Übersicht bei *Hermeler* 2000, 67 ff.

223 Vgl. hierzu aus datenschutzrechtlicher Sicht Roßnagel-*Schirmer*, Kap. 7.12, Rn. 32 ff.; Roßnagel-*Miedbrodt*, Kap. 4.9, Rn. 88 ff.; *Bäumler*, MedR 1998, 400; *Klöcker/Meister* 2001, 27 ff.; s. zu § 203 StGB ausführlich unten 4.2.3.5.1.

224 Die Musterverordnung ist unter http://www.bundesaerztekammer.de/30/Berufsordnung/Mbopdf.pdf abrufbar. Sie wird rechtswirksam, wenn sie von der Kammerversammlung der jeweiligen Ärztekammer als (landesrechtliche) Satzung beschlossen und von den Aufsichtsbehörden genehmigt wird.

225 S. zur ärztlichen Dokumentation ausführlich *Wendt* 2001 (insbes. Teil 1 C); *Laskaridis* 2003, 23 ff. m.w.N.; Laufs/Uhlenbruck-*Uhlenbruck/Schlund* 2002, 480 ff.; zur Erfüllbarkeit der Dokumentationspflicht durch elektronische Dokumente *Hermeler* 2000, 107 ff.; *Laskaridis* 2003, 156 ff.

226 BGHZ 72, 132 (137); 85, 327 (329) in Abkehr von der vorherigen Rspr., die in ihr lediglich eine Gedächtnisstütze sah, s. BGH, VersR 1963, 168 f.; dies entsprach bis BGHZ 72, 132 auch der h.M., s. *Kilian* 1979, 123; *Bockelmann* 1985, 702; wie die jetzige Rspr. *Schmidt-Beck* 1994, 37 ff.; *Hermeler* 2000, 24; Staudinger-*Richardi*, vor §§ 611 ff. Rn. 1273; Richtlinien der *BÄK*, DÄ 1996, A-2809, 2810; gegen die Einordnung der Dokumentationspflicht als materielle Verbindlichkeit des Leistungs-

Beim Verhältnis zwischen ärztlicher Schweigepflicht und Dokumentationspflicht einerseits und dem Datenschutzrecht andererseits ist nach den Schritten der Datenverwendung zu unterscheiden. Die Datenerhebung ist notwendiger Bestandteil des Behandlungsvertrags, da eine Behandlung ohne die Kenntnis von Gesundheitsinformationen nicht möglich ist.[228] Gleichzeitig beinhaltet der Vertrag typischerweise nur eine Befugnis zur Erhebung von Daten, die zur Aufgabenerfüllung, das heißt zur Durchführung der Behandlung, erforderlich sind.[229]

Die Dokumentationspflicht gestattet (und gebietet) dem Leistungserbringer die dauerhafte Speicherung der Daten zu Dokumentationszwecken, ohne dass der Versicherte das Recht hat, seine Einwilligung zur Speicherung – wie sonst im Datenschutzrecht üblich – auf bestimmte Angaben zu beschränken oder eine selektive Löschung von Daten zu verlangen.[230] Die Dokumentation ist aber auf solche Daten beschränkt, die der Versicherte freiwillig offenbart hat; eine Ausforschung gegen seinen Willen ist unzulässig.

Hinsichtlich einer Übermittlung von Daten an Dritte haben ärztliche Schweigepflicht und Datenschutzrecht dieselbe Schutzrichtung.[231] § 1 Abs. 3 Satz 2 BDSG bestimmt, dass Schweigepflichten durch das Bundesdatenschutzgesetz „unberührt" bleiben. Das Gesetz wird also nicht unanwendbar, sondern verändert lediglich nicht den Inhalt dieser Pflichten.[232] Beide sind somit nebeneinander anwendbar. Dies kann in Einzelfällen aufgrund der unterschiedlichen Tatbestandsvoraussetzungen von Bedeutung sein. Die wichtigsten Unterschiede sind, dass einerseits § 203 StGB nicht jede Datenverarbeitung erfasst, da die Norm nur Geheimnisträger verpflichtet und ein „Offenbaren" verlangt, und andererseits im Rahmen des Strafrechts auch mündliche und mutmaßliche Einwilligungen möglich sind.[233]

2.2.2.2 Neue Bestimmungen im GKV-Modernisierungsgesetz

Das am 1. Januar 2004 in Kraft getretene GKV-Modernisierungsgesetz sieht in § 291a SGB V die Einführung einer elektronischen Gesundheitskarte bis spätestens zum 1. Januar 2006 vor.[234] Diese wird für gesetzlich Versicherte verpflichtend sein. Für privat Versicherte gibt es bislang keine Bestimmungen. Angedacht ist, dass die privaten Krankenkassen entsprechende Vereinbarungen in ihre Verträge aufnehmen.[235] Im Unterschied zur bisherigen Rechtslage werden nach § 264 Abs. 4 Satz 2 SGB V auch nicht versicherte Empfänger laufender Leistungen zum Lebensunterhalt und von Hilfe in besonderen Lebenslagen eine

---

erbringers gegenüber dem Versicherten *Wendt* 2001, 296 ff.; gegen einen isoliert einklagbaren Erfüllungsanspruch *Inhester*, NJW 1995, 685, 688; *Schmidt-Beck*, NJW 1991, 2335, 2336.

227 S. die Bsp. bei *Hermeler* 2000, 24.; *Wendt* 2001, 43 ff.; *Laskaridis* 2003, 28; vgl. auch unten 6.3.1.

228 Roßnagel-*Schirmer*, Kap. 7.12, Rn. 27.

229 *Wehrmann/Wellbrock*, CR 1997, 754, 755.

230 Ein Patient hat keinen Anspruch gegen den Arzt, eine Diagnose zu widerrufen (BGH, NJW 1989, 774 f.). Wird deren Richtigkeit bestritten, so kann lediglich eine Sperrung verlangt werden, vgl. *Kilian*, NJW 1992, 2313, 2315.

231 *Hermeler* 2000, 84.

232 OLG Bremen, NJW 1992, 757 f.; Simitis-*Walz*, § 1 Rn. 174, 185 f. m.w.N.; *Körner-Dammann*, NJW 1992, 729, 730; Roßnagel-*Schirmer*, Kap. 7.12, Rn. 26; *Bongen/Kremer*, NJW 1990, 2911, 2913; *Hermeler* 2000, 84 f.; *Meier* 2003, 30 f. m.w.N. (mit dem zutreffenden Argument, dass bei einer Unanwendbarkeit des BDSG die Regelungen in §§ 13 Abs. 2 Nr. 7, 28 Abs. 7 BDSG überflüssig wären); a.A. Roßnagel-*Abel*, Kap. 7.11, Rn. 8 ff.

233 S. *Hermeler* 2000, 85 ff.; die Unterschiede werden vermengt durch *Fuest* 1999, 56.

234 Vgl. zum Folgenden bereits *Hornung* 2004a, 226 ff.; zum Stand des Projekts vgl. oben 2.1.2.

235 Vgl. die Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten *Sehling*, *Storm*, *Widmann-Mauz*, weiterer Abgeordneter und der Fraktion der CDU/CSU v. 30.3.2004, BT-Drs 15/2810, 1; s.a. *BITKOM/VDAP/VHitG/ZVEI* 2003, 3.

Gesundheitskarte erhalten. Damit sollen diese Personen bei der Inanspruchnahme von Gesundheitsleistungen den Versicherten verfahrensmäßig gleichgestellt werden.[236] Außerdem wird die Durchführung des Abrechnungsverfahrens und die Anwendung von Steuerungsinstrumenten wie der Wirtschaftlichkeitsprüfung nach § 106 SGB V ermöglicht. Die Krankenkassen sind nach § 284 Abs. 1 Nr. 2 SGB V ermächtigt, Sozialdaten zu erheben und zu speichern, soweit sie für die Ausstellung der elektronischen Gesundheitskarte erforderlich sind.[237]

Inhalt und Funktionsweise der Karte sind gegenüber der bisherigen Krankenversichertenkarte wesentlich erweitert.[238] Während diese nach § 291 Abs. 1 Satz 3 SGB V a.F. lediglich zum Nachweis der Berechtigung zur Inanspruchnahme von Leistungen im Rahmen der vertragsärztlichen Versorgung sowie für die Abrechnung mit den Leistungserbringern verwendet werden durfte, gliedern sich die Funktionen der elektronischen Gesundheitskarte in einen verpflichtenden und einen freiwilligen Bereich.[239] Die entsprechenden Regelungen in § 291a Abs. 2 und 3 SGB V verdrängen die allgemeinen datenschutzrechtlichen Normen: Bei den verpflichtenden Anwendungen (§ 291a Abs. 2 Satz 1 SGB V) ist entgegen § 4 Abs. 1 BDSG kein Raum für Erweiterungen aufgrund einer Einwilligung. Im Rahmen von § 291a Abs. 3 SGB V (freiwillige Anwendungen) gibt es besondere Verfahrensvorschriften für die Einwilligung, sodass lediglich ergänzend auf § 4a BDSG zurückgegriffen werden kann.

Die drei verpflichtenden Teile (§ 291a Abs. 2 Satz 1 SGB V) sind die Speicherung der Versicherungsstammdaten, die Übermittlung des elektronischen Rezepts sowie die Ablage des Berechtigungsnachweises zur Inanspruchnahme von Leistungen in den Mitgliedstaaten der Europäischen Union. Gegenüber der früheren Rechtslage (§ 292 Abs. 2 SGB V a.F.) werden die Stammdaten um Angaben zum Geschlecht und zum Zuzahlungsstatus, sowie um ein aufgedrucktes Lichtbild[240] erweitert. Das elektronische Rezept soll einen medienbruchfreien Transport von der Ausstellung bis zur Abrechnung ermöglichen. Der Gesetzgeber hat keine Entscheidung darüber getroffen, ob das Rezept auf der Karte selbst gespeichert werden oder diese lediglich einen entsprechenden Verweis (Pointer) enthalten wird. Denkbar ist auch eine Wahlmöglichkeit des Patienten.[241] Der europäische Berechtigungsnachweis wird – entsprechend den Plänen der Europäischen Kommission – in der ersten Kartengeneration lediglich als Sichtausweis auf der Rückseite der Gesundheitskarte aufgedruckt werden, weil andernfalls jeder Leistungserbringer in Europa kurzfristig über ein entsprechendes Lesegerät verfügen müsste.[242] Der Aufdruck wird eine standardisierte Aufnahme der Daten bei Auslandsreisen ermöglichen und so (vergleichbar der Einführung

236 S. die Gesetzesbegründung, BT-Drs. 15/1525, 141.

237 Die Datenerhebung für die Gesundheitskarte war im ersten Entwurf noch übersehen worden und wurde erst im gemeinsamen Entwurf von SPD, CDU/CSU und BÜNDNIS 90/DIE GRÜNEN (BT-Drs. 15/1525) eingefügt.

238 S. bereits *Hornung* 2004a, 226 ff.; s.a. *Hornung/Goetz/Goldschmidt*, WI 2005, 171 ff.

239 Die Funktionen entsprechen den Vorstellungen der Telematik-Expertise der Wirtschaft, s. *BITKOM/VDAP/VHitG/ZVEI* 2003, 4.

240 Hiervon wurden durch das Gesetz zur Vereinfachung der Verwaltungsverfahren im Sozialrecht (BGBl. I 2005, 818) in § 291 Abs. 2 Satz 1, letzter Halbsatz SGB V Ausnahmen für Versicherte bis zum 16. Lebensjahr sowie Versicherte, deren Mitwirkung bei der Erstellung des Lichtbildes nicht möglich ist, gemacht.

241 So der Vorschlag von *BITKOM/VDAP/VHitG/ZVEI* 2003, 13, 36; s. zum elektronischen Rezept aus technischer und organisatorischer Sicht *ATG/GVG* 2001a, insbes. 21 ff., 34 ff.; seit dem 11.3.2005 liegt eine erste Spezifikation vor, s. *Struif* (Ed.) 2005, Teil 3; zur Frage des Speicherorts unten 4.2.3.3.

242 Diskutiert wird, den Nachweis auch in der ersten Kartengeneration zusätzlich elektronisch zu speichern.

der gegenwärtigen Krankenversichertenkarte in Deutschland) zu erheblichen Einspareffekten führen.

§ 291a Abs. 3 Satz 1 SGB V enthält demgegenüber diejenigen Anwendungen, zu deren Ausführung die Gesundheitskarte zwar in der Lage sein muss, über deren Einsatz der Inhaber jedoch selbst entscheiden kann. Im Einzelnen sind dies die medizinischen Notfalldaten,[243] der elektronische Arztbrief (Befunde, Diagnosen, Therapieempfehlungen und Behandlungsberichte für einen einrichtungsübergreifenden Behandlungsfall),[244] die elektronische Patientenakte (ebendiese Angaben, jedoch fallübergreifend),[245] die Daten zur Prüfung der Arzneimitteltherapiesicherheit,[246] vom Patienten selbst zur Verfügung gestellte Daten[247] und Daten über in Anspruch genommene Leistungen und deren vorläufige Kosten für den Versicherten nach § 305 Abs. 2 SGB V („Patientenquittung"). Die Einwilligung bedarf nach § 4a Abs. 1 Satz 3 BDSG der Schriftform.[248] Sie ist nach § 291a Abs. 3 Satz 4 SGB V auf der Karte zu dokumentieren,[249] jederzeit widerruflich und auf einzelne Anwendungen beschränkbar.

§ 291a Abs. 3 Satz 2 SGB V normiert eine umfassende Aufklärungspflicht der Krankenkasse, die in verständlicher Form zu erfolgen hat. Sie dient der Transparenz der Kartenstruktur und der auf ihr ablaufenden Datenverarbeitungsprozesse. Es ist zweifelhaft, ob sich die Pflicht lediglich auf die freiwilligen Anwendungen nach § 291a Abs. 3 Satz 1 SGB V oder auch auf die verpflichtenden Applikationen nach § 291a Abs. 2 Satz 1 SGB V bezieht. Die Gesetzessystematik spricht für die erste Lösung, da die Pflicht im Zusammenhang des § 291a Abs. 3 SGB V geregelt wurde und sich die folgenden Sätze dieses Absatzes eindeutig nur auf seinen ersten Satz beziehen. Andererseits ist der Wortlaut von § 291a Abs. 3 Satz 2 SGB V gerade nicht auf die freiwilligen Anwendungen begrenzt. Auch das teleologische Argument spricht für ein weites Verständnis der Norm, da nur so dem verfassungsrechtlichen Transparenzgedanken[250] genügt werden kann. Schließlich lässt sich das systematische Argument auch umkehren: Gerade weil die Folgesätze in § 291a Abs. 3

---

243 In Anlehnung an den international standardisierten Notfalldatensatz ISO 21549-3. Das Gesetz enthält keine Angaben darüber, welche Informationen im Einzelnen gemeint sind. *BITKOM/VDAP/VHitG/ZVEI* 2003, 46 schlagen vor, über den Standard hinaus Erweiterungen um patientenspezifische Notfalldaten zuzulassen. Hierfür kämen chronische Organleiden, Dialyseinformationen, Allergien und Arzneimittelunverträglichkeiten in Betracht, vgl. *Weichert*, DuD 2004, 391, 396.

244 S. zur Umsetzbarkeit *ATG/GVG* 2001b; der Arztbrief wird von deutschen Ärzten etwa 80 Mio. mal pro Jahr ausgestellt, s. *Grätzel v. Grätz* 2004c, 130.

245 Zur Rechtslage bezüglich des elektronischen Arztbriefs und der elektronischen Patientenakte vor Inkrafttreten des GKV-Modernisierungsgesetztes s. *Dierks/Nitz/Grau* 2003, 109 f., 113 ff.; s.a. *ATG/GVG* 2005; vgl. zu den Chancen und Anwendungsszenarien der elektronischen Patientenakte auch *Grätzel v. Grätz* 2004c, 62 ff.

246 Dieser Terminus wurde durch das Gesetz zur Vereinfachung der Verwaltungsverfahren im Sozialrecht (s.o. Fn. 240) an die Stelle von „Arzneimitteldokumentation" gesetzt und soll neben den verordneten Arzneimitteln auch akute und chronische Erkrankungen umfassen, s. die Gesetzesbegründung, BT-Drs. 15/4228, 28.

247 Die Gesetzesbegründung nennt beispielhaft Verlaufsprotokolle bei chronischen Krankheiten und Patientenverfügungen (BT-Drs. 15/1525, 145), die Begründung des ersten Entwurfs auch den Organspendeausweis (BT-Drs. 15/1170, 123).

248 Jede andere Form der Einwilligung wäre angesichts der Komplexität der Funktionsweise der Gesundheitskarte nicht angemessen; ebenso *Weichert*, DuD 2004, 391, 399; a.A. *Schneider* 2004, 153.

249 Nach *Weichert*, DuD 2004, 391, 400 soll es „entgegen dem Wortlaut" nicht erforderlich sein, die Einwilligung auf der Karte selbst zu dokumentieren. Das angeführte Argument, eine Dokumentation auf einem Server sei ebenso geeignet, ist zwar inhaltlich einleuchtend, jedoch nicht geeignet, sich gegen den eindeutigen Wortlaut der Norm durchzusetzen. Es handelt sich in der Sache um einen Vorschlag de lege ferenda.

250 Dazu unten 4.2.1.2.5.

SGB V sich ausdrücklich nur auf die Anwendungen aus § 291a Abs. 3 Satz 1 SGB V beziehen, muss die Aufklärungspflicht nach § 291a Abs. 3 Satz 2 SGB V auch für die verpflichtenden Anwendungen aus § 291a Abs. 2 Satz 1 SGB V gemeint sein. Die Vorschrift ist damit in diesem Sinne weit zu verstehen und umfasst freiwillige und verpflichtende Anwendungen.

§ 291a Abs. 4 Satz 1 Nr. 1 SGB V gestattet den Zugriff auf das elektronische Rezept für Ärzte, Zahnärzte, Apotheker, Apothekerassistenten, Pharmazieingenieure und Apothekenassistenten. Darüber hinaus können Personen auf die Daten zugreifen, die bei den Genannten oder in einem Krankenhaus als berufsmäßige Gehilfen oder zur Vorbereitung auf den Beruf tätig sind, jedoch nur im Rahmen ihrer Tätigkeiten und unter Aufsicht eines Leistungserbringers.[251] Schließlich werden auch sonstige Erbringer ärztlich verordneter Leistungen auf die Rezepte zugreifen können.

Die Funktionen nach § 291a Abs. 3 Satz 1 SGB V (außer den Daten nach § 305 Abs. 2 SGB V) durften in der ursprünglichen Gesetzesfassung gemäß § 291a Abs. 4 Satz 1 Nr. 2 SGB V a.F. ausschließlich Ärzten, Zahnärzten und Apothekern, die Notfalldaten auch anderen Angehörigen eines Heilberufes zugänglich sein. Der Kreis der Zugriffsberechtigten wurde mit dem Gesetz zur Vereinfachung der Verwaltungsverfahren im Sozialrecht[252] erheblich ausgeweitet und umfasst nunmehr neben Psychotherapeuten auch das in § 291a Abs. 4 Satz 1 Nr. 1 SGB V genannte Apothekenpersonal und berufsmäßige Gehilfen. Die Versicherten selbst haben nach § 291a Abs. 4 Satz 2 SGB V das Recht, auf alle Daten „zuzugreifen". Hinter diesem missverständlichen Wortlaut verbirgt sich allerdings lediglich ein datenschutzrechtliches Auskunftsrecht.[253]

§ 291a Abs. 5 Satz 1 SGB V bindet jedes Erheben, Verarbeiten und Nutzen von Daten der freiwilligen Funktionen mittels der Gesundheitskarte an das Einverständnis des Versicherten. Das betrifft sowohl den lesenden wie den schreibenden Zugriff. § 291a Abs. 5 Satz 2 SGB V verlangt (mit Ausnahme der Notfalldaten) eine technische Absicherung der Autorisierung des Versicherten im Einzelfall. Dies kann zum Beispiel mittels PIN oder biometrischen Merkmals erfolgen.[254] Im Umkehrschluss folgt daraus, dass für die verpflichtenden Funktionen – Zugriff auf Stammdaten, elektronisches Rezept und einen zu Beginn oder künftig elektronisch gespeicherten europäischen Berechtigungsnachweis – eine derartige Autorisierung nicht erforderlich ist.[255] Allerdings ist nach § 291a Abs. 5 Satz 3, 1. Halbsatz SGB V der Zugriff auf die Daten des elektronischen Rezepts und der freiwilligen Funktionen nach § 291a Abs. 3 Satz 1 SGB V in jedem Einzelfall an den Einsatz eines elektronischen Heilberufsausweises gekoppelt (im Fall des Rezepts auch eines anderen Berufsausweises), der über eine Möglichkeit zur sicheren Authentifizierung und „über eine qualifizierte elektronische Signatur verfügen"[256] muss.[257]

---

251 Diese Bestimmung wurde durch das Gesetz zur Vereinfachung der Verwaltungsverfahren im Sozialrecht (BGBl. I 2005, 818) eingeführt. Ausweislich der Gesetzesbegründung (BT-Drs. 15/4228, 28) soll damit keine Aufsicht durch technische Verfahren gemeint sein.

252 S.o. Fn. 251.

253 S. ausführlich unten 4.3.7.3.

254 Beide Verfahren werden nicht im Gesetz, wohl aber in der Begründung angesprochen, s. BT-Drs. 15/1525, 145. Nach dem gegenwärtigen Stand der Technik stellt die PIN allerdings – zumindest für die erste Kartengeneration – das einzige praktikable Verfahren dar; s. näher unten 6.3.3.2.

255 Dies ist in Teilbereichen datenschutzrechtlich problematisch, s.u. 4.2.3.4.2.1.

256 Gemeint ist die Möglichkeit zur Erstellung qualifizierter elektronischer Signaturen. Diese sind nach § 2 Nr. 1 SigG Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch mit ihnen verknüpft sind und die zur Authentifizierung dienen; s.a. unten 5.1. Der Heilberufsausweis „verfügt" deshalb nicht über eine solche Signatur, sondern stellt sie her; vgl. zur technischen Funktionsweise unten 2.3.2.

Von dieser Koppelung gibt es Ausnahmen. Der Zugriff auf die selbst zur Verfügung gestellten Daten ist nach § 291a Abs. 5 Satz 3, 1. Halbsatz SGB V auch mit einer eigenen Signaturkarte des Versicherten möglich, wenn diese über die Möglichkeit zur Erstellung qualifizierter elektronischer Signaturen verfügt.[258] § 291a Abs. 5 Satz 4 SGB V lässt einen Zugriff durch Hilfspersonen, die nicht Inhaber eines eigenen elektronischen Heilberufsausweises sind, im Umfang ihrer Berechtigung dann zu, wenn sie durch einen Träger eines solchen Ausweises oder eines entsprechenden Berufsausweises autorisiert wurden und der Zugriff und die Autorisierung „nachweisbar elektronisch protokolliert werden".

Der Zugriff auf das elektronische Rezept kann schließlich entsprechend § 291a Abs. 5 Satz 4 SGB V vom Versicherten auch selbst freigeschaltet werden. Damit soll ein Einlösen im Ausland ermöglicht werden.[259] Wenn das Rezept zwingend den Einsatz eines elektronischen Heilberufsausweises erfordern würde, wäre eine Verwendung nicht möglich, falls der Leistungserbringer des Gastlandes nicht über einen solchen verfügt oder dieser nicht mit der elektronischen Gesundheitskarte interoperabel ist. Die verschiedenen Prototypen für elektronische Heilberufsausweise in den Ländern der Europäischen Union sind zwar weitgehend miteinander kompatibel. Es dürfte jedoch noch etliche Jahre dauern, bis sämtliche Leistungserbringer in allen Mitgliedstaaten mit entsprechenden Karten ausgerüstet sind.

§ 291a Abs. 6 Satz 1 SGB V normiert ein besonderes Löschungsrecht. Auf Verlangen des Versicherten sind sowohl die Daten des elektronischen Rezepts wie die der freiwilligen Anwendungen nach § 291a Abs. 3 Satz 1 SGB V zu löschen.[260] Es ist fraglich, ob diese Befugnis ohne Einschränkungen gilt. Nach dem Wortlaut ist ein Löschungsverlangen nicht an einen (nach § 291a Abs. 3 Satz 4 SGB V jederzeit möglichen) Widerruf der Einwilligung in die Anwendung gebunden. Danach könnte der Versicherte die Löschung der Daten der jeweiligen Anwendung verlangen, die Anwendung selbst jedoch weiterlaufen lassen. Für die überwiegende Zahl der freiwilligen Applikationen bestehen hiergegen auch keine Bedenken. Soweit sie jedoch (wie insbesondere die Daten zur Prüfung der Arzneimitteltherapiesicherheit) auf eine fortlaufende und vollständige Datenspeicherung angewiesen sind, kann der Versicherte die Anwendung nicht weiterführen. Hier ist es vielmehr zulässig, die Einwilligungserklärung so zu formulieren, dass der Versicherte die Gesundheitskarte bei jedem Behandlungs- und Medikationsvorgang vorlegen muss.[261] Auch in diesem Fall bleibt die gesetzliche Befugnis zum Widerruf der Einwilligung nach § 291a Abs. 3 Satz 4 SGB V erhalten. Da die Anwendung nach Löschung der bisher erhobenen Daten sinnlos wird, muss man deshalb insoweit in einem Löschungsverlangen zugleich diesen Widerruf sehen.

Des Weiteren sind nach § 291a Abs. 6 Satz 2 SGB V mindestens die letzten 50 Zugriffe auf die Daten der Gesundheitskarte zu Zwecken der Datenschutzkontrolle zu protokollieren. § 291a Abs. 6 Satz 3 SGB V bestimmt, dass die Protokolldaten nur für diesen Zweck eingesetzt werden dürfen. Sie sind außerdem nach § 291a Abs. 6 Satz 4 SGB V durch

---

257 Die Koppelung des Datenzugriffs an einen elektronischen Heilberufsausweis wurde auch gefordert von *BITKOM/VDAP/VHitG/ZVEI* 2003, 47 ff.

258 Unzutreffend *Weichert*, DuD 2004, 391, 395, wonach dies für alle Daten der freiwilligen Anwendungen gelten soll.

259 S. die Gesetzesbegründung, BT-Drs. 15/1525, 145; zur grundfreiheitlichen Inanspruchnahme von Gesundheitsleistungen im europäischen Binnenmarkt s. EuGH, Rs. C-385/99 – Müller-Fauré und van Riet, EuR 2003, 628 (dazu *Nowak*, EuR 2003, 644 ff.) und Rs. C-56/01 – Patricia Inizan, Entscheidung v. 23.10. 2003 (abrufbar unter http://curia.eu.int/jurisp/cgi-bin/form.pl?lang=de).

260 Hierauf ist beim Einzug der Gesundheitskarte nach Beendigung des Versicherungsverhältnisses ausdrücklich erneut hinzuweisen, s. § 291 Abs. 4 Satz 6 SGB V.

261 S. ausführlich unten 4.2.3.1.

geeignete Vorkehrungen gegen zweckfremde Verwendung und sonstigen Missbrauch zu schützen.

§ 291a Abs. 7 Satz 1 SGB V verpflichtet die Spitzenverbände der Krankenkassen, die Kassenärztliche Bundesvereinigung, die Kassenzahnärztliche Bundesvereinigung, die Bundesärztekammer, die Bundeszahnärztekammer, die Deutsche Krankenhausgesellschaft sowie die für die Wahrnehmung der wirtschaftlichen Interessen gebildete maßgebliche Spitzenorganisation der Apotheker auf Bundesebene zur Schaffung der für die Einführung und Anwendung der elektronischen Gesundheitskarte, insbesondere des elektronischen Rezepts und der elektronischen Patientenakte, erforderlichen interoperablen und kompatiblen Informations-, Kommunikations- und Sicherheitsinfrastruktur (Telematikinfrastruktur).[262] Diese Aufgabe wird durch eine Gesellschaft für Telematik wahrgenommen. § 291b SGB V regelt die innere Organisation dieser Gesellschaft, die gemäß § 291b Abs. 2 Nr. 2 SGB V Entscheidungen mit der Mehrheit von 67 Prozent der sich aus den Geschäftsanteilen ergebenden Stimmen fällen kann. Ihre Beschlüsse zur Telematikinfrastruktur sind dem Bundesministerium für Gesundheit und Soziale Sicherung vorzulegen, das insoweit eine Rechtsaufsicht ausübt und zuvor dem Bundesbeauftragten für den Datenschutz Gelegenheit zur Stellungnahme zu geben hat (§ 291b Abs. 4 Satz 1 SGB V). Kommt keine Vereinbarung zustande, wird das Ministerium dazu ermächtigt, im Benehmen mit den zuständigen obersten Landesbehörden die notwendigen Inhalte der Telematikinfrastruktur durch Rechtsverordnung ohne Zustimmung des Bundesrates festzulegen.

§ 291a Abs. 8 SGB V enthält weitere Schutzvorschriften für die Daten, die im Zusammenhang mit der elektronischen Gesundheitskarte verarbeitet werden. Nach § 291a Abs. 8 Satz 1 SGB V ist es verboten, vom Versicherten zu verlangen, den Zugriff auf das elektronische Rezept und alle Daten nach § 291a Abs. 3 Satz 1 SGB V anderen als berechtigten Personen oder zu anderen Zwecken als denen der Versorgung und Abrechnung zu gestatten oder über eine solche Gestattung eine Vereinbarung zu treffen. Aus der Bewirkung oder Verweigerung des Zugriffs dürfen gemäß § 291a Abs. 8 Satz 2 SGB V weder Vornoch Nachteile erwachsen. Verstöße gegen § 291a Abs. 8 Satz 1 (nicht jedoch Satz 2) SGB V werden nach § 307 Abs. 1 SGB V als Ordnungswidrigkeit geahndet.[263] Dort ist auch die Höhe des Bußgeldes bestimmt. Gegenüber dem normalen Maximalbetrag von 2.500 Euro kann ein Verstoß gegen § 291a Abs. 8 Satz 1 SGB V mit einem Bußgeld von bis zu 50.0000 Euro geahndet werden.

Während § 307 Abs. 1 SGB V damit Einflussnahmen auf den Versicherten als Ordnungswidrigkeit normiert, ist ein Zugriff auf die auf oder mittels der Gesundheitskarte gespeicherten Daten, der entgegen den Zugriffsbefugnissen des § 291a Abs. 4 Satz 1 SGB V erfolgt, nach § 307a Abs. 1 SGB V eine Straftat. Sie ist mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bedroht. Bei einem Handeln gegen Entgelt oder in Bereicherungs- oder Schädigungsabsicht kann nach § 307a Abs. 2 SGB V eine Freiheitsstrafe von bis zu drei Jahren verhängt werden. Die Tat ist Antragsdelikt. In Anlehnung an die allgemeine Strafvorschrift des § 44 Abs. 2 BDSG[264] ist nicht nur der Betroffene, sondern auch der

262 Die Spitzenverbände der Krankenkassen können überdies Regeln für die Weiternutzung der Gesundheitskarte bei einem Kassenwechsel vereinbaren (§ 291 Abs. 4 Satz 2 SGB V). Die Norm wurde durch das Gesetz zur Vereinfachung der Verwaltungsverfahren im Sozialrecht (s.o. Fn. 251) eingeführt. Es ist bislang unklar, ob sich die Krankenkassen auf ein solches Vorgehen einigen können, das insbesondere eine einheitliche äußere Gestaltung erfordern würde.

263 Eine parallele Vorschrift wurde durch das GKV-Modernisierungsgesetz in § 57 Abs. 4 des Zweiten Gesetzes über die Krankenversicherung der Landwirte eingeführt.

264 Dazu Simitis-*Dammann*, § 44 Rn. 1 ff.; Hoeren/Sieber-*Sieber*, Kap. 19, Rn. 543 ff.

Bundesbeauftragte für den Datenschutz oder die jeweils zuständige Aufsichtsbehörde antragsbefugt.

Nach dem Gesetz (§ 291a Abs. 2 Satz 2 und Abs. 3 Satz 5 SGB V) findet außerdem die Transparenzregel des § 6c BDSG in den Fällen der § 291a Abs. 2 Satz 1 und Abs. 3 Satz 1 SGB V Anwendung. Schließlich wird der Beschlagnahmeschutz in § 97 Abs. 2 StPO ausgeweitet. Dieser erstreckt sich nunmehr auch auf die Gesundheitskarte selbst sowie auf Dienstleister, die für Ärzte, Zahnärzte, Psychotherapeuten, Apotheker und Hebammen personenbezogene Daten erheben, verarbeiten oder nutzen.[265]

2.3 Technische Grundlagen

Betrachtet man die rechtliche Zulässigkeit technischer Anwendungen in der Einführungsphase oder rechtliche Anforderungen an ihre Gestaltung (im Rahmen der zeitlich vorgelagerten Entwicklung), so ist ein möglichst präzises Verständnis der jeweiligen technischen Funktionsweise unumgänglich. Nur dann können die rechtlichen Auswirkungen und Probleme erfasst und Alternativen aufgezeigt werden. Deshalb erläutert dieses Kapitel Verfahren und Systeme, die für die weitere Untersuchung relevant sind. Grundbegriffe der Informationstechnologie werden dabei vorausgesetzt.

2.3.1 Chipkarten und ihre Einsatzumgebungen

Chipkarten finden in immer mehr Lebensbereichen Verwendung und sind aus dem Alltag längst nicht mehr wegzudenken. Den Anfang der Entwicklung bildete im Jahre 1950 die erste Vollplastik-Kreditkarte des Diners-Club.[266] Lange Zeit wurde als Material für den Kartenkörper ausschließlich PVC eingesetzt. Für langlebige Anwendungen findet heute allerdings überwiegend Polykarbonat Verwendung.[267] Zur Sicherung der Kartenoberfläche gibt es eine Vielzahl graphischer Sicherheitstechniken.[268]

Das erste Patent für eine Karte mit Chip wurde von den Deutschen *Dethloff* und *Gröttrup* im Jahre 1968 eingereicht.[269] Mit dem Fortschreiten der Mikroelektronik wurde es in den 70er Jahren des vorigen Jahrhunderts möglich, Chips mit minimalem Raumbedarf herzustellen und schließlich auch auf Plastikkarten zu installieren. Die Leistungsfähigkeit der Chips nahm mit der Zeit zu, und ein Ende dieses Prozesses ist gegenwärtig nicht absehbar.[270] Heutzutage kann man zwischen einfachen Speicherchips und Mikroprozessorkarten unterscheiden.[271] Die in dieser Arbeit behandelten Chipkarten fallen durchweg in die letzte Kategorie, da die verwendeten Daten (staatliche Identifikationsdaten, medizinische Angaben, Signaturschlüssel) eine Speicher- und Verarbeitungstechnik erfordern, die höchsten Sicherheitsanforderungen genügt.

---

265 Dies wurde auch von der Telematik-Expertise gefordert, s. *BITKOM/VDAP/VHitG/ZVEI* 2003, 73; näher unten 4.2.3.5.2.

266 *Rankl/Effing* 2002, 2. Die Karte wurde zuerst in den USA ausgegeben.

267 Weitere Möglichkeiten beim Material sind ABS und PET, s. *Rankl/Effing* 2002, 42 ff.

268 Bspw. Guillochen, Mikroschrift, Irisverläufe, Sicherheitsdruck, kopierresistente Druckfarben, optisch variable Merkmale, Lasergravur, optisch variable Farben, Laser-Kippbild, UV-Druck und Hologramm; s. *Rankl/Effing* 2002, 35 ff.

269 Die Erteilung erfolgte im Jahre 1969 (Patent DE 19 45 777 C3).

270 Der begrenzende Faktor ist hier insbesondere die Größe des Chips, die von den Herstellern auf maximal 25 mm^2 festgelegt ist. Dies resultiert allerdings nicht aus den Eigenschaften des Chips, sondern aus dem maximalen Biegeradius der Karte.

271 *Rankl/Effing* 2002, 7 ff., 20 ff., weitere Unterteilungen bei *Janke* 2002, 204; *Kruse/Peuckert*, DuD 1995, 142, 143. Beispiele für Speicherkarten sind die Krankenversichertenkarte der gesetzlichen Krankenversicherung und die vorbezahlte Telephonkarte.

Der technische Aufbau eines Smartcard-Chips besteht in diesem Fall aus mehreren Komponenten, wobei sich Prozessor, Speicher, Schnittstellen und weitere Peripherie unterscheiden lassen. Der Prozessor steuert, initiiert und überwacht alle Aktivitäten des Chips.[272] Darunter fallen das Signieren und Verschlüsseln von Dokumenten, die Bearbeitung biometrischer Daten und die Freigabe von gespeicherten Daten über die Schnittstelle. Außerdem ermöglicht die Verwendung von Prozessoren Prüfvorgänge im Rahmen von Authentisierungsprozessen gegenüber der Karte. In einem geschützten Speicherbereich des Chips werden hierzu Referenzdaten hinterlegt (etwa eine PIN oder ein biometrisches Merkmal) und durch den Prozessor mit den Daten verglichen, die zur Authentisierung von der Peripherie übermittelt werden. Als Betriebssystem wird auf den Prozessoren mittlerweile ganz überwiegend die offene Plattform Java Card verwendet.[273] Neuere Prozessorentypen haben eine Speicherbreite von 32 Bit. Das ist insbesondere dann erforderlich, wenn der Chip mit rechenintensiven Betriebssystemen wie Java arbeitet und größere Speicher (ab 64 Kilobyte) verwaltet werden sollen.[274]

Die Speichertechnologien eines Mikrochips lassen sich in nichtflüchtige und flüchtige Speicher unterteilen.[275] Nichtflüchtige Speicher bewahren auch nach einem kontrollierten oder unkontrollierten Abschalten der Versorgungsspannung zuverlässig die gespeicherten Daten auf. Einige dieser Systeme sind überdies so konstruiert, dass sie bei der Herstellung unabänderlich auf einen logischen Wert festgelegt werden können. Der Grund für den Einsatz verschiedener Speichertechnologien ist die Verwendung unterschiedlicher Datenkategorien auf dem Chip. So enthalten einige Arbeitsbereiche Daten, die niemals die Karte verlassen dürfen. Ein Beispiel hierfür ist der geheime Schlüssel im Signaturverfahren. Bei Identifikationsdaten ist zwar ein Auslesevorgang zulässig (oder erwünscht), sie dürfen jedoch auf der Karte nicht veränderbar sein. Gleiches gilt für das Betriebssystem. Einige Speicherbereiche müssen dagegen bei unterschiedlichen Rechenoperationen als Arbeits- und Zwischenspeicher immer wieder neu belegt werden. Die Verwendung unterschiedlicher Speicher ermöglicht hier bereits auf der Basis der Hardware eine grundsätzlich ausdifferenzierte Zugriffsverwaltung.

Der flüchtige Speicher eines Chips wird durch den RAM gebildet, dessen Speicherzellen aus je sechs Transistoren bestehen.[276] Er wird zur Zwischenspeicherung bei der Bedienung der Schnittstellen und der Verschlüsselungseinheit sowie als Arbeitsspeicher des Prozessors eingesetzt. Nichtflüchtige Speicherzellen basieren demgegenüber derzeit auf der ROM- und EEPROM-Technologie. ROM-Speicherzellen[277] sind kompakt und verfügen über sehr kurze Zugriffszeiten. In ihnen wird regelmäßig das Betriebssystem gespeichert. Eine spätere Änderung des Speicherinhalts ist nicht möglich. EEPROM-Zellen[278] können demgegenüber durch eine erhöhte Spannung einzeln gelöscht und programmiert werden. Eine ähnliche Technik findet bei der Flash-EEPROM Speicherzelle Verwen-

272 Näher *Rankl/Effing* 2002, 67 ff.

273 S. zu den Gründen *Stocker* 1998, 227 ff.; *Rankl/Effing* 2002, 237 ff., insbes. 308 ff. (dort auch zu Alternativen). Offene Plattformen haben den Vorteil, dass unabhängig vom Betriebssystemhersteller die Möglichkeit für Dritte besteht, Anwendungen und Programme auf die Chipkarte laden zu können.

274 S. *Rankl/Effing* 2002, 69.

275 S. *Vedder/Weikmann* 1998, 5 f.

276 RAM steht für Random Access Memory. Es gibt auch dynamische RAMs aus einem Transistor und einem kleinen Kondensator. Diese werden jedoch nicht in Chipkarten eingesetzt.

277 Read Only Memory; näher *Rankl/Effing* 2002, 73 f.; *Volpe/Volpe* 1996, 41 ff.

278 Electrical Erasable and Programmable Read Only Memory; s. *Rankl/Effing* 2002, 74 ff.; *Volpe/Volpe* 1996, 44 ff.

dung.[279] Diese wird noch nicht standardmäßig in Chipkarten eingesetzt, eröffnet aber perspektivisch Vorteile bezüglich einer kompakten Realisierung. Weitere nichtflüchtige Speichertechnologien befinden sich in der Entwicklungsphase.[280]

Schnittstellen verbinden die Chipkarte mit der Außenwelt. Hierzu gibt es grundsätzlich zwei Möglichkeiten, nämlich kontaktbehaftete (oder -orientierte) und kontaktlose Schnittstellen.[281] Bei der kontaktbehafteten Variante verfügt der Chip über einen Bereich, an dem er zur Datenübermittlung über eine galvanische Verbindung in direkten Kontakt zu einem Lesegerät tritt. Dazu müssen die Kontakte an einer genormten Stelle liegen.[282] Bei der kontaktlosen Variante verfügt die Karte dagegen über eine Sende- und Empfangsantenne. Der Kartenchip wird durch induktive Kopplung angesteuert und so sowohl die Energieversorgung als auch die Datenübertragung bewerkstelligt.[283] Man spricht deshalb auch von einem Radio Frequency (RF)-Chip. Je nach der Komplexität des Chips kann die Datenübertragung aus einer mehr oder weniger großen Entfernung geschehen. Während einfache Speicherkarten aus mehreren Metern Entfernung ausgelesen werden können, benötigen Mikroprozessoren regelmäßig Entfernungen von ungefähr zehn Zentimetern.[284]

Beide Schnittstellen haben spezifische Vorteile. Wird mit Kontakten gearbeitet, so sind Angriffe auf die Schnittstelle erheblich schwieriger, insbesondere dann, wenn die Lesegeräte einem hohen Sicherheitsstandard genügen. Deshalb können Identifikationsdaten wie die PIN unverschlüsselt an die Karte übertragen werden. Dies ist bei einer kontaktlosen Antenne nicht möglich, weil hier Daten durch die Luft übertragen werden und dabei heimlich mitgeschnitten werden können. Auf der anderen Seite sind die Übertragungsgeschwindigkeiten dieser Technik deutlich höher. Außerdem werden Abnutzungen vermieden, die nach einer Vielzahl von Steckzyklen oder durch Verschmutzung an den Kontakten der Schnittstelle auftreten können.[285]

Eine dritte Möglichkeit ist schließlich, den Chip auf der Karte mit beiden Schnittstellen auszurüsten. Man spricht dann von einem Dual-Interface-Chip.[286] Der Einsatz solcher Chips bietet sich insbesondere bei Multiapplikationskarten an, die in bestimmten Einsatzbereichen auf eine schnelle Datenübertragung, in anderen auf eine hohe Sicherheit angewiesen sind.

Chipkarten interagieren über diese Schnittstellen auf vielfältige Art mit ihrer Umwelt. Bisweilen arbeiten dabei Peripheriekomponenten unter der Kontrolle der Karte. Dies ist dann sinnvoll, wenn der Kartenchip bestimmte Aufgaben aufgrund seiner begrenzten Leistungsfähigkeit nicht übernehmen kann. Beispiele hierfür sind aufwendige Verschlüsse-

279 S. *Rankl/Effing* 2002, 79 ff. Diese benötigt nur etwa die Hälfte der Zellengröße einer normalen EEPROM-Zelle, s. ebd., 72.

280 Dabei geht es um ferroelektrische und magnetorestriktive Speicher sowie um Antifuse-Technologie, s. *Küblbeck/Heusinger/Ronge*, in: Reichl/Roßnagel/Müller 2005, 185 f. Auch diese Systeme streben schnellere Zugriffszeiten und weniger Platzbedarf an.

281 S. *Rankl/Effing* 2002, 91 ff.; *Volpe/Volpe* 1996, 27 ff., 95 ff.

282 Diese sind in der ISO/IEC 7816 standardisiert. Die Verbindung besteht danach aus sechs oder acht Kontakten an festgelegten Stellen, die zum Schutz vor Korrosion in der Regel vergoldet sind.

283 Näher *Rankl/Effing* 2002, 95 ff. Diese „passive" Variante ist bislang die Regel. Möglich ist auch ein „aktiver" RF-Chip, der über eine eigene Stromversorgung verfügt. Aufgrund der langen Laufzeiten von Chipkartenausweisen ist dies jedoch im hier betrachteten Zusammenhang unrealistisch; s. für Reisedokumente *ICAO* 2004b, 10.

284 S. zu den verschiedenen Standards unten 6.1.2.

285 *Rankl/Effing* 2002, 23; *Volpe/Volpe* 1996, 95.

286 *Rankl/Effing* 2002, 9.

lungsaufgaben, die Generierung von Zufallszahlen zur Schlüsselerzeugung sowie (zumindest bislang noch) die Extraktion von Templates aus biometrischen Rohdaten.[287]

Regelmäßig ist die Aufgabenverteilung allerdings umgekehrt: Das Lesegerät sendet eine Anfrage an die Chipkarte, die diese (gegebenenfalls nach vorheriger gegenseitiger Authentisierung) bearbeitet. Dazu verfügt das Terminal über einen eigenen Prozessor und Speicher, bei kontaktbehafteten Systemen auch über eine Kontaktierungseinheit. Terminals werden je nach Sicherheitsstufe in unterschiedliche Klassen unterteilt.[288] Kontaktorientierte Varianten können durch eine Reihe technischer Maßnahmen sehr hohen Sicherheitsanforderungen genügen.[289] Diese treiben jedoch den Preis des Lesegeräts in die Höhe, sodass sie für private Nutzungen kaum geeignet sind.

Chipkarten werden mittlerweile in immer mehr Lebensbereichen eingesetzt.[290] Die Telephonkarte[291] und die Versicherungskarte der gesetzlichen Krankenversicherung[292] gehören zu den ältesten Anwendungen. Einen zahlenmäßig immer größeren Anteil machen mittlerweile die Karten im GSM- und Mobilfunkbereich aus.[293] Auch EC-Karten verfügen schon seit einigen Jahren über einen Chip.[294] Dieser wird zwar bislang nur für die Geldkartenfunktion eingesetzt,[295] soll aber in Zukunft auch für den Zugang zu Geldautomaten Verwendung finden. In diesem Zusammenhang werden aller Voraussicht nach auch Kreditkarten einen Chip erhalten.[296] Neuere Entwicklungen finden sich etwa im Bereich von Signaturkarten,[297] elektronischen Mautsystemen,[298] Studentenkarten,[299] Kundenkarten,[300]

---

287 Hierzu unten 2.3.3.2.

288 Nach der Spezifikation des deutschen Zentralen Kreditausschusses verfügt ein Terminal der Klasse 1 über eine Kontaktiereinheit und Schnittstelle zu anderen Systemen, Klasse 2 darüber hinaus über Funktionselemente und Display, Klasse 3 über die Elemente der Klasse 2 und eine Tastatur, Klasse 4 über die Elemente der Klasse 3 und ein Sicherheitsmodul; ausführlich zu Chipkarten-Terminals *Rankl/Effing* 2002, 661 ff.; s.a. *Ullrich/Seßler*, in: Reichl/Roßnagel/Müller 2005, 281 ff.

289 Etwa elektrisch angetriebene Kontaktiereinheit, Sicherheitsgehäuse, autarkes Arbeiten auch bei abgeklemmter Spannungsversorgung und „Shutter" am Kartenschlitz, um mit der Karte verbundene Kabel oder Drähte abzuschneiden, die aus der Kontaktiereinheit führen; s.a. unten 6.1.1.

290 Das gegenwärtige und potentielle Anwendungsfeld kontaktloser RFID-Chips ohne standardisierten Kartenkörper ist noch größer und kaum zu überblicken. Sie dürften in Zukunft in vielen Logistikprozessen Anwendung finden und dazu in einer Reihe von Alltagsgegenständen implementiert werden. Die datenschutzrechtliche Problematik dieser Chips liegt außerhalb des Themas dieser Arbeit; vgl. etwa *FoeBuD e.V. et. al.* 2003; *Müller*, DuD 2004, 215 ff. m.w.N.; *ders./Handy*, DuD 2004, 655 ff.; *Hansen/Wiese*, DuD 2004, 109; *Gräfin von Westerholt/Döring*, CR 2004, 710 ff.; *Art. 29 DPWP* 2005; zur strafprozessualen Perspektive vgl. *Eisenberg/Puschke/Singelnstein*, ZRP 2005, 9, 10 ff.; aus technischer Sicht s. *Kelter/Wittmann*, DuD 2004, 331 ff.; für eine allgemeine Bewertung der Chancen und Risiken *BSI* 2004.

291 Erste Feldversuche wurden in Frankreich bereits 1984 durchgeführt. Telephonkarten kommen heute in über 50 Ländern weltweit zum Einsatz, s. *Rankl/Effing* 2002, 4.

292 Näher *Rankl/Effing* 2002, 822 ff.; *Volpe/Volpe* 1996, 110 ff. und oben 2.1.2.

293 Hierzu *Rankl/Effing* 2002, 731 ff.

294 Die Spezifikation hierzu wurde 1996 vom Zentralen Kreditausschuss herausgegeben, vgl. *Rankl/Effing* 2002, 5; s.a. *Zitzelsberger/Hogen*, DuD 202, 271 ff.; *Volpe/Volpe* 1996, 13 ff.

295 Dazu *Kruse/Peuckert*, DuD 1995, 142, 148.

296 Hierzu existieren bereits seit 1996 internationale Spezifikationen (EMV); näher *Schürer* 2004, 107 ff.

297 S. aus technischer Sicht *Rankl/Effing* 2002, 831 ff. und unten 2.3.2.

298 *Rankl/Effing* 2002, 827 ff.

299 Etwa in Gießen, Freiburg und Worms. Die Karten werden zur Online-Abwicklung von Rückmeldungen, Prüfungsverwaltung und Dokumentübermittlung eingesetzt; s. *Kraus/Wagemann*, V&M 2002, 297 ff.; *Ptascheck* 1998, 192 ff. Die Karte in Gießen hat einen kontaktorientierten (zum Signieren) und einen kontaktlosen (für Bibliothek, Mensa und Cafeteria) Chip und wird mit einem Leser und Software zum subventionierten Preis abgegeben. Der universitätsinterne Zertifizierungsdiensteanbieter arbeitet nicht entsprechend dem SigG, s. näher http://www.uni-giessen.de/chipkarte/. Das Chipkar-

Fahrkartenausweisen[301] und Kurkarten.[302] Weitere Beispiele sind Identitätskarten für Waffenbesitzer,[303] Betriebs- und Dienstausweise,[304] Identifikationskarten im Pay-TV[305] und Fußball-Saisonkarten.[306] Zur Zutritts-, Zugangs- und Zugriffskontrolle werden Chipkarten schon seit Jahren eingesetzt.[307] Bei Personalausweisen gibt es aus dem Ausland mittlerweile eine Reihe von Anwendungsbeispielen.[308] Gleiches gilt für Führerscheine.

Digitale Ausweise in Form von „Bürgerkarten" werden auch in anderen Bereichen erprobt. So haben die Städte Ulm, Bremerhafen und Passau zusammen mit der Bundesdruckerei GmbH und dem Zertifizierungsdiensteanbieter D-Trust seit dem Dezember des Jahres 2002 ungefähr 500 Bürgerkarten ausgegeben.[309] Diese enthalten die Signaturfunktion sowie die Meldedaten des Besitzers. Mit diesen Karten und ihren Funktionen können städtische Dienstleistungen und privatwirtschaftliche Angebote genutzt werden.

Die Darstellung dieser Arbeit beschränkt sich ganz überwiegend auf den digitalen Personalausweis und die elektronische Gesundheitskarte. Eine Vielzahl der hierbei auftretenden Probleme und Anforderungen ergeben sich jedoch auch bei anderen Chipkarten. Da es sich bei Personalausweis und Gesundheitskarte um Prozessorchipkarten handeln wird, gilt das allerdings für reine Speichermedien, Magnetkarten oder Karten mit 2D-Barcodes nur mit erheblichen Einschränkungen.[310]

2.3.2 Verschlüsselung, elektronische Signatur und Authentisierung

Kryptographische Verfahren dienen – zumindest im Ausgangspunkt[311] – der Herstellung von Vertraulichkeit bei der Übermittlung von Daten.[312] Herkömmliche Verschlüsselungsmethoden existieren bereits seit Jahrtausenden. Die moderne Datenverarbeitung

---

tenprojekt an der TU Berlin wurde dagegen im Frühjahr 2004 eingestellt, vgl. http://www.heise.de/newsticker/meldung/48537.

300 Diese sind bislang i.a.R. keine Chipkarten. Es gibt aber Ansätze in diese Richtung, z.B. die Karte von Starbucks in Taiwan, s. http://www.cardtechnology.com/cgi-bin/readstory.pl?story=20040609CTDN394.xml.

301 Insbesondere in Nordrhein-Westfalen, s. http://www.heise.de/newsticker/meldung/41988; aus datenschutzrechtlicher Sicht *Die Landesbeauftragte für Datenschutz Nordrhein-Westfalen* 2003, 72 f.; die Industrie plant für die Zukunft eine bundesweit einsetzbare Nahverkehrskarte, s. OMNICARD-newsletter März 2005; ein entsprechendes Projekt wurde im März 2005 in Irland gestartet, vgl. http://europa.eu.int/idabc/en/document/4093/194.

302 Bspw. die „ostseecard", der das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein im Herbst 2004 das datenschutzrechtliche Auditzeichen verliehen hat, vgl. http://www.datenschutzzentrum.de/audit/kurzgutachten/a0409/ostseecard_gutachten.pdf.

303 Bspw. in Honduras, s. http://www.cardtechnology.com/cgi-bin/readstory.pl?story=20040210CTDN386.xml.

304 In einem Pilotprojekt für einen digitalen Dienstausweis des Bundes wurde bspw. eine Karte mit zwei Chips getestet: ein kontaktloser für Zutrittskontrollen und Zeiterfassung und ein kontaktorientierter für kryptographische Grundfunktionen (elektronische Signatur, Verschlüsselung, Authentifizierung) und die Zugangskontrolle zu Rechnern und Servern; s. näher *Bundesdruckerei* 2002.

305 S. *Volpe/Volpe* 1996, 17 ff.

306 Z.B. bei den Vereinen PSV Eindhoven, Real Madrid und 1. FC Köln; vgl. http://futurezone.orf.at/futurezone.orf?read=detail&id=259851; OMNICARD-newsletter März 2004.

307 Vgl. z.B. *Kruse/Peuckert*, DuD 1995, 142, 146 f.

308 Hierzu ausführlich unten 3.

309 *Roßnagel*, in: Reichl/Roßnagel/Müller 2005, 9.

310 Das bedeutet allerdings nicht, dass derartige Karten keine datenschutzrechtlichen Probleme aufwerfen würden; zu (nicht mit einem Chip ausgestatteten) Kundenkarten s. insoweit *ULD* 2003b.

311 Zur Verwendung im Rahmen der elektronischen Signatur s. weiter unten in diesem Abschnitt.

312 S. ausführlich *Buchmann* 2001; *Schneier* 1996 (insbes. 1 ff.); *Beutelspacher/Schwenk/Wolfenstetter* 2004; zum historischen Hintergrund vgl. *Singh* 1999, 15 ff. et passim.

schafft jedoch Möglichkeiten für die weite Verbreitung kryptographischer Verfahren, die – immer bezogen auf den gegenwärtigen und absehbaren zukünftigen Stand der Technik – auch von solchen Angreifern nicht überwunden werden können, die hoch motiviert und mit modernster Informationstechnik ausgestattet sind.

Verschlüsselungsverfahren lassen sich in zwei Gruppen einteilen, nämlich symmetrische und asymmetrische. Symmetrische Verfahren verwenden zum Ver- und Entschlüsseln denselben Schlüssel, wobei die Funktion zum Entschlüsseln umgekehrt wird.[313] Der bekannteste und am meisten verbreitete Mechanismus hierzu ist der Data Encryption Standard (DES).[314] Symmetrische Verfahren setzen voraus, dass beide Partner des Kommunikationsprozesses über den Verschlüsselungsalgorithmus verfügen. Das ist in dauerhaften Kommunikationsverbindungen im Regelfall unproblematisch. Wenn jedoch immer mehr Rechtsgeschäfte und Handlungen des täglichen Lebens in offene Netze verlagert werden, stößt die symmetrische Verschlüsselung auf unüberwindbare Hindernisse. Es ist praktisch nicht durchführbar, zunächst mit jedem Kommunikationspartner auf herkömmliche (und mit Sicherheitsrisiken behaftete) Art und Weise einen Schlüssel auszutauschen, um danach mit ihm gesichert interagieren zu können. Das gilt umso mehr, als der Gegenüber sich an einem beliebigen Ort weltweit befinden kann. Verfahren, die im netzbasierten Rechts- und Geschäftsverkehr eingesetzt werden, müssen auch bei einem Erstkontakt zweier Partner eine gesicherte Kommunikation ohne zeitliche Verzögerung gewährleisten.

Diese Probleme können durch die Verwendung asymmetrischer Verschlüsselungsverfahren gelöst werden.[315] Hierbei werden zum Ver- und Entschlüsseln zwei verschiedene Schlüssel verwendet, die jedoch mathematisch untrennbar miteinander verbunden sind.[316] Der Verschlüsselungsschlüssel wird allgemein öffentlich gemacht oder an jeden beliebigen Kommunikationspartner übermittelt. Man spricht deshalb von einer Public-Key-Infrastructure (PKI). Der Entschlüsselungsschlüssel wird demgegenüber geheim gehalten, etwa auf dem Computer des Schlüsselinhabers oder – sicherer – auf einer Chipkarte.

Die Sicherheit asymmetrische Verfahren beruht darauf, dass dem Inhaber des geheimen Schlüssels schnelle mathematische Verfahren zur Verfügung stehen, während ein möglicher Angreifer auf langsame Verfahren angewiesen ist.[317] Das bedeutet, dass die Verschlüsselungsverfahren zwar nicht unüberwindlich sind. Es ist jedoch möglich, die Schlüssellänge so zu dimensionieren, dass nach dem jeweils gegenwärtigen Stand der Technik auch Angreifer, die auf Großrechenanlagen oder zusammengeschaltete Rechnernetze zurückgreifen können, nicht in der Lage sind, einen Angriff erfolgreich zu führen. Die

313 S. *Rankl/Effing* 2002, 183 ff.; *Schneier* 1996, 32 ff.; *Beutelspacher/Schwenk/Wolfenstetter* 2004, 6 ff. Einfachstes Beispiel: beim Verschlüsseln wird jeder Buchstabe durch den im Alphabet nachfolgenden ersetzt. Zum Entschlüsseln wird demzufolge jeder Buchstabe des verschlüsselten Texts durch den im Alphabet vorausgehenden ersetzt.

314 Dieser wurde von IBM und dem US National Bureau of Standards entwickelt, s. näher *Rankl/Effing* 2002, 183 ff.; *Buchmann* 2001, 95 ff.; *Tanenbaum* 2003, 795 ff.; *Volpe/Volpe* 1996, 58 ff.

315 S. *Schneier* 1996, 37 ff.; *Rankl/Effing* 2002, 191 ff.; *Tanenbaum* 2003, 811 ff.; *Beutelspacher/Schwenk/Wolfenstetter* 2004, 10 ff.; *Singh* 1999, 324 ff.; *Buchmann* 2001, 113 ff.; *Bauer* 1997, 176 ff.

316 Hierfür existiert kein triviales Beispiel. Mathematisch lautet z.B. die Funktion des RSA-Verfahrens zum Verschlüsseln $y = x^e \bmod n$, die zum Entschlüsseln $x = y^d \bmod n$, mit $n = p \cdot q$, wobei x der Klartext, y der Schlüsseltext, e der öffentliche Schlüssel, d der geheime Schlüssel, n der öffentliche Modulus und p und q geheime Primzahlen sind. Anschaulich lässt sich das System mit dem Versand von geöffneten Vorhängeschlössern vergleichen: Jedermann ist in der Lage, eine Kiste sicher zu verschließen, nur der Sender kann diese jedoch wieder öffnen.

317 Bspw. bei der Verwendung zweier Primzahlen: Während es sehr leicht ist, diese miteinander zu multiplizieren, ist eine Faktorisierung des Resultats (das per definitionem nur durch sich selbst, eins und die beiden Primzahlen teilbar ist) sehr zeitaufwendig. Dieses Problem ist die Grundlage des RSA-Verfahrens.

heute gängigsten asymmetrischen Verfahren sind RSA,[318] das Verfahren von *El Gamal*[319] und die Verwendung elliptischer Kurven.[320]

Allerdings haben asymmetrische Verfahren auch Nachteile. Der größte ist der enorme Rechenaufwand, der beim Ver- und Entschlüsseln entsteht. Symmetrische Verfahren arbeiten demgegenüber erheblich schneller: das asymmetrische RSA benötigt zum Ver- und Entschlüsseln etwa 1000mal mehr Zeit als das symmetrische DES.[321] In der Praxis werden deshalb beide Prozesse im Rahmen eines so genannten Hybridverfahrens miteinander kombiniert.[322] Ein solches Verschlüsselungsverfahren wird regelmäßig auch als Funktionalität von Signaturkarten angeboten. In diesem Fall generiert die Chipkarte des Absenders zunächst einen einmaligen, symmetrischen Schlüssel (Session-Key). Mit diesem wird das Dokument in der Peripherie des Absenders verschlüsselt. Danach wird der verwendete symmetrische Schlüssel mit dem öffentlichen asymmetrischen Schlüssel des Erklärungsempfängers verschlüsselt. Das Ergebnis dieses Prozesses wird zusammen mit dem symmetrisch verschlüsselten Dokument an den Empfänger versandt. Dieser entschlüsselt mit seinem geheimen asymmetrischen Schlüssel auf seiner Chipkarte den verwendeten symmetrischen Schlüssel und hiernach mit diesem in seiner Peripherie das empfangene Dokument.

Durch dieses System wird sichergestellt, dass einerseits der geheime Schlüssel des Empfängers nie die Signaturkarte verlässt und so nur er zum Entschlüsseln in der Lage ist („Ende-zu-Ende-Verschlüsselung"), und andererseits das System auch dann funktioniert, wenn größere Dokumente verschickt werden, die nicht mehr selbst auf der Karte ver- und entschlüsselt werden könnten. Überdies ist es mit Hybridverfahren auch sehr leicht möglich, ein Dokument verschlüsselt an mehrere Empfänger zu versenden. Statt jedes Mal das gesamte Dokument mit einer Vielzahl von öffentlichen Schlüsseln verschlüsseln zu müssen, kann einfach der verwendete symmetrische Schlüssel mehrfach asymmetrisch verschlüsselt und dem immer gleich symmetrisch verschlüsselten Dokument beigefügt werden.

Asymmetrische Verschlüsselungsverfahren können auch dazu verwendet werden, ein Dokument elektronisch zu signieren.[323] Im Unterschied zur Verschlüsselung verwendet der Absender dabei nicht den öffentlichen Schlüssel seines Gegenübers, sondern seinen eigenen geheimen Schlüssel. Zunächst wird das Dokument durch einen allgemein bekannten (Hash-)Algorithmus stark verkürzt.[324] Das Ergebnis, der so genannte Hash-Wert, wird

---

318 Benannt nach seinen Erfindern *Rivest*, *Shamir* und *Adleman*, s. *Rivest/Shamir/Adleman*, C.ACM 1978, 120 ff. RSA wird z.B. für das (nicht chipkartenbasierte und ohne Zertifikate verwendete) Verschlüsselungsverfahren PGP verwendet; s. näher *Bourseau/Fox/Thiel*, DuD 2002, 84 ff.; *Buchmann* 2001, 115 ff.; *Beutelspacher/Schwenk/Wolfenstetter* 2004, 19 ff.

319 *ElGamal*, IEEE.IT 1985, 469 ff. Dieses Verfahren beruht auf dem Problem des diskreten Logarithmus; s.a. *Beutelspacher/Schwenk/Wolfenstetter* 2004, 124 ff.; *Buchmann* 2001, 133 ff.

320 S. *Menezes* 1993.

321 *Bauer* 1997, 192.

322 S. *Schneier* 1996, 38 ff.; *Buchmann* 2001, 114.

323 Zur Funktionsweise der Signaturerstellung s. *Struif*, GMD-Spiegel 1998, 38; *Hammer*, DuD 1993, 636 ff., *provet/GMD* 1994, 54 ff.; *Schneier* 1996, 41 ff., 97 ff.; *Roßnagel* 1996, 17 ff.; RMD-*Roßnagel*, Einl. SigG Rn. 11 ff. m.w.N.; *Borges* 2003, 54 ff.; *Gassen* 2003, 22 ff.; *Rapp* 2002, 8 ff. m.w.N.; *Rankl/Effing* 2002, 229 ff. (dort wird allerdings der Einsatz der Schlüssel zum Ver- und Entschlüsseln des Hash-Werts verwechselt); zur Diskussion vor 1989 vgl. die Nachweise bei *Roßnagel/Wedde/Hammer/Pordesch* 1990, 241.

324 Das ist zur Funktionsweise des Verfahrens nicht unbedingt erforderlich, entspricht aber dem Vorgehen bei Smartcards, da andernfalls eine Verschlüsselung auf der Karte nicht möglich wäre. Hash-Funktionen sind, vereinfacht ausgedrückt, Einwegfunktionen zur Komprimierung von Daten. Der Hash-Wert hat eine feste Datenstruktur. Wichtigste Bedingung für seine Berechnung ist, dass trotz der

mittels des geheimen Schlüssels verschlüsselt. Der verschlüsselte Text (dies ist die elektronische Signatur) und das Dokument werden an den Empfänger versandt. Dieser entschlüsselt zunächst mittels des öffentlichen Schlüssels des Absenders die Signatur und bestimmt danach erneut den Hash-Wert des empfangenen Dokuments. Stimmen diese beiden Werte überein, so ist zweierlei nachgewiesen: Derjenige, der über den geheimen Schlüssel verfügt, hat die elektronische Signatur zu diesem Dokument erstellt, und das Dokument wurde während des Übertragungsvorgangs nicht verändert. Ersteres nennt man Authentizität, letzteres Integrität der versandten Erklärung.[325] Elektronische Signaturverfahren erzeugen demgegenüber keine Vertraulichkeit hinsichtlich des signierten Dokuments. Möchte der Absender auch dessen Inhalt geheim halten, so muss er parallel ein Verschlüsselungsverfahren einsetzen.[326]

Authentizität und Integrität der Erklärung können allerdings nur dann gewährleistet werden, wenn zwei Unsicherheitsfaktoren minimiert werden. Zunächst muss der geheime Schlüssel in der ausschließlichen Verfügungsgewalt einer einzelnen Person stehen. Der genannte Prüfvorgang beweist lediglich, dass eine elektronische Signatur mit einem bestimmten geheimen Schlüssel angefertigt wurde, nicht aber, wer diesen Verarbeitungsmechanismus ausgelöst hat. Dieses Problem kann dadurch verkleinert werden, dass der geheime Schlüssel auf einer Chipkarte gespeichert wird, diese nie verlässt und nur mittels einer PIN des Inhabers aktiviert werden kann.[327] Der andere Unsicherheitsfaktor besteht darin, dass weder aus der Signatur noch aus dem öffentlichen Schlüssel die Person des Absenders erkennbar wird. Wenn elektronische Signaturen auf der Basis asymmetrischer Verschlüsselungsverfahren im elektronischen Rechtsverkehr als Funktionsäquivalent zur Unterschrift eingesetzt werden, so ist deshalb ein Schlüsselmanagement erforderlich.[328]

Der hierzu vom Signaturgesetz eingeschlagene Weg ist der des Einsatzes eines vertrauenswürdigen Dritten (Zertifizierungsdiensteanbieter), der die Zugehörigkeit eines öffentlichen Schlüssels zu einer Person in einem Zertifikat bestätigt. Der Anbieter überzeugt sich von der Identität des Antragstellers, ordnet ihm ein Schlüsselpaar zu und stellt das Zertifikat aus. Dieses ist selbst eine Datei, die vom Zertifizierungsdiensteanbieter mit seinem eigenen geheimen Schlüssel elektronisch signiert wird.[329] Der Zertifizierungsdiensteanbieter führt außerdem eine Liste mit allen Zertifikaten, die von jedermann mit Hilfe einer OCSP (Online Certificate Service Protocol)-Abfrage abgerufen werden kann. Wenn ein Zertifikat (beispielsweise weil der geheime Schlüssel nicht mehr sicher oder dem Signatur-

---

Komprimierung jede Änderung auch nur eines einzelnen Bits des Gesamtdokuments eine Veränderung des Hash-Werts zur Folge haben muss, s. *Raßmann*, CR 1998, 36, 38; *Merz* 1999, 128; näher *Dobbertin*, DuD 1997, 82 ff.; *Rankl/Effing* 2002, 210 ff.

325 Aus mathematischer Sicht ist die Signatur damit ein Mittel zur Sicherung von Daten. Inwieweit an diese Funktion und ihre Sicherheit rechtliche Folgen (Formäquivalenz, Beweiswert) geknüpft werden, ist demgegenüber eine Frage der Zuschreibung; s. hierzu unten 5.1.1.

326 Bei der Normierung der elektronischen Signatur im SigG wurde diese Frage bewusst nicht geregelt, um eine Vermischung dieser Diskussion mit der um die Zulässigkeit von Verschlüsselungsverfahren (Kryptokontroverse) zu vermeiden, s. RMD-*Roßnagel*, Einl. SigG Rn. 13 m.w.N.

327 Auch in diesem Fall besteht allerdings noch keine Bindung an eine Person, sondern „nur" an die Legitimationsmechanismen Besitz und Wissen, die beide übertragbar sind; zur Frage, ob diesem Problem mit Hilfe biometrischer Verfahren beigekommen werden kann, s.u. 5.2.6.

328 S. *Hammer/Schneider* 1995, 15 ff.; RMD-*Roßnagel*, Einl. SigG, Rn. 19 ff.; *Grimm* 2003, 93 f.; *Rankl/Effing* 2002, 232 ff.; *Borges* 2003, 59 ff.; *Tanenbaum* 2003, 825 ff.; Manssen-*Skrobotz*, § 1 SigG Rn. 28 ff.; *Buchmann* 2001, 209 ff.

329 Die Zertifikate bestimmter (akkreditierter) Anbieter werden im selben Verfahren durch eine staatliche Wurzelzertifizierungsinstanz, die Regulierungsbehörde für Telekommunikation und Post, ausgestellt. Andere Anbieter müssen hierauf verzichten und sich selbst ein Zertifikat ausstellen, dessen Vertrauen dann nur aus sich selbst wirkt; zu den verschiedenen Signaturstufen s.u. 5.1.1.

schlüssel-Inhaber abhanden gekommen ist) seine Gültigkeit verliert, so wird es in der Liste als gesperrt vermerkt.

Symmetrische und asymmetrische Verschlüsselungsverfahren werden auch zur elektronischen Authentisierung,[330] also zur Überprüfung der Identität und Authentizität eines Kommunikationspartners, eingesetzt. Ein solches Verfahren kann etwa den Zugang zu Rechnern und Netzen (Single Sign On), den Zugriff auf Daten oder den Zutritt zu Räumen sichern. Im Chipkartenbereich basieren Authentisierungsverfahren durchgängig auf dem so genannten Challenge-Response-Verfahren.[331] Ein Kommunikationspartner sendet seinem Gegenüber eine Anfrage (Challenge). Dieser verschlüsselt die Anfrage und sendet das verschlüsselte Ergebnis zurück (Response). Beim ursprünglichen Absender wird die Antwort wieder entschlüsselt und mit der ursprünglichen Anfrage verglichen. Stimmen beide überein, war die Authentisierung erfolgreich. Aus Sicherheitsgründen kann bei jeder Anfrage ein anderer Inhalt verwendet werden; man spricht dann von dynamischen Verfahren. Authentisierungsverfahren können ein- oder mehrseitig sein, je nachdem, ob sich nur ein oder alle Partner eines Kommunikationsprozesses authentisieren.[332] Ein Beispiel hierfür ist die gegenseitige Authentisierung von Chipkarte und Lesegerät, bevor sensible Daten ausgetauscht werden.

Das beschriebene Verfahren funktioniert sowohl mit symmetrischer als auch mit asymmetrischer Verschlüsselung. Die symmetrische Variante weist jedoch die bereits beschriebenen Nachteile auf, sodass in der Praxis mit asymmetrischen Schlüsseln gearbeitet wird. Auf Signaturkarten sind diese vom Signaturschlüssel verschieden, da vermieden werden soll, dass dem Signaturschlüssel-Inhaber eine Anfrage untergeschoben wird, die eine rechtsgeschäftliche Erklärung beinhaltet, und dieser sie versehentlich signiert. Asymmetrische Authentisierungsverfahren setzen überdies wie Signaturverfahren ein Zertifikatsmanagement voraus.

2.3.3 Biometrische Verfahren

Biometrische Verfahren werden vielfach als eine der entscheidenden Sicherheitstechnologien der Zukunft angesehen.[333] In kleineren Hochsicherheitsumgebungen finden sie bereits seit längerer Zeit Verwendung. Seit den Anschlägen auf das World Trade Center und das Pentagon am 11. September 2001 wird im Rahmen der nachfolgenden Diskussion um die Verbesserungsfähigkeit von Identifizierungsmaßnahmen in sicherheitsrelevanten Bereichen auch eine weitreichende Einführung von Biometrie vorangetrieben. Hierzu gehört die Aufnahme biometrischer Merkmale in Reisepapiere. Diese ist zwar bislang noch nicht erfolgt, die entsprechenden Entscheidungen sind jedoch – insbesondere auf Druck der USA – längst gefallen.[334] Programme zur Implementierung biometrischer Daten in Aus-

330 Statt Authentisierung wird auch der Begriff Authentifizierung (oder Authentifikation) verwendet. Die Bedeutung ist identisch, s. *Rankl/Effing* 2002, 219. „Authentifikation" hat allerdings einen mehr personalen Bezug. Dementsprechend wird in dieser Arbeit z.B. von biometrischer Authentifikation gesprochen.

331 S. *Rankl/Effing* 2002, 219 ff.; *Volpe/Volpe* 1996, 108 f.; *Kruse/Peuckert*, DuD 1995, 142, 145 f.; *Buchmann* 2001, 201 ff.

332 Eine gegenseitige Authentisierung kann durch zwei einseitige Vorgänge oder ein ineinander verflochtenes System vorgenommen werden, s. näher *Rankl/Effing* 2002, 223.

333 Für eine generelle Einführung in die Biometrie und die damit verbundenen Rechtsfragen s. *Albrecht* 2003a; *Hornung*, KJ 2004, 344 ff.

334 Das gilt für die politische Ebene durchgängig. Tlw. bestehen auch formelle Beschlüsse, s. z.B. für die EU-Reisepässe die Verordnung (EG) Nr. 2252 v. 13. Dezember 2004; dazu unten 3.1.2.

weispapiere sind auch der Hauptgrund für die optimistischen Wachstumsprognosen der Branche.[335]

Beim Einsatz von Biometrie ist die Verwendung von Chipkarten nicht unbedingt erforderlich, bietet jedoch eine Reihe von Vorteilen wegen der dezentralen Verfügbarkeit der Daten und der (datenschutzrechtlich positiv zu bewertenden) Kontrollierbarkeit durch den Karteninhaber. Bislang ist eine grundsätzliche Entscheidung des Gesetzgebers zur Verwendung von Biometrie nur beim Reisepass und beim digitalen Personalausweis gefallen.[336] Es ist jedoch wahrscheinlich, dass diese auch bei anderen Chipkartenausweisen eingesetzt werden wird. Im Folgenden werden Begriffe und Arbeitsweisen biometrischer Verfahren erläutert. Daran schließt sich ein Überblick über Chancen und Problemfelder an.

2.3.3.1 Begriffsbestimmungen und Arten biometrischer Verfahren

Das Wort Biometrie setzt sich zusammen aus den griechischen Bestandteilen bios (Leben) und metron (Maß) und bezeichnet damit die Körpermessung an Lebewesen.[337] Im Zusammenhang mit den hier relevanten Verfahren wird der Begriff allerdings in einem engeren Sinn verstanden. Biometrie ist danach die automatisierte Messung von natürlichen, hoch charakteristischen, physiologischen oder verhaltenstypischen Merkmalen von Menschen zum Zweck der Unterscheidung von anderen Personen.[338]

Beim Einsatz von Biometrie kann man zwischen biometrischen Verfahren und Systemen unterscheiden. Erstere sind Mechanismen zur Erkennung eines Menschen anhand seiner biometrischen Merkmale, letztere Gesamtsysteme zur biometrischen Authentifizierung und schließen damit kombinierte Hard- und Softwarebestandteile ein, die (mindestens) ein biometrisches Verfahren beinhalten.[339] Wird beim Einsatze von Chipkartenausweisen Biometrie verwendet, so sind die Karten somit biometrische Systeme oder Teile von diesen.

Anfänge wissenschaftlicher Beschäftigung mit der Biometrie finden sich am Ende des 19. Jahrhunderts.[340] Sie befasste sich zunächst fast ausschließlich – kriminalistisch – mit dem Fingerabdruck. Dieses Merkmal ist heute auch in anderen Anwendungsbereichen national und international am weitesten verbreitet.[341] Verwendet werden daneben vor allem das Gesicht, die Iris, die Handgeometrie, die Stimme und die Handschrift. Der Gesichtserkennung wird hierbei zunehmend Potential eingeräumt. Sie wird von der International

---

335 Die *International Biometric Group* prognostizierte für 2004 ein Wachstum von 68 % auf dann 1,2 Mrd. USD weltweit, vgl. http://www.cardtechnology.com/cgi-bin/readstory.pl?story=20040107CTDN979.xml; s.a. *Teegler*, in: Reichl/Roßnagel/Müller 2005, 284 ff.; *Woodward/Orlans/Higgins* 2003, XXIII f. m.w.N.; *Rejman-Greene* 2003b, 25 ff., 34 ff.; http://www.heise.de/newsticker/meldung/48560; sehr positiv auch die generelle Einschätzung von *JRC/IPTS* 2005; s. allgemein zu den ökonomischen Aspekten der Biometrie ebd., 80 ff.

336 S.o. 2.2.1.2.

337 *Nolde* 2002, 20; *Golembiewski/Probst* 2003, 9.

338 *Behrens/Roth* 2001a, 1 f.; *TAB* 2002, 9. Die Begriffsbestimmung in der Literatur ist zwar nicht einheitlich (s. etwa *Donnerhacke*, DuD 1999, 151; *Behrens/Roth*, DuD 2000, 327 f.; *dies.* 2001b, 9 f.; *Nanavati/Thieme/Nanavati* 2002, 9 f.; *Woodward/Orlans/Higgins* 2003, 27; *Albrecht* 2003a, 31 m.w.N.; *OECD* 2004, 10 f. m.w.N.), in der Sache besteht jedoch weitgehend Einigkeit.

339 *Albrecht* 2003a, 31 m.w.N.

340 Zur historischen Entwicklung s. *Albrecht* 2003a, 33 f. m.w.N. (dort auch zu noch älteren Wurzeln; hierzu auch *Breitenstein* 2002, 35; *Ashbourn* 2000, 1 ff.); *Woodward/Orlans/Higgins* 2003, 25 f.; 45 ff.; *Weichert*, CR 1997, 369 f.; zur forensischen Verwendung des Fingerabdrucks s. *Frank*, Die Polizei 2004, 336 ff.

341 *Woodward/Orlans/Higgins* (2003, 213) nennen einen Marktanteil von einem Drittel.

Civil Aviation Organisation (ICAO) für den Einsatz in Reisedokumenten favorisiert[342] und als erstes Merkmal in die Reisepässe der EU-Mitgliedstaaten eingeführt werden.[343] Erprobt wird daneben die Erkennung von Bewegungsmustern beim Gang, Hand- und Gesichtsvenenmustern, Geruch, Tippverhalten und Ohrmuschelkontur.[344] Auf eine Darstellung der spezifischen Funktionsweise und Besonderheiten der jeweiligen Verfahren wird an dieser Stelle verzichtet.[345] Soweit sich aus diesen Besonderheiten rechtlich relevante Unterschiede ergeben, werden diese an den jeweiligen Stellen erläutert.

Biometrische Merkmale werden (uneinheitlich) in verschiedene Kategorien geordnet. Gängig ist etwa die Unterscheidung zwischen verhaltensbezogenen (behavioralen) und physiologischen Merkmalen.[346] Verhaltensgebundene biometrische Merkmale sind zum Beispiel Sprache, Hand- oder Unterschrift, Laufbewegung und Tippverhalten.[347] Physiologische Attribute wie Finger-, Hand- und Gesichtsgeometrie oder Irismuster knüpfen demgegenüber an gegenständliche Körpermerkmale des Trägers an.

Die Terminologie ist allerdings vielförmig. Es ist notwendig, zwischen diesen rein das Merkmal beschreibenden Kriterien und den Eigenschaften des Erkennungssystems zu unterscheiden. So macht es datenschutzrechtlich etwa einen Unterschied, ob ein System das jeweilige Merkmal unbemerkt erheben kann oder der Betroffene es in einer definierten Weise präsentieren muss und somit von der Datenerhebung erfährt.[348] Dieses Kriterium der datenschutzrechtlichen Mitwirkungsgebundenheit stimmt jedoch nicht mit der Einordnung nach verhaltensbezogenen und physiologischen Merkmalen überein. So kann das verhaltensgebundene Merkmal der Laufbewegung zwar nicht ohne ein Verhalten des Betroffenen (Gehen), wohl aber ohne eine Merkmalspräsentation erhoben werden, bei der der Betroffene von der Datenerhebung erfährt. Im datenschutzrechtlichen Sinn liegt dann keine (informierte) Mitwirkung vor. Umgekehrt erfordern die physiologischen Merkmale Fingerabdruck und Iriserkennung zumindest beim heutigen Stand der Technik eine Mitwirkung des Betroffenen. Damit ist zwar nicht das Merkmal selbst, wohl aber der Gesamtvorgang der Präsentation „verhaltensbezogen". An diesen Gesamtvorgang muss die datenschutzrechtliche Bewertung anknüpfen.

Es ist überdies kaum möglich, biometrische Merkmale selbst in die Kategorien der Mitwirkungsabhängigkeit oder -unabhängigkeit einzuordnen, weil bisweilen dasselbe Merkmal je nach System mitwirkungsabhängig präsentiert werden muss (beispielsweise ein Gesicht in einem festgelegten Abstand und Position zu einer Kamera) oder unbemerkt, zum Beispiel im Vorbeigehen, erhoben werden kann. Mit zunehmendem technischem Fortschritt werden sich hier die Unterschiede auch bei anderen biometrischen Merkmalen

342 Zur Rolle der ICAO vgl. unten 3.1.1.

343 S.u. 3.1.2.

344 Zu diesen und anderen „esoterischen" biometrischen Verfahren s. *Woodward/Orlans/Higgins* 2003, 115 ff.; *Rejman-Greene* 2003b, 123 ff.; für einen Überblick über verwendete und in der Entwicklung befindliche Systeme vgl. auch *TAB* 2002, 9.

345 S. insoweit *Jain/Bolle/Pankanti* 1999, Kap. 2-13; *Ashbourn* 2000, 45 ff.; *Behrens/Roth* (Hrsg.) 2001, II. Teil; *Breitenstein* 2002, 35 ff.; *Rejman-Greene* 2003b, 90 ff.; *Woodward/Orlans/Higgins* 2003, Kap. 3-7; *Albrecht* 2003a, 39 ff.; *Bolle/Connell/Pankanti/Ratha/Senior* 2004, 31 ff., 51 ff.; *Reid* 2004, 73 ff.; *JRC/IPTS* 2005, 54 ff., 122 ff. Ein ideales biometrisches Merkmal sollte universell (bei jedem Menschen vorhanden), einzigartig, permanent und erfassbar sein, s. *Jain/Bolle/Pankanti* 1999, 4; *TeleTrusT* 2002, 7; *Behrens/R*oth 2002, 400 f.

346 *TeleTrusT* 2002, 1, 6; *Nolde* 2002, 21; *Rankl/Effing* 2002, 509; *Nanavati/Thieme/Nanavati* 2002, 10; *Albrecht* 2003a, 35; *Rejman-Greene* 2003b, 10; *Bolle/Connell/Pankanti/Ratha/Senior* 2004, 6 f.

347 Einige von diesen beinhalten allerdings eine physiologische Komponente. Das gilt etwa für die physiologische Ausprägung des Sprachapparats, s. *Woodward/Orlans/Higgins* 2003, 78.

348 S.u. 4.2.2.4.1.2.

weiter verwischen. Die Mitwirkungsgebundenheit ist damit keine Eigenschaft eines biometrischen Merkmals allein, sondern abhängig von Merkmal und verwendetem Erfassungssystem.[349]

Für die rechtliche Analyse bleibt die Mitwirkungsgebundenheit im datenschutzrechtlichen Sinn die entscheidende Kategorie. Folglich wird im Folgenden diese Einteilung anstelle der sonst häufig gebrauchten Termini „dynamische" und „statische"[350] oder „aktive" und „passive"[351] Verfahren verwendet. Diese können zu Verwirrung führen, weil sie sich in der Literatur uneinheitlich auf Eigenschaften des Merkmals, des Präsentationsvorgangs oder des Gesamtsystems beziehen.

Neben der Mitwirkungsgebundenheit ist aus rechtlicher Sicht auch die Frage relevant, ob ein Merkmal „flüchtig" ist. Flüchtige biometrische Merkmale sind solche, die der Träger nicht dauerhaft in seiner Umwelt hinterlässt. Die ganz überwiegende Mehrzahl der verwendeten Merkmale ist in diesem Sinne flüchtig. Eine Ausnahme ist der Fingerabdruck, den jeder Mensch in nicht kontrollierbarer Weise in der Umgebung zurücklässt. Mit Einschränkungen sind auch die Handschrift und der Geruch nicht flüchtig. Nicht flüchtige Merkmale bergen datenschutzrechtliche Gefahren, weil eine Rückverfolgbarkeit zu einem späteren Zeitpunkt nicht ausgeschlossen werden kann.

Speziell beim Personalausweis ist zu beachten, dass dieser bereits Angaben über Eigenschaften des Inhabers enthält, nämlich Augenfarbe, Größe, Gesichtsbild, Alter und Unterschrift.[352] Bis auf die Größe scheiden diese Angaben allerdings bereits deshalb als biometrische Merkmale im Sinne der obigen Definition aus, weil sie nicht vermessen werden.[353] Dementsprechend finden sie auch keine Verwendung im Rahmen automatisierter Vorgänge bei der Authentifikation.[354] Zumindest beim Gesicht wäre das aber durchaus auch auf Basis des aktuellen Bildes möglich.[355] Größe und Alter erfüllen demgegenüber nicht das Kriterium eines „hoch charakteristischen" Merkmals, da sie bei einer Vielzahl von Individuen identisch und somit nicht zu einer Unterscheidung geeignet sind. Das Alter ist darüber hinaus nicht (exakt) automatisiert messbar.

Im Ergebnis befinden sich bislang im Personalausweis mangels automatisierter Auswertbarkeit der körperlichen Angaben keine biometrischen Daten im eigentlichen Sinne. Dementsprechend erfolgt eine terminologische Präzisierung dahin, dass immer dann, wenn an dieser und anderer Stelle von „biometrischen Daten" die Rede ist, diejenigen gemeint

---

349 S.a. *Probst*, DuD 2000, 322, 323.

350 Roßnagel-*Gundermann/Probst*, Kap. 9.6, Rn. 7; *Probst*, DuD 2000, 322, 323; *Tönnessen*, DuD 1999, 161; *Borges* 2003, 64.

351 *Kuip* 2002, 369 ff.; *Nolde* 2002, 21; *Albrecht* 2003a, 35 (dort auch zum Unterschied zwischen beiden Bezeichnungen); *Schnabel*, Spektrum der Wissenschaft 7/2003, 77; *Reid* 2004, 55 f.

352 Die vier Merkmale werden nicht immer alle erkannt. So übersehen Roßnagel-*Gundermann/Probst*, Kap. 9.6, Rn. 3 die Unterschrift, die zwar nicht anhand ihres Druckverlaufs, wohl aber in ihrem Aussehen ein behaviorales Merkmal ist. § 1 Abs. 4 Satz 1 PersAuswG erwähnt nur Bild und Unterschrift.

353 Gesicht und Unterschrift werden lediglich abgebildet, bei der Augenfarbe erfolgt eine reine Angabe. Es handelt sich deshalb nicht um biometrische, sondern um biologische Merkmale, s. Roßnagel-*Gundermann/Probst*, Kap. 9.6, Rn. 3. Das wurde vom Gesetzgeber in § 1 Abs. 4 Satz 1 PersAuswG übersehen, der von Bild und Unterschrift als biometrischen Merkmalen spricht.

354 Regelmäßig spielen alle Merkmale bis auf das Gesicht insoweit nur eine sehr untergeordnete oder gar keine Rolle: Die Alltagserfahrung zeigt, dass eine Identifizierung – selbst an der Grenze oder auf Flughäfen – normalerweise lediglich durch einen Vergleich mit dem auf dem Ausweis befindlichen Bild vorgenommen wird. Eine Unterschrift zur Identifikation ist nicht üblich. Die Rückseite des Ausweises (auf der sich Größe und Augenfarbe befinden) wird meist nicht zur Kenntnis genommen.

355 Ein solches Verfahren ist allerdings wegen der hohen Fehlerraten für den Masseneinsatz nicht verwendbar, s. *BSI/BKA/Secunet* 2004, 9 f., 49.

sind, um deren zusätzliche Einführung es beim digitalen Personalausweis geht.[356] Die Vernachlässigung der herkömmlich im Ausweis enthaltenen Merkmale entspricht insoweit auch dem allgemeinen Sprachgebrauch.

2.3.3.2 Funktionsweise

Biometrische Erkennungssysteme arbeiten im Wesentlichen nach verallgemeinerbaren Prozessabläufen.[357] Um eine Authentifikation (Bezeugung der Echtheit eines Merkmalsträgers)[358] mittels biometrischer Merkmale zu ermöglichen, müssen zunächst mit Sensoren Referenzdaten gewonnen werden. Dies geschieht im Rahmen des so genannten Enrolments, das die erstmalige Merkmalsgewinnung, Verarbeitung und Umwandlung, etwaige Extraktions- und Komprimierungsverfahren, sowie die Speicherung der Referenzdaten umfasst. Zum Teil wird das Merkmal mehrmals aufgenommen, um es hinreichend genau zu erfassen. Schlägt der Prozess des Enrolments fehl, so wird der prozentuale Anteil der fehlgeschlagenen Versuche als False Enrolment Rate oder Failure to Enrol Rate (FER) bezeichnet. Ein solcher Vorgang kann zum einen durch Fehler des Systems bedingt sein. Zum anderen gibt es bei den meisten Merkmalen einen gewissen Prozentsatz der Bevölkerung, der dieses entweder überhaupt nicht oder nicht in hinreichender Ausprägung für die biometrische Authentifikation besitzt.[359]

Im Rahmen des späteren Vergleichsprozesses (Matching) werden die aktuell beim Merkmalsträger erhobenen Daten mit den gespeicherten Referenzdaten verglichen. Hierzu gibt es unterschiedliche Verfahren. Eine Möglichkeit besteht darin, die beim Enrolment gewonnen Daten komplett aufzubewahren und später abzugleichen. In der Praxis wird jedoch stattdessen mit aufbereiteten Daten gearbeitet. Dies kann auf zwei Arten geschehen: mittels eines standardisierte Datenformats, das aber im Wesentlichen immer noch alle erhobenen Daten enthält (Volldaten, beispielsweise JPEG-, JPEG 2000- oder WSQ-komprimierte Bilder) oder mittels eines extrahierten Datensatzes, der nur einzelne, charakteristische Teile der erhobenen Rohdaten berücksichtigt (Template). Beispiele hierfür sind die Abstände bestimmter Charakteristika des Gesichts (Augen, Nase und andere) oder der Ort und die Art von endenden Tälern, Verzweigungslinien und Schweißporen beim Fingerabdruck (so genannte Minutien).[360] Templates werden in der Praxis insbesondere aufgrund des teilweise erheblichen Speicherbedarfs biometrischer Volldatensätze eingesetzt.[361] Das Matching erfolgt, indem aus den neu erhobenen Rohdaten erneut Templates berechnet und diese dann mit den gespeicherten Templates verglichen werden.

Terminologisch sollte zwischen diesen drei Arten von Daten unterschieden werden:

- biometrische Rohdaten sind die unmittelbar vom Sensor stammenden, unverarbeiteten Daten,

356 Für das Gesicht gilt das mit der Einschränkung, dass zwar nach wie vor dasselbe Merkmal verwendet wird, jedoch im Unterschied zu bisherigen Verfahren in automatisierter Messung.

357 S. zum Folgenden *Wirtz*, DuD 1999, 129 f.; *Behrens/Roth* 2001b, 10 ff.; *Nolde* 2002, 22; *TeleTrusT* 2002, 2 f.; *Nanavati/Thieme/Nanavati* 2002, 15 ff.; *Woodward/Orlans/Higgins* 2003, 28 ff.; Roßnagel-*Gundermann/Probst*, Kap. 9.6, Rn. 8 ff.; *Albrecht* 2003a, 35 ff.; *Hornung*, KJ 2004, 344, 346 ff.

358 Zu den Begriffen Authentifikation, Identifikation und Verifikation s.u. in diesem Abschnitt.

359 Wie hoch die FER ist, hängt vom jeweiligen System, dem verwendeten Merkmal, der Enrolmentsumgebung und der Auswahl der Nutzer ab; zu einzelnen Prozentzahlen s.u. 4.2.2.4.7.

360 S. *Breitenstein* 2002, 37 f.

361 Das Komplettbild des Fingerabdrucks benötigt ca. 250 Kilobyte, s. *Behrens/Roth* 2001a, 6 ff.; *TAB* 2002, 12.

- biometrische Voll- oder Bilddaten demgegenüber behandelte Datensätze, die aber immer noch ein vollständiges Abbild des Merkmals des Betroffenen enthalten,
- biometrische Templates dagegen Datensätze, die mittels eines Algorithmus aus einem Rohdatensatz berechnet werden und gegenüber den Rohdaten wesentlich weniger Informationen enthalten.[362]

Eine letzte Möglichkeit besteht in der Verwendung templatefreier Verfahren.[363] Dabei wird aus den biometrischen Rohdaten ein kryptographischer Schlüssel berechnet und mit diesem ein beliebiger Text verschlüsselt. Dieser Text wird im Klartext und in seiner verschlüsselten Form als Referenzdatensatz gespeichert. Beim Matching wird aus den neu erhobenen Rohdaten erneut der Schlüssel berechnet und mit diesem der Klartext verschlüsselt. Stimmen die verschlüsselten Datensätze überein, ist die Verifikation erfolgreich. Derartige Verfahren kommen ohne die Speicherung biometrischer Referenzdaten aus.[364] Außerdem können mit denselben biometrischen Daten unterschiedliche Referenzdaten bestimmt werden, indem (etwa bei Kompromittierung eines Klartext-Chiffrat-Paares) diese durch die Wahl eines anderen Klartextes neu berechnet werden.

Auch hinsichtlich des Speicher- und Abgleichsort gibt es unterschiedliche Verfahren. Möglich ist zunächst eine Zentralspeicherung der Referenzdaten (je nach Verfahren Volldaten, Templates oder Klartext nebst verschlüsseltem Text). Dann werden vor Ort die biometrischen Daten erhoben und an eine zentrale Recheneinheit gesandt, die das Matching vornimmt. Die Referenzdaten können aber auch auf einem portablen Medium gespeichert werden.[365] Bei einer derartigen dezentralen Speicherung kann dann das Matching an unterschiedlichen Stellen erfolgen. Entweder wird eine Kontrolleinheit mit Sensor verwendet, die die Referenzdaten aus der Karte ausliest und das Matching vornimmt. Oder die Kontrolleinheit sendet umgekehrt die durch den Sensor erhobenen Daten an die Karte, und die Überprüfung findet in der Karte statt (Matching-On-Card).[366] Außerdem gibt es Verfahren, bei denen das Medium nicht nur über einen Mikrochip zum Matching, sondern auch über einen (Fingerabdruck-)Sensor verfügt. Dann kann auf eine Kontrolleinrichtung völlig verzichtet werden.

Biometrische Systeme dienen der Authentifikation (Bezeugung der Echtheit) eines Merkmalsträgers. Autorisierung heißt demgegenüber, dass nach erfolgreicher Authentifikation (hier mittels eines biometrischen Systems) die Person ermächtigt wird, gewisse Handlungen durchzuführen oder bestimmte Dienste zu nutzen.[367] Eine Authentifikation

362 Die Unterscheidung zwischen Volldaten und Templates ist insbesondere für die datenschutzrechtliche Analyse essentiell. Zumindest missverständlich deshalb *Albrecht* 2003a, 36, wo nur zwischen Rohdaten und Templates unterschieden wird. Bisweilen werden auch Volldatensätze als „Templates" bezeichnet, z.B. bei *Bromba* 2003; zur Frage der Verwendung von Templates s.u. 4.2.2.4.2.

363 *Albrecht/Probst* 2001, 39 f.; Roßnagel-*Gundermann/Probst*, Kap. 9.6, Rn. 24 f.; *Probst* 2002, 124 f.; *Albrecht* 2003a, 56 f. Ein Bsp. hierfür ist die sog. „Virtual PIN" von G&D, vorgestellt auf dem BIOSIG-Workshop des CAST-Forums am 24.7.2003 in Darmstadt; s.a. http://europa.eu.int/idabc/en/2578/194.

364 Es ist allerdings nicht zutreffend, dass hierdurch jede Verwendung personenbezogener Daten entfiele, wie dies bisweilen dargestellt wird; s. dazu unten 4.1.2.2.2.4.

365 Dabei war bislang die Speicherung von Volldaten aus Speicherplatzgründen problematisch. Mit der zunehmenden Leistungsfähigkeit der Chips dürfte dieses Problem jedoch für alle Merkmale in Zukunft entfallen.

366 Zur rechtlichen Relevanz von Matching-On-Card s.u. 4.2.2.4.4.

367 *TeleTrusT* 2002, 5; *Woodward/Orlans/Higgins* 2003, 3 f.

kann durch zwei Verfahren geschehen, nämlich durch Verifikation oder Identifikation.[368] Bei der Verifikation findet ein Vergleich der im Einzelfall erhobenen Daten mit einem konkreten Referenzdatensatz statt (1:1). Es wird überprüft, ob es sich bei einer Person um diejenige handelt, für die sie sich ausgibt. Die Identifikation hingegen erfolgt durch einen Vergleich der erhobenen Daten mit allen Referenzdaten (1:n), die dann zentral gespeichert werden oder zumindest insgesamt zugänglich sein müssen. Beim Abgleich wird das Referenzmuster bestimmt, das am besten passt,[369] und damit überprüft, um welche Person es sich handelt. Ein solches Verfahren wird zum Beispiel regelmäßig bei Fahndungsdatenbanken eingesetzt.

Der Vorgang des Matchings erfolgt durch einen Vergleich von konkreten Datensätzen. Im Unterschied zu einer Passwortkontrolle, die stets ein eindeutiges Ergebnis liefert (1 oder 0; das Passwort ist richtig oder falsch) arbeiten biometrische Verfahren jedoch mit relativen Übereinstimmungsgraden, weil wegen der Funktionsweise der Systeme keine vollständige Übereinstimmung erreichbar ist.[370] Mängel können auf unterschiedlichen Ebenen im gesamten Prozess auftreten.[371] Sie betreffen etwa eine zu geringe Ausprägung der Merkmale, Mess- und Bedienungsfehler beim Enrolment und Matching, Probleme bei der Berechnung der Templates (wegen der starken Datenreduktion können auch an sich hinreichend unterschiedliche Merkmale ähnliche Templates ergeben) und Änderungen der verwendeten biometrischen Merkmale über die Zeit.

Eine totale Gleichartigkeit der Datensätze ist allerdings auch nicht erforderlich. Wenn eine hinreichende Unterschiedlichkeit des verwendeten Merkmals vorliegt, kann auch eine niedrigere Übereinstimmung für die Praxis ausreichend sein. Der Wert, der hierfür eingestellt wird (Schwellwert), beeinflusst die Fehlerraten des biometrischen Systems. Da dieses mit Wahrscheinlichkeiten arbeitet, gibt es aufgrund der genannten Fehlerursachen immer die Möglichkeit, dass bei der Überprüfung fälschlicherweise eine Übereinstimmung oder Nicht-Übereinstimmung festgestellt wird. Die Wahrscheinlichkeit einer ungerechtfertigten Zurückweisung wird als False Rejection Rate (FRR), die einer ungerechtfertigten Akzeptanz als False Acceptance Rate (FAR) bezeichnet.[372] Die FRR ist damit eine Angabe darüber, wie viel Prozent der an sich berechtigten Nutzer vom System zurückgewiesen werden, während die FAR die Wahrscheinlichkeit dafür angibt, dass ein an sich zurückzuweisender Merkmalsinhaber dennoch fälschlich als Berechtigter identifiziert wird. Beide Raten sind nicht theoretisch herleitbar, sondern müssen immer auf der Basis praktischer Tests bestimmt werden.

---

368 S. *Probst*, DuD 2000, 322; *Behrens/Roth* 2001b, 10 ff.; *TeleTrusT* 2002, 4 f.; *Nolde* 2002, 22 f., 26 f.; Roßnagel-*Gundermann/Probst*, Kap. 9.6, Rn. 11 f.; *Woodward/Orlans/Higgins* 2003, 7 f.; *Albrecht* 2003a, 38.

369 *Albrecht* 2003a, 38; Roßnagel-*Gundermann/Probst*, Kap. 9.6, Rn. 12; *TeleTrusT* 2002, 5. Der Abgleich mit einer Datenbank kann auch dazu benutzt werden festzustellen, dass sich die biometrischen Daten einer Person nicht in dieser befinden („screening"), s. *Bolle/Connell/Pankanti/Ratha/Senior* 2004, 26.

370 Vgl. *Albrecht* 2003a, 36; Roßnagel-*Gundermann/Probst*, Kap. 9.6, Rn. 14 ff.; *Munde* 2002, 148 f. Eine vollständige Übereinstimmung dürfte sogar umgekehrt auf eine Replay-Attacke hindeuten und somit verdächtig sein, s. *Daum* 2002, 184; ausführlich zu Fehlermessungen und -berechnungen *TeleTrusT* 2002, 9 ff.; *Nanavati/Thieme/Nanavati* 2002, 25 ff.; *Bolle/Connell/Pankanti/Ratha/Senior* 2004, 63 ff., 87 ff., 269 ff.

371 S. näher Roßnagel-*Gundermann/Probst*, Kap. 9.6, Rn. 15 f.; *Behrens/Roth* 2002, 402 f.; *Albrecht* 2003a, 53.

372 *Albrecht* 2003a, 52; *TAB* 2002, 11; Roßnagel-*Gundermann/Probst*, Kap. 9.6, Rn. 14 ff.; *Nolde* 2002, 23 f.; *Woodward/Orlans/Higgins* 2003, 35 ff.

FRR und FAR sind vom eingestellten Schwellwert und von der Grundgenauigkeit des Systems abhängig. Je höher der Schwellwert liegt, desto geringer wird die FAR. Eine niedrige FAR ist etwa für die Zugangssicherung zu Hochsicherheitsbereichen erwünscht. Gleichzeitig steigt jedoch die FRR an. Dies ist für die Benutzer problematisch, da sich das Risiko erhöht, einen erneuten Zugangsversuch machen zu müssen, dabei unter Verdacht zu geraten oder sogar insgesamt zurückgewiesen zu werden. Aus Sicht der Merkmalsträger ist deshalb regelmäßig eine geringe FRR vorteilhaft.[373] In diesem Fall steigt jedoch die FAR an, was zu Sicherheitsproblemen führen kann. Die beiden Fehlerraten beeinflussen sich also gegenseitig.[374]

Bei der Systemeinstellung ist es möglich, FRR und FAR gleich groß zu halten. Man spricht dann von einer Equal Error Rate (EER).[375] Diese wird allerdings nur in Ausnahmefällen den Bedürfnissen der jeweiligen Anwendungsumgebung entsprechen, da jeder Systembetreiber Sicherheit und Komfort je nach dem geplanten Einsatzszenario unterschiedlich gewichten wird. Die EER ist aber eine geeignete Möglichkeit, die Leistungsfähigkeit unterschiedlicher biometrischer Systeme miteinander zu vergleichen.[376]

Je genauer das System im Grundsatz arbeitet, desto geringer ist seine Gesamtfehlerrate. Für jeden einzelnen Schwellwert ergibt sich diese aus der Summe aus FRR und FAR. Die Gesamtfehlerrate kann jedoch nicht abstrakt angegeben werden. FRR und FAR beeinflussen sich zwar in der genannten Weise, aber nicht derart, dass ihre Summe stets gleich bliebe oder die beiden sich antiproportional zueinander verhielten. Aus juristischer Sicht sind die jeweiligen Fehlerraten ein Problem der Eignung und der objektiven Zumutbarkeit im Rahmen der Verhältnismäßigkeitsprüfung.[377]

2.3.3.3 Einsatz in der Praxis

Bedingt durch die Schnelllebigkeit des Marktes und die rasante technische Entwicklung ist es schwierig, einen Überblick über alle bereits in der Praxis eingesetzten oder in der Entstehung befindlichen Systeme zu gewinnen. Oftmals überlappen beide Bereiche auch, da eine Vielzahl der eingesetzten Verfahren Pilot- oder Feldversuche sind. Der folgende Überblick ist deshalb notwendigerweise unvollständig.

Bis in die jüngere Vergangenheit wurde Biometrie ganz überwiegend als kriminaltechnische Methode eingesetzt.[378] Die Weiterentwicklung der Verfahren ermöglicht heute verstärkt den Einsatz in anderen hoheitlichen und privaten Bereichen. Bereits vorhandene Einsatzfelder biometrischer Systeme haben unterschiedliche Verwendungszwecke, nämlich insbesondere die Aktivierung von Chipkarten-Funktionen, die Zutritts- und Zugangs-

373 Eine Ausnahme besteht bspw., wenn der Merkmalsträger das biometrische Verfahren zur Zugangssicherung zu eigenen Daten verwendet. Dann besteht sein vorrangiges Interesses in einer niedrigen FAR.

374 *Daum* 2002, 184; *Köhntopp* 1999, 180; *Nolde* 2002, 24; zu den daraus entstehenden „trade-offs“ *Bolle/Connell/Pankanti/Ratha/Senior* 2004, 81 ff.

375 *TeleTrusT* 2002, 13; *Albrecht* 2003a, 53 m.w.N.

376 Dies allerdings mit der Einschränkung, dass auch die Leistungsfähigkeit immer relativ zur gewünschten Umgebung zu bestimmen ist. Jeder Systembetreiber sollte deshalb – ausgehend von der eigenen Prioritätenbildung – eine FRR oder FAR bestimmen und dann das System mit der jeweils niedrigsten anderen Fehlerrate wählen.

377 S.u. 4.2.2.4.1.1, dort auch zu aktuell ermittelten Fehlerraten.

378 Vgl. *Weichert*, CR 1997, 369 f.

sicherung, die kriminalistische Erkennung, die Vermeidung von Doppelbezügen staatlicher Leistungen und den Convenience-Bereich.[379]

Einzelbeispiele zeigen ein kaum zu überblickendes und nahezu flächendeckendes Einsatzfeld.[380] Man kann eine grobe Einteilung in hoheitliche und nicht-hoheitliche Anwendungen vornehmen. Im staatlichen Bereich wird die Fingerabdruckserkennung schon seit längerer Zeit in automatisierter Form zur Verbrechensbekämpfung eingesetzt.[381] In Zukunft werden zwei große Anwendungsfelder hinzutreten, nämlich Grenzkontrollen und staatliche Identifikationsdokumente. Im Grenzkontrollbereich existiert seit dem Jahre 2001 ein Iriserkennungsverfahren am Amsterdamer Flughafen Schiphol.[382] Ein ähnliches System wird in den Vereinigten Arabischen Emiraten betrieben.[383] Das US-amerikanische INSPASS verwendet demgegenüber die Handgeometrie zur Grenzkontrolle und Passagierabfertigung.[384] Am Grenzübergang Erez zwischen Israel und dem Gaza-Streifen wird ein kombiniertes System aus Hand- und Gesichtserkennung eingesetzt.[385] In Frankfurt läuft seit dem 13. Februar 2004 ein Pilotprojekt zur Iriserkennung.[386]

Weltweit gibt es eine Reihe von Ansätzen zur Implementierung von Biometrie in Identitätspapieren.[387] Die USA verlangten ursprünglich von den Staaten des Visa-Waiver-Abkommens, ab Oktober des Jahres 2004 Programme zur Aufnahme biometrischer Daten in ihre Reisepässe in Gang zu setzten.[388] Die Frist ist mittlerweile allerdings um ein Jahr verlängert worden. Die Länder der Europäischen Union haben am 13. Dezember 2004 eine Verordnung verabschiedet, die die Mitgliedstaaten zur Einführung biometrischer Gesichts- und Fingerabdrucksdaten in ihre Pässe verpflichtet.[389] Auch die Internationale Arbeitsorganisation (ILO) hat auf einer Arbeitskonferenz im Juni des Jahres 2003 beschlossen, in einer neuen Konvention biometrische Daten in Ausweisen für Seeleute vorzuschreiben.[390] In Staaten, die Führerscheine zur Identifikation einsetzen, gibt es Projekte, diese mit biometrischen Daten auszustatten.[391]

Vorgesehen ist auch die schnelle Einführung eines einheitlichen Visums zur Einreise in die Europäische Union. Deutsche Pilotprojekte hierzu laufen bei der Visa-Beantragung in

379 Roßnagel-*Gundermann/Probst*, Kap. 9.6, Rn. 28 ff. Im Jahr 2002 machte der Bereich der Zugangskontrolle mit 42 % Marktanteil nach Umsätzen den größten Anteil aus, s. *BITKOM* 2003, 50.

380 S. zum Folgenden schon *Hornung*, KJ 2004, 344, 349 und die Aufzählungen von *Ashbourn* 2000, 21 ff.; *Albrecht* 2001, 7 ff.; *TAB* 2002, 35 f.; *Nanavati/Thieme/Nanavati* 2002, 143 ff.

381 S. ausführlich *Woodward/Orlans/Higgins* 2003, 45 ff.

382 *Junginger/v. Beek* 2002, 218 ff.; *Albrecht* 2003a, 25 m.w.N.; auch das kanadische Einreisesysteme CANPASS nutzt die Iriserkennung, s. *OECD* 2004, 29; weitere Bsp. bei *TAB* 2004, 20 ff.

383 Vgl. http://www.heise.de/newsticker/meldung/35938.

384 S. näher http://www.immigration.gov/graphics/fieldoffices/washingtondc/inspass.htm. Das System ist inzwischen wegen schlechter Erkennungsraten tlw. eingestellt worden, vgl. *OECD* 2004, 24. Auch am Ben Gurion Airport in Israel wird die Handgeometrie verwendet, s. *Woodward/Orlans/Higgins* 2003, 289.

385 S. OMNICARD-newsletter Oktober 2003.

386 S. http://www.bundesgrenzschutz.de/Auto_Grenzkontrolle/index.php. Dieser hatte ursprünglich eine Laufzeit bis August 2004, wurde jedoch um zwölf Monate verlängert, s. http://europa.eu.int/ida/en/document/3226/194; s.a. *Der Bundesbeauftragte für den Datenschutz* 2005, 62 f.

387 Bsp. bei *Petermann*, TAB-Brief Nr. 24 (2003), 19, 20; für Personalausweise s.u. 3.

388 S.o. 2.1.1.

389 S.u. 3.1.2.

390 Diese sollen mit Fingerabdrucksdaten versehen werden, um die weltweit 1,2 Mio. Seeleute eindeutig zu identifizieren; s. http://www.ilo.org/public/english/bureau/inf/pr/2003/25.htm; s.a. *TAB* 2004, 17; *Der Bundesbeauftragte für den Datenschutz* 2005, 83.

391 Bspw. in den USA, s.u. 3.5.2.1.

Lagos (Fingerabdruck) und Manila (Iris-Scan).[392] Im Aufbau befindet sich mittlerweile das europäische EURODAC-Programm zur zentralen Erfassung der Fingerabdrucksdaten von Asylbewerbern.[393] Bei der Einreise in die USA werden bereits seit dem 1. Januar 2004 von visumpflichtigen Reisenden biometrische Daten erhoben.[394] In Deutschland wird auch die Einführung eines Flugpasses mit biometrischen Daten angedacht, um einen Bordkartentausch zu verhindern.[395]

Im hoheitlichen Bereich werden überdies Gesichtserkennungssysteme in Sportstadien zur Gewaltbekämpfung oder zu Fahndungszwecken,[396] sowie Iriserkennungsverfahren bei der Gefangenenregistrierung eingesetzt.[397] Außerdem gibt es Spracherkennungssysteme zur Überwachung von Personen, die unter Hausarrest stehen.[398] Honduras wollte im Laufe des Jahres 2004 alle Waffenbesitzer zum Besitz einer Chipkarte mit Fingerabdrucksdaten verpflichten.[399] Betont werden auch Möglichkeiten der Biometrie im Rahmen der sekundären (das heißt technischen) Prävention.[400] Angeblich messen britische Entwickler der Geruchserkennung Potential bei der Verbrechensbekämpfung zu.[401]

Die Niederlande geben bereits seit dem Jahre 1997 Asylbewerberausweise mit biometrischen Daten zur Leistungsausgabe und Aufenthaltskontrolle aus.[402] Dort wurden auch Systeme zur Kontrolle der Abgabe von Methadon eingerichtet.[403] Der US-Bundesstaat Connecticut setzt ein Fingerabdrucksverfahren zur Missbrauchsbekämpfung im Sozialhilfebereich ein.[404] In der kanadischen Provinz Ontario ist der Einsatz von Biometrie zu diesem Zweck seit dem Jahre 1997 zulässig.[405] Im Rahmen der Ausgabe von Hilfslieferungen durch den UN-Flüchtlingskommissar in Pakistan werden die Iris-Scans der Antragsteller gespeichert.[406] Bei der Wählerregistrierung in Mexiko werden Gesichtserkennungsverfahren verwandt,[407] und der Fingerabdruck dient zur Authentifizierung an Wahlautomaten in der Schweiz.[408]

Ein wichtiges Einsatzgebiet biometrischer Verfahren sowohl im hoheitlichen als auch im privaten Bereich wird in Zukunft die Zugangskontrolle in Behörden und Betrieben

---

392 S. http://www.heise.de/newsticker/meldung/38877; http://www.heise.de/newsticker/meldung/41482. Hier werden zentrale Datenbanken eingerichtet, um eine erneute Antragstellung unter anderem Namen zu verhindern. Ein gemeinsames Visa Information System soll beim Aufbau einer einheitlichen Visapolitik und der Bekämpfung illegaler Einwanderung helfen, s. *Europäische Kommission* KOM(2003) 323, 4, 9 und 19. Ein Feldversuch sollte Mitte 2005 starten, s. http://europa.eu.int/idabc/en/document/4288/194.

393 Vgl. *Golembiewski/Probst* 2003, 11 f.; s.a. unten 3.1.2.

394 Vgl. etwa den Bericht unter http://www.spiegel.de/reise/aktuell/0,1518,249412,00.html.

395 S. *DFK* 2004, 44 ff.

396 Etwa beim Super Bowl 2001 in Tampa (USA), s. *Woodward* 2001; *Nanavati/Thieme/Nanavati* 2002, 273 ff.; *Woodward/Orlans/Higgins* 2003, 247 ff.; weitere Bsp. bei *Lyon* 2001, 301.

397 *Nanavati/Thieme/Nanavati* 2002, 82; *Woodward/Orlans/Higgins* 2003, 293.

398 *Nanavati/Thieme/Nanavati* 2002, 93.

399 S. http://www.cardtechnology.com/cgi-bin/readstory.pl?story=20040210CTDN386.xml.

400 Vgl. die Workshop-Dokumentation des *DFK* (2002).

401 S. *Burke/Warren*, The Observer v. 28.12.2003.

402 *Weichert*, CR 1997, 369, 373.

403 S. *Albrecht* 2001, 16.

404 http://www.dss.state.ct.us/digital.htm; dazu *Albrecht* 2001, 85 f.; weitere Programme gibt es in Arizona, Kalifornien, Massachusetts, New York und Texas, s. *Woodward/Orlans/Higgins* 2003, 284 ff.

405 S. *Lyon* 2991, 300.

406 *Woodward/Orlans/Higgins* 2003, 287 f.

407 S. *Nanavati/Thieme/Nanavati* 2002, 72.

408 http://www.heise.de/newsticker/meldung/42814; OMNICARD-Newsletter Januar 2004.

sein.[409] Die zahlenmäßig größte Anwendung ist die Common Access Card des US-Verteidigungsministeriums, die mittlerweile an über vier Millionen Angehörige der Streitkräfte ausgegeben wurde und Fingerabdrucksdaten speichert. Ihre Spezifikationen gleichen denen für internationale Reisedokumente. Die USA planen, ab Oktober des Jahres 2006 an alle staatlichen Bediensteten Ausweise nach einem einheitlichen Standard auszugeben.[410] Hiervon wären über sieben Millionen Menschen betroffen. In Charlotte (North Carolina, USA) wird ein Iriserkennungssystem bei Flughafenmitarbeitern eingesetzt.[411] Atomkraftwerke sichern den Zutritt schon seit längerem mittels Biometrie.[412] Am London City Airport läuft ein System im Vollbetrieb, bei dem 1.600 Angestellte mit dem Fingerabdruck Zugang zu Sicherheitsbereichen erhalten.[413] Im Hafen von Antwerpen wird hierzu die Handgeometrie verwendet.[414] Ein Einsatz ist auch zur Zeiterfassung in Behörden[415] oder – mittels des Tippverhaltens – zur Nutzererkennung am PC[416] möglich. Schrifterkennungsverfahren werden zur Sicherung von Dokumentverwaltungssystemen eingesetzt.[417] Casinos in den USA arbeiten schon seit längerem mit Gesichtserkennungsverfahren,[418] und die University of Georgia hat kürzlich ein neues Verfahren zur Erkennung der Handgeometrie eingeführt, das ein 33 Jahre altes Vorgängermodell ersetzte.[419] Mehrere US-Schulen kontrollieren die Essensausgabe mit biometrischen Systemen.[420] In Großbritannien sollen sich Kinder ab dem siebten Lebensjahr mit dem Fingerabdruck zur Buchausleihe in Schulbibliotheken authentifizieren.[421] Der Zugang zum Olympischen Dorf der Sommerspiele in Atlanta im Jahre 1996 wurde mittels Handgeometrie gesichert.[422] Auch bei den Olympischen Spielen in Athen im Jahre 2004 regelte ein biometrisches Akkreditierungssystem den Zutritt zum Deutschen Haus.[423] Bereits seit dem Jahre 1998 existieren Fingerabdrucksysteme zur Zutrittssicherung bei Selbstbedienungs-Videoautomaten.[424]

Weitere Beispiele aus dem privaten Bereich umfassen fingerabdruckbasierte Schusswaffensicherungen, die automatische Aktivierung individueller Fahrzeugeinstellungen in

---

409 S. etwa http://www.heise.de/newsticker/meldung/44593. Diese ist im privaten Bereich nach § 87 Abs. 1 Nr. 1 und Nr. 6 BetrVG mitbestimmungspflichtig. Das gilt auch, wenn das System von einer Fremdfirma betrieben wird, bei der die Beschäftigten als Monteure arbeiten, s. BAG, DuD 2004, 433 ff.; vgl. in der ersten Instanz auch ArbG Frankfurt a.M., RDV 2002, 248; zur Problematik *Hornung*, KJ 2004, 344, 354 f.; *Hornung/Steidle*, AuR 2005, i.E.; s.a. *Steidle* 2005, Kap. 10.9; 14.7; 15.2.4.

410 http://www.cardtechnology.com/cgi-bin/readstory.pl?story=20050407CTDN335.xml. Darüber hinaus wird es ein Verfahren zur gegenseitigen Anerkennung von Dienst- und Betriebsausweisen von Behörden und Unternehmen geben, s. http://www.gcn.com/vol1_no1/daily-updates/26077-1.html.

411 S. http://www.fcw.com/fcw/articles/2003/0623/cov-side4-06-23-03.asp.

412 Vgl. zuletzt Computerwoche 32/2003, 31 (Zugangskontrolle per Gesichtserkennung).

413 S. *Fenner* 2003. Dabei findet ein 1:n Abgleich mit allen Daten der Datenbank statt; zu ähnlichen Plänen in Deutschland vgl. *DFK* 2004, 17 ff.

414 Vgl. http://europa.eu.int/idabc/en/document/4217/194.

415 S. http://www.silicon.de/cpo/news-adn/detail.php?nr=12498.

416 http://www.heise.de/newsticker/meldung/39958.

417 Etwa bei der Mercedes-AMG GmbH, s. http://www.siglab.de/siglab/signews/softpro030828.php.

418 S. ausführlich *Woodward/Orlans/Higgins* 2003, 330 ff.

419 Vgl. http://www.cardtechnology.com/cgi-bin/readstory.pl?story=20050215IDNN046.xml.

420 S. *Albrecht* 2003a, 25 m.w.N.

421 Vgl. http://www.heise.de/newsticker/meldung/29279.

422 *Breitenstein* 2002, 63; *Lyon* 2001, 304.

423 Vgl. den Bericht unter http://www.heise.de/newsticker/meldung/49309.

424 S. den Fall von BGH, MMR 2003, 582 (dort wurde mittels einer Chipkarte und biometrischen Daten ein System zur Überprüfung der Volljährigkeit bei Benutzern des Automaten zur Ausleihe von „weicher Pornographie“ installiert); zu einem vergleichbaren System vgl. *Albrecht* 2003a, 24.

Kraftfahrzeugen per Fingerabdruckserkennung,[425] die so genannte „Siemens ID Maus“,[426] den Einsatz von Iris- und Handvenenmustererkennung bei Geldautomaten[427] und von Stimmerkennung im Online-Banking,[428] die Unterschrifterkennung zum Ausfüllen von Meldescheinen nach § 26 Abs. 2 MeldeG NW in einem Bonner Hotel,[429] die Zugriffssicherung für PCs[430] und Speichermedien[431] mit Hilfe von Fingerabdrucksensoren, Online-Bezahlfunktionen im Mobilfunkbereich,[432] im Handel[433] und in der Gastronomie,[434] sowie Zugangskontrollen für Saisonkarteninhaber in Disney World (Fingerabdruck[435] und Handgeometrie[436]) und im Zoo der Stadt Hannover (Gesicht).[437] Der IT-Branchenverband BITKOM möchte überdies die im Jahre 2006 in Deutschland stattfindende Fußball-Weltmeisterschaft als Testfeld für die Biometrie-Technik nutzen.[438]

2.3.3.4 Chancen und Problemfelder

Chancen wie Risiken der Biometrie resultieren aus der grundsätzlich untrennbaren Bindung[439] des jeweiligen Merkmals an die betroffene Person. Potentielle Vorteile ergeben sich in den Bereichen Zugangssicherung, Nutzerfreundlichkeit und Rechtssicherheit. Biometrische Verfahren können Alternativen oder Ergänzungen zu bisherigen Kontrollsystemen sein, die regelmäßig mit einer Sicherung durch Besitz (Chipkarte, Schlüssel) und Wissen (PIN, Passwort) arbeiten. Der Vorteil biometrischer Merkmale liegt darin, dass sie weder weitergegeben, noch (im Unterschied zum Besitz) verloren gehen oder (im Unter-

425 Die Firma Audi bietet dies für das Modell A8 an, vgl. http://www.audi.com/de/de/neuwagen/a8/limousine/elektronik_ausstattungen/bedienung_komfort/one_touch_memory/one_touch_memory.jsp.

426 S. http://www.bromba.com/tdidmad.htm.

427 S. z.B. http://www.cardtechnology.com/cgi-bin/readstory.pl?story=20050308CTDN132.xml; zum Einsatz an Geldautomaten s.a. *Albrecht* 2001, 12; *Woodward/Orlans/Higgins* 2003, 337 ff. Die Verwendbarkeit im Bankenbereich wurde durch das Projekt BioTrusT evaluiert, s. http://www.biotrust.de.

428 *Breitenstein* 2002, 62; *Woodward/Orlans/Higgins* 2003, 345 f.

429 S. *Albrecht* 2003a, 24.

430 Z.B. der „e-Identity token“ (CE Infosys), s. http://www.ce-infosys.com.sg/CeiProducts_eIdentity_Ger.asp.

431 Es gibt inzwischen eine Reihe von USB-Speichern, die über einen Fingerabdrucksensor verfügen, etwa die „ClipDrive Bio“ von Memory Experts International, vgl. http://www.clipdrivebio.com; s.a. http://www.cardtechnology.com/cgi-bin/readstory.pl?story=20040715IDNN722.xml; http://www.heise.de/newsticker/meldung/57546.

432 S. http://www01.silicon.de/cpo/news-mobile/detail.php?nr=11759&directory=news-mobile.

433 Vgl. *Ziegler*, c't 12/2003, 38. Dort nutzten nach sechs Monaten Herstellerangaben zufolge ca. 100 Kunden das System auf freiwilliger Basis. Anfang 2005 führte ein EDEKA-Markt in Rülzheim ein entsprechendes System ein, vgl. http://www.heise.de/newsticker/meldung/57055. Auch die amerikanische Supermarktkette Piggly Wiggly Carolina Co. wollte ab Juli 2004 das Bezahlen mit Fingerabdruck in vier ihrer Geschäfte in South Carolina testen, s. OMNICARD-Newsletter März 2004/2; s.a. *Albrecht* 2001, 14.

434 S. http://www.heise.de/newsticker/meldung/39192/.

435 *Hadley*, EMBO reports 2004, 124, 125.

436 In der Anlage in Florida, s. *Woodward/Orlans/Higgins* 2003, 67 f.

437 http://www.heise.de/newsticker/meldung/36097; s.a. *Golembiewski/Probst* 2003, 10.

438 Etwa zur Sicherung von Sportlerkabinen und VIP-Bereichen oder zur Überwachung von Hooligans, s. http://www.heise.de/newsticker/meldung/42677; http://www.spiegel.de/netzwelt/technologie/0,1518,280015,00.html.

439 Das gilt vorbehaltlich einer gewaltsamen Abtrennung von Körperteilen. Offenbar kam es im April 2005 erstmals zu einem Fall, in dem Räuber den Zeigefinger des Eigentümers eines PKW abtrennten, um das biometrische Türöffnungssystem des Wagens zu überwinden, s. http://www.telepolis.de/r4/artikel/19/19798/1.html; http://www.theregister.co.uk/2005/04/04/fingerprint_merc_chop/. Diesem Problem kann allerdings bis zu einem gewissen Grad mit Lebenserkennungssystemen entgegengewirkt werden, s. dazu unten 6.2.2.

schied zu Wissen) vergessen werden können.[440] Dies eröffnet eine höhere Zugangssicherheit und ist im Interesse des Nutzers, der eine größere Datensicherheit gewinnt und sich keine PIN mehr merken muss. Aus derartigen Szenarien wird deutlich, dass der Einsatz von Biometrie durchaus dem Datenschutz dienen kann.[441]

Ein Gewinn an Rechtssicherheit kann durch eine Verbesserung der Authentizität erreicht werden, die gerade im elektronischen Rechtsverkehr von entscheidender Bedeutung ist.[442] Aktionen, die innerhalb und durch ein biometrisch gesichertes System ausgeführt werden, gewährleisten eine hohe Zurechenbarkeit zu einer Person. So wäre etwa bei Signaturkarten durch den Einsatz von Biometrie eine echte Bindung der Signaturerstellung an die Person des Signaturschlüssel-Inhabers möglich.[443] Durch die Verbesserung von Authentizität wird auch der Verbraucherschutz gestärkt.[444]

Bieten biometrische Authentifikationsverfahren damit eine Reihe von Vorteilen, so existieren doch auch Probleme und Risiken. Zunächst können die genannten Vorteile nur dann zum Tragen kommen, wenn das jeweilige System mit hinreichender Genauigkeit arbeitet. In diesem Bereich bestehen noch erhebliche Defizite, die sowohl für die Einsetzbarkeit im hoheitlichen Bereich als auch im Rahmen der elektronischen Signatur Probleme bereiten.

Auch wenn die Funktionsfähigkeit mit geringen Fehlerraten im manipulationsfreien Betrieb vorausgesetzt wird, verbleibt das Problem der Herstellung einer hinreichenden Überwindungssicherheit.[445] Nahezu jeder Verfahrensschritt kann Gegenstand eines Angriffs sein, wobei Sensoren und frei zugängliche Datenleitungen in unbeobachteten Einsatzszenarien besonders gefährdet sind. Problematisch ist in diesem Zusammenhang vor allem, dass im Unterschied zu Sicherungen durch Besitz und Wissen ein Austausch von kompromittierten Merkmalsdaten nicht, oder nur begrenzt möglich ist.[446]

Auf der datenschutzrechtlichen Ebene ergeben sich mehrere Fragen. Aufgrund der lebenslangen Bindung an den Betroffenen eignen sich biometrische Merkmale besonders gut zur generellen Überwachung und Profilbildung.[447] Im Rahmen der Verhältnismäßigkeitsprüfung müssen Vor- und Nachteile der Merkmale hinsichtlich ihrer Mitwirkungsgebundenheit und Flüchtigkeit berücksichtigt werden.[448] Besonders problematisch ist, dass einige biometrische Merkmale Zusatzinformationen, zum Beispiel über Krankheiten des Trägers, enthalten können. Zentrale Referenzdatendatenbanken bringen gegenüber einer dezentralen Speicherung deutlich höhere Gefahren von Profilbildungen, Hackerangriffen und staatlichen Zweckänderungen mit sich.[449]

Schließlich ist das Augenmerk auf die Akzeptanz biometrischer Systeme zu richten.[450] Sofern diese freiwillig eingesetzt werden, ist die Annahme durch die Nutzer notwendige

---

440 *Woodward* 1999, 388; *Weichert*, CR 1997, 369, 372; *Behrens/Roth*, DuD 2000, 327 ff.; *Nanavati/Thieme/Nanavati* 2002, 3 ff.; *Nolde* 2002, 28; *Albrecht* 2003a, 32 f., 48 ff.; s. zu den Problemen wissensbasierter Systeme *Adams/Sasse*, C.ACM 12/1999, 41 ff.; *Rejman-Greene* 2003b, 87.

441 *Köhntopp* 1999, 179 f.; *Woodward* 1999, 400 f.; *Albrecht/Probst* 2001, 29; *Lyon* 2001, 306; *Nolde* 2002, 25; *Probst* 2002, 125; *Rejman-Greene* 2003b, 140 ff.; *Woodward/Orlans/Higgins* 2003, 210 ff.

442 Vgl. zu diesem Aspekt *Albrecht* 2003a, insbes. 64 ff.

443 S. hierzu ausführlich unten 5.2.6.

444 *Bobrowski*, DuD 1999, 159; s. zum Nutzen der Biometrie für den Verbraucher auch *VZBV* 2002, 38 ff.; *Albrecht*, DuD 2000, 332 ff.

445 Zu den unterschiedlichen Angriffsmöglichkeiten s.u. 4.3.8.1.

446 *Schneier*, C.ACM 8/1999, 136; *Rankl/Effing* 2002, 510; *Albrecht* 2003a, 50 f.

447 S. dazu unten 4.2.2.1.2.

448 S.u. 4.2.2.4.1.2.

449 Vgl. unten 4.2.2.4.3.

450 S. ausführlich unten 7.3.3.1.

Bedingung für die Verbreitung. Im hoheitlichen Bereich entstehen demgegenüber erhebliche politische Risiken, wenn biometrische Systeme ohne Rücksicht auf die Akzeptanz in der Bevölkerung eingeführt werden. In diesem Zusammenhang ist es wichtig, bei der Auswahl eines biometrischen Merkmals und Identifikationssystems die Möglichkeiten technischen Fortschritts stets mitzubedenken. Teilweise stellen sich nämlich bestimmte Systeme beim heutigen Stand der Technik als unproblematisch dar. Durch ihre Implementierung werden jedoch Fakten geschaffen, die zukünftige Gefahrenlagen verursachen können.

2.4 Zum Verhältnis von Recht und Technik

Recht und Technik bestimmen in hohem Maße sowohl die individuelle Lebenswirklichkeit des Einzelnen als auch die sozialen Entwicklungsbedingungen der Gesellschaft. Sie sind auf unterschiedliche Art und Weise miteinander verbunden und beeinflussen sich gegenseitig in einem Prozess der Wechselwirkung. Technische Neuerungen können Verhaltensweisen ermöglichen, die neuer rechtlicher Regelung bedürfen. Ebenso können sie Verwirklichungs- und Umgehungsmechanismen für bereits bestehende Rechtsnormen liefern. Umgekehrt wirken generelle rechtliche Rahmensetzungen, Anreize und Restriktionen langfristig auf mögliche technische Entwicklungen, und konkrete Planungs- und Genehmigungsentscheidungen bestimmen über die Verwirklichung oder Verhinderung technischer Einrichtungen und Anlagen.

Der Geltungsanspruch des Rechts in diesem Prozess ist der einer normativen Selbstregulierung der Gesellschaft. Ist eine bestimmte Technologie oder Anwendung rechtswidrig, so darf sie de lege lata nicht verwendet werden; impliziert ihre Verwendung verfassungswidrige Folgen, so kann daran auch eine Initiative des Parlaments nichts ändern, solange sie nicht in eine Verfassungsänderung mündet. De facto sind die Einwirkungen der Technik auf das Recht jedoch so erheblich, dass man an der Verwirklichung dieses Überlegenheitsanspruchs zweifeln muss.[451] Technische Fortentwicklungen können unmittelbar auf eine rechtliche Bewertung Einfluss nehmen. Ist etwa eine – eingriffsintensive – strafprozessuale Überwachungsmaßnahme nur zulässig, wenn andere Ermittlungsmaßnahmen aussichtslos, wesentlich schwerer oder mit unverhältnismäßig hohem Aufwand verbunden sind,[452] so führt eine technische Vereinfachung der Maßnahme dazu, dass die Verhältnismäßigkeitsschwelle direkt herabgesetzt wird. Nicht so offensichtlich, jedoch ungleich wichtiger ist hingegen ein mittelbarer Zusammenhang. Neue technische Möglichkeiten beeinflussen soziale und gesellschaftliche Verhältnisse. Rechtsnormen dienen aber in aller Regel der Regulierung von Konflikten innerhalb dieser Verhältnisse. Deshalb ändern neue Technologien die faktischen Verwirklichungsbedingungen des Rechts, wirken so indirekt auf das Rechtssystem und können dieses im Wege der Rechtsinterpretation, das heißt auch ohne formelle Umgestaltung von Rechtsnormen, inhaltlich verändern.[453]

---

451 *Roßnagel/Wedde/Hammer/Pordesch* 1990, 57 ff.; *Roßnagel* 1997b, 143, 148; *ders*. 2003, 428.

452 Z.B. §§ 100a, 100c Abs. 1 Nr. 1 - 3, 100g Abs. 2, 100i Abs. 2 Satz 1 und 2, 110a Abs. 1 Satz 3 StPO.

453 S. *Roßnagel*, Der Staat 1983, 551 ff.; *ders*. 1984, 17 ff.; 222 ff.; *ders*. 1993, 105 ff.; *ders.* 1997b, 149; *Westphalen/Neubert* 1988, 257 ff. Dabei handelt es sich um ein allgemeines Problem des Verhältnisses von Norm und Tatsache, das allerdings im Bereich des Technikrechts besonders ausgeprägt ist. Da technische Veränderungen den normativen Gehalt rechtlicher Vorschriften verändern können, ohne ihren Wortlaut anzutasten, ist auch der bloße Hinweis, eine bestimmte Entwicklung sei heute rechtswidrig, perspektivisch gesehen eine ungenügende Aussage, s. *Roßnagel/Wedde/Hammer/Pordesch* 1990, 6.

Die Neuinterpretation bestehender Rechtsnormen ist insbesondere im Bereich des Verfassungsrechts zu beobachten, das in hohem Maße auslegungsfähig und -bedürftig ist. Ein Beispiel hierfür ist das Recht auf informationelle Selbstbestimmung, dessen dogmatische Entwicklung in Literatur und Rechtsprechung ausschließlich eine Reaktion auf technische Entwicklungen und Neuerungen ist.[454] Erst die Zunahme und Automatisierung der Verarbeitung personenbezogener Daten führten zum Bedürfnis nach verfassungsrechtlicher Verankerung und einfachgesetzlicher umfassender Normierung des Datenschutzes. Auch die aktuelle Modernisierungsdiskussion ist bestimmt durch technische Fortentwicklungen im Bereich der Erhöhung der Informationsverarbeitungskapazitäten, der Globalisierung, Dezentralisierung, Vernetzung und technischen Konvergenz der Medien.[455]

Dieses Phänomen kann man als „Reaktivität" des Rechts bezeichnen.[456] Es führt zu einer fortwährenden Anpassungsbedürftigkeit und – zumindest in den Bereichen, die einen starken Technikbezug aufweisen – zu einem chronischen Vollzugsdefizit des jeweils aktuellen Normengefüges.[457] Um diesem zu begegnen, versuchen neuere Ansätze, das Verhältnis von Recht und Technik dergestalt neu zu bestimmen, dass Recht seine Ziele dann effektiver erreicht, wenn es Technologien integriert und „instrumentalisiert". Das gilt insbesondere für das Verhältnis zwischen Datenschutzrecht und Informations- und Kommunikationstechnologie,[458] aber auch in anderen Rechts- und Technikgebieten.[459]

Für das Datenschutzrecht existieren seit einiger Zeit Ansätze, die vor allem für den globalen Electronic Commerce von Bedeutung sind. Wenn dessen Nutzer immer weniger auf einzelstaatliche Schutzinstrumente setzen können, so sind sie selbst stärker gefordert. Durch den Einsatz von Technik zum Selbstdatenschutz werden unter anderem Möglichkeiten zur Herstellung anonymen und pseudonymen Handelns eröffnet.[460] Derartige Privacy Enhancing Technologies (PET) sind gerade im Internet von großer Bedeutung.[461] Hier wandelt sich auch die Rolle des Staates. Wenn es ihm in einer globalisierten Welt nur noch eingeschränkt möglich ist, selbst für den umfassenden Schutz der informationellen Selbstbestimmung seiner Bürger zu sorgen, so beinhaltet der staatliche Schutzauftrag mindestens die Ermöglichung eines effektiven Selbstschutzes.[462]

Systemdatenschutz bedeutet demgegenüber, die Struktur von Datenverarbeitungssystemen so zu gestalten, dass diese möglichst datenschutzfreundlich, insbesondere datenver-

454 *Simitis*, DuD 2000, 714, 716; *Scholz* 2003, 21 m.w.N.

455 *Roßnagel/Pfitzmann/Garstka* 2001, 22 ff.; *Scholz* 2003, 21 ff., jeweils m.w.N.

456 Hierzu *Roßnagel*, DuD 1999, 253, 254; *ders*. 1993, 14 ff.; *Westphalen/Neubert* 1988, 259 ff.; s.a. *Simitis*, NJW 1998, 2473, 2478 f.; *Bull*, ZRP 1998, 310, 313; *Berg*, JZ 1985, 401 ff.; *Vieweg* 1996, 36 ff.; *Scholz* 2003, 349 ff.

457 Das gilt insbesondere, wenn – wie beim Internet – ein starker Bezug zum Ausland besteht; s. dazu näher *Roßnagel*, ZRP 1997, 26, 27 f.; *Simitis* 1997, 298 ff.; *Hoffmann-Riem*, AöR 1998, 513, 533.

458 *Roßnagel*, DuD 1999, 253, 255; *Simitis* 1997, 301 ff.; *Kloepfer* 1998, 99 f.; *Bizer* 1999, 45 ff.; *Konferenz der Datenschutzbeauftragten*, DuD 1997, 735; *Roßnagel/Pfitzmann/Garstka* 2001, 35 f.; *Nedden* 2001, 67 ff.; *Hoffmann-Riem*, AöR 1998, 513, 535; *Schulte* 2000, 33 f.; *Scholz* 2003, 345 f.; s.a. *Richter* 2004, 245 ff.; vgl. bereits *Podlech*, DVR 1972/73, 149, 155; *ders*. 1982, 451 ff.

459 Vgl. insoweit *Roßnagel* 2001b, 195 ff.

460 Dazu *Scholz* 2003, 200 ff. et passim; s.a. *Roßnagel/Scholz*, MMR 2000, 721 ff.; *Roßnagel*, ZRP 1997, 26 ff.; Roßnagel-*Roßnagel*, Kap. 3.4; *Simitis*, NJW 1998, 2473, 2478; s.a. die Beiträge in DuD 2003, Heft 3.

461 *Weichert*, NJW 2001, 1463, 1466; s.a. Scholz 2003, 357 ff. m.w.N.

462 *Roßnagel*, ZRP 1997, 26 ff.; s.a. *BT-Enquetekommission Zukunft der Medien* 1998, 60 und 70; *Pitschas*, DuD 1998, 139, 145; Roßnagel-*Roßnagel*, Kap. 3.4, Rn. 17 ff. m.w.N.

meidend und datensparsam, arbeiten.[463] Konzepte der Selbstregulierung (Codes of Conduct und andere)[464] können für eine stärkere Verpflichtung von Unternehmen sorgen, wenn der Staat seiner Ordnungsaufgabe nicht mehr gerecht werden kann. Durch die unabhängige Evaluierung von Anbietern im Rahmen eines Datenschutz-Audits besteht außerdem die Möglichkeit, eine höhere Transparenz für die Betroffenen und einen Wettbewerb um datenschutzfreundliche Technologien zu ermöglichen.[465]

Im Rahmen dieser neuen Ansätze ist dem Recht auf informationelle Selbstbestimmung allerdings mit blindem Glauben weder an die Schutzpotentiale des Rechts, noch an die der Technik Genüge getan. Das Zusammenspiel beider ist vielmehr je nach Schutzgegenstand, -umgebung und -zielrichtung kontextadäquat zu bestimmen. Das impliziert sowohl eine technikorientierte Fortentwicklung des Rechts als auch eine rechtsverträgliche Gestaltung der Technik. Normative Lösungen sind dort wichtig, wo technische Mittel nicht praktikabel sind oder umgangen werden können. Ohne rechtliche Absicherung können staatliche Organe Änderungen an technischen Schutzmechanismen erzwingen.[466] Außerdem kollidiert der Einsatz datenschutzfreundlicher Technik in manchen Bereichen mit Rechten oder Interessen Dritter.[467] In diesen Fällen sind rechtliche Regelungen zum Schutz des Rechts auf informationelle Selbstbestimmung erforderlich.

Nur wenn derartige Unzulänglichkeiten des jeweils gewählten datenschutzrechtlichen Schutzinstrumentariums immer wieder neu in den Blickpunkt gerückt werden, kann dessen Leistungsfähigkeit kontinuierlich weiterentwickelt werden. In einer solchen „Allianz“[468] haben Recht und Technik das Potential, sich zur Förderung der Grundrechtsverwirklichung in ihren jeweiligen Stärken zu ergänzen.

2.5 Methodische Überlegungen

Das Verhältnis von Recht und Technik kann nicht ohne Folgen für die Methodik des Umgangs mit Recht bleiben, wenn es um einen Regelungsbereich geht, der Bezüge zur Technik aufweist. Die rechtswissenschaftliche Methodenlehre befasst sich mit der Anwendung eines Rechtssatzes auf einen Lebenssachverhalt. Nicht notwenig, aber regelmäßig gliedern sich Normen in zwei Teile: Tatbestand und Rechtsfolge.[469] Das Verhältnis der beiden Teile ist in der Regel konditional. Im Wege der Subsumtion bestimmt der Rechtsanwender, ob der Rechtssatz auf den konkreten Sachverhalt anwendbar ist, das heißt letzterer den Tatbestand erfüllt. Ist dies der Fall, tritt eine bestimmte Rechtsfolge ein. Sofern

---

463 Grundlegend *Podlech* 1982, 451 ff.; s. ferner Roßnagel-*Dix*, Kap. 3.5; *Roßnagel* 1994a, 227 ff.; *Roßnagel/Pfitzmann/Garstka* 2001, 39 f.; *Büllesbach/Garstka* 1997, 383 ff.; *Kloepfer* 1998, 99 f.; Simitis-*Bizer*, § 3a Rn. 22 ff.; s.a. unten 4.3.2.

464 Dazu *Bizer*, DuD 2001, 168; *Jacob/Heil* 2002, 213 ff.; Roßnagel-*Roßnagel*, Kap. 3.6.; *ders*. 200b; *Roßnagel/Pfitzmann/Garstka* 2001, 153 ff. (vgl. die Kritik von *Ahrend/Bijok/Diekmann/Eitschberger/Eul/Guthmann/Schmidt/Schwarzhaupt*, DuD 2003, 433, 437 f.); *Schaar*, DuD 2003, 421 ff.

465 Ausführlich Roßnagel-*Roßnagel*, Kap. 3.7.; *ders*. 2000a.; s.a. Simitis-*Bizer*, § 9a Rn. 2 ff.; *Duhr/Naujok/Peter/Seiffert*, DuD 2002, 5, 34.

466 So geschehen beim Anonymisierungsverfahren JAP der TU Dresden, s. *Bäumler/Federrath/Golembiewski* 2003.

467 So ist etwa im Arbeitsumfeld eine vollständige Anonymität der Netzaktivitäten gegenüber dem Arbeitgeber nicht möglich, da dieser zur Kontrolle der Arbeitsleistung und der Verwendung der betrieblichen Mittel in der Lage bleiben muss, s. Roßnagel-*Büllesbach*, Kap. 6.1, Rn. 81. Hier müssen Regeln zum Schutz des Arbeitnehmers und über den Umfang der Kontrollbefugnisse des Arbeitgebers gefunden werden.

468 *Roßnagel* 2001a, 23 ff.; *ders*. 2003, 431 f.

469 Ausführlich *Larenz/Canaris* 1995, 71 ff.; *Röhl* 1994, 220 ff.; *Rüthers* 2005, 96 ff.

Zweifel hinsichtlich des Anwendungsbereichs des Tatbestandes oder des genauen Inhalts der Rechtsfolge bestehen, wird der Inhalt der Norm durch Auslegung konkretisiert.[470]

Mit Hilfe dieser Vorgehensweise ist es möglich, eine bestimmte technische Lösung zu bewerten und eine Aussage darüber zu treffen, ob sie rechtlich zulässig oder unzulässig ist. Das verfassungsrechtliche Verhältnismäßigkeitsgebots verlangt beispielsweise, dass der Staat auf eine Maßnahme, die in Grundrechte eingreift, dann verzichten muss, wenn sie zur Erreichung des angestrebten Ziels nicht erforderlich ist. Daraus kann sich ergeben, dass eine konkrete technische Ausgestaltung eines biometrischen Systems (etwa die zentrale Speicherung aller Referenzdaten) verfassungsrechtlich unzulässig ist. Dieses Ergebnis, also die Entscheidung entlang der Dichotomie der Rechtmäßigkeit oder Rechtswidrigkeit, oder – enger – der Verfassungsmäßigkeit oder Verfassungswidrigkeit, ist das typische Produkt der methodischen Rechtsanwendung.

Unter den beschriebenen Bedingungen des subtilen Einflusses von Technik auf Recht verliert dieses Instrumentarium allerdings mehr und mehr an Effektivität. Zwar treten innerhalb des Normensystems und des Prozesses seiner Handhabung durch den Rechtsanwender keine unmittelbaren Schwierigkeiten auf. Es existieren weiterhin Rechtsnormen, und sie sind auch in der beschriebenen Art und Weise auf technisierte Lebenssachverhalte anwendbar. Dennoch tritt eine Veränderung der Prozesswirkung ein. Statt mehr oder weniger autonom die Regelungsziele zu verwirklichen, die hinter den angewendeten Rechtsregeln stehen, wird der Vorgang der Rechtsanwendung durch die technisch veränderte Wirklichkeit so beeinflusst, dass diese Ziele nicht oder nicht im selben Umfang erreicht werden.[471]

Um dieser Entwicklung zu entgehen, besteht die Möglichkeit, Recht und rechtliche Regelungen nicht nur[472] zur konkreten rechtlichen Bewertung einer konkreten Anwendung anhand einer konkreten Rechtsnorm, sondern auch zur zukunftsorientierten Entwicklung technischer Gestaltungsvorschläge zu verwenden.[473] Die besondere Qualität des Rechts bei der Bestimmung dieser Vorschläge liegt darin, dass es sich bei Rechtsnormen um „Ergebnisse kollektiver demokratischer Selbstbestimmung“ handelt.[474] Die von der Projektgruppe verfassungsverträgliche Technikgestaltung (provet) entwickelte Methode KORA[475] beginnt beispielsweise mit der Bestimmung der Regelungsziele, die hinter einer oder mehrerer Rechtsnormen stehen. Über die Zwischenschritte der rechtlichen Kriterien und technischen Gestaltungsziele werden aus diesen Zielen technische Gestaltungsvorschläge abgeleitet. Existieren mehrere mögliche Technikgestaltungen, so lässt sich dergestalt ermitteln, welche von ihnen die Regelungsziele möglichst optimal verwirklicht.

---

470 Zu den anerkannten Methoden der Auslegung s. *Larenz/Canaris* 1995, 133 ff.; *Röhl* 1994, 628 ff.; *Rüthers* 2005, 447 ff.

471 S.o. 2.4.

472 Die folgenden Ausführungen dürfen keinesfalls als Ersatz für die übliche Form der Rechtsanwendung missverstanden werden. Vorausschauende Technikgestaltung unter Einschluss rechtlicher Technikfolgenforschung kann nicht an die Stelle der (insbesondere gerichtlichen) Rechtmäßigkeitskontrolle konkreter technischer Anwendungen treten, sondern diese nur ergänzen.

473 Grundlegend zum Folgenden *Roßnagel* 1993, 241 ff. et passim; s. ferner *ders.* 1997a, 361 ff.; *ders.*, ZRP 1992, 55 ff.; *Steinmüller* 1993, 595 ff.; *Scholz* 2003, 346 ff.

474 S. *Scholz* 2003, 347. Zumindest im Bereich des Verfassungsrechts sind diese in weiten Bereichen „konsentiert“, was den aus ihnen abgeleiteten Gestaltungsvorschlägen eine hohe Legitimation verschafft.

475 „Konkretisierung rechtlicher Anforderungen“. Die Methode wurde entwickelt in *Hammer/Pordesch/Roßnagel* 1993, 43 ff.; s. ferner *Roßnagel* 1996, 159 f.; *Pordesch/Roßnagel*, DuD 1994, 82, 84 ff.; *Hammer/Pordesch/Roßnagel/Schneider* 1994; *Pordesch* 2003, 257 ff.

Das Ergebnis dieses Prozesses ist das der Rechtsverträglichkeit oder Rechtsunverträglichkeit, oder – enger – der Verfassungsverträglichkeit oder Verfassungsunverträglichkeit. Im Unterschied zur schlichten Rechtsanwendung ist allerdings ein qualitatives Urteil über eine Technologie oder Anwendung möglich. Eine Anwendung kann mit anderen Worten niemals „rechtmäßiger", wohl aber „rechtsverträglicher" sein, weil sie ein Regelungsziel besser erfüllt als andere Anwendungen.[476] Diese Form des Umgangs mit Recht setzt einerseits früher, nämlich nicht erst bei Rechtsnormen, sondern bereits bei den hinter ihnen liegenden Regelungszielen an.[477] Gleichzeitig führt sie die Analyse aber auch weiter, weil sie in der Lage ist, noch innerhalb der Kategorie der Rechtmäßigkeit weiter zu differenzieren. Schließlich ist sie zukunftsorientiert, weil sie auf etwas Einfluss zu nehmen sucht, das bislang noch nicht als rechtmäßig oder rechtswidrig zu beurteilen ist, weil es zum einen noch nicht existiert und zum anderen in seiner Existenz möglicherweise auf neue und veränderte Rechtsnormen treffen wird.

Betrachtet man vor diesem Hintergrund den Gegenstand dieser Arbeit, so sind Chipkartenausweise ein Beispiel dafür, wie technische Entwicklungen den Lebensalltag der Betroffenen und die Verwirklichungsbedingungen von Recht verändern können. Das gilt insbesondere für die elektronische Gesundheitskarte, die viele Versicherte sehr häufig verwenden werden und das Arzt-Patient-Verhältnis in seiner sozialen und rechtlichen Ausgestaltung vor ganz neue Herausforderungen stellen wird. Gleichzeitig ist jedoch in den Ausführungen zu den technischen Grundlagen bereits deutlich geworden, dass die Verfahren und Systeme, die bei Chipkartenausweisen zum Einsatz kommen werden, schon heute verfügbar sind und teilweise sogar schon verwendet werden.[478] Das gilt für die Chipkarten selbst und für die auf ihnen ablaufenden Applikationen, also elektronische Signatur, Verschlüsselung und Authentisierung einerseits, biometrische Verfahren andererseits.

Überdies wird über den Einsatz dieser Medien und Verfahren in relativ kurzen Zeiträumen entschieden werden. Die elektronische Gesundheitskarte und das JobCard-Verfahren sollten ursprünglich zum 1. Januar 2006 eingeführt werden; für den digitalen Personalausweis war sogar für das Jahr 2004 ein Gesetzgebungsverfahren angekündigt worden.[479] Sofern technische Fortentwicklungen noch zu erwarten sind, werden diese sich im Bereich der Steigerung der Speicher- und Rechenkapazitäten der Chips, beziehungsweise der Verbesserung der Erkennungssicherheit biometrischer Verfahren bewegen. Eine grundlegend neue Funktionsweise von Trägermedien und Applikationen ist kaum zu erwarten. Die vorliegende Analyse muss sich an diesem sehr knappen Zeithorizont orientieren. Gefordert ist deshalb nicht die Entwicklung von Regelungszielen, die in einem langfristigen Prozess eine Technologie oder einen stark technisierten Lebensbereich mitgestalten helfen. Vielmehr bewegt sich die Arbeit – trotz ihres starken Bezugs zur fortschreitenden Einführung von Informations- und Kommunikationstechnologien in immer mehr Lebensbereichen – methodisch ganz überwiegend im rein normativen Bereich; analysiert werden Fragen der Rechtmäßigkeit, nicht der Rechtsverträglichkeit. Nur dort, wo die Analyse unter Berück-

476 Übertragen auf die Verfassung bedeutet das insbesondere, dass Verfassungsverträglichkeit nicht identisch mit Verfassungsmäßigkeit und nicht das Gegenteil von Verfassungswidrigkeit ist, s. näher *Roßnagel/Wedde/Hammer/Pordesch* 1990, 7.

477 In Ansätzen ist dies (in Form der historischen und der teleologischen Auslegung) auch bei der „normalen" Rechtsanwendung möglich. Beide sind jedoch durch den Wortlaut als äußerste Auslegungsgrenze beschränkt, vgl. *Larenz/Canaris* 1995, 163, 141 ff.

478 S.o. 2.2.

479 Bei allen Projekten gibt es mittlerweile Verzögerungen. Die elektronische Gesundheitskarte wird 2006 voraussichtlich nur für ca. 100.000 Patienten in Testregionen verfügbar sein, (s.o. 2.1.2), das JobCard-Verfahren frühestens 2007 den Betrieb aufnehmen (s.o. 2.1.3). Dieses Jahr wird nunmehr auch als Starttermin für den digitalen Personalausweis genannt (s.o. 2.1.1).

sichtigung aller Rechtmäßigkeitskriterien (insbesondere auch der Verhältnismäßigkeit) tatsächlich mehrere zulässige technische Lösungen ergibt, erfolgt ein Vorschlag für diejenige Lösung, die verfassungsrechtliche und einfachgesetzliche – insbesondere datenschutzrechtliche – Anforderungen vorbildlich umsetzt.

3 Internationale Entwicklungen

Die Einführung von Chipkartenausweisen wird nicht nur in Deutschland, sondern nahezu in jedem Staat weltweit diskutiert. Insbesondere beim digitalen Personalausweis ist Deutschland – anders als bei der Einführung der bisherigen, maschinenlesbaren Variante – im internationalen Vergleich nicht Vorreiter, sondern eher Nachzügler.[480] Dagegen gibt es bisher kein Land, in dem eine elektronische Gesundheitskarte mit ähnlichen Neuerungen wie im GKV-Modernisierungsgesetz festgeschrieben im Einsatz ist.[481] Für diese international „Patient Data Cards" genannten Chipkarten plant jedoch eine größere Zahl der Industrienationen Projekte, die dem deutschen vergleichbar sind. Ein dem geplanten JobCard-Verfahren ähnliches Projekt gibt es im Ausland nicht.

Der in diesem Kapitel gegebene Überblick dient dazu, die deutsche Debatte über die Chancen und Gefahren und die rechtliche Zulässigkeit von Chipkartenausweisen besser einordnen und bewerten zu können. Die Übersicht erfolgt mit einer Reihe von Einschränkungen:

- Projekte zur Einführung biometrischer Daten auf Reisepässen bleiben außer Betracht. Auf Druck der USA und unter dem Einfluss der ICAO planen nahezu alle Länder weltweit entsprechende Änderungen ihrer Reisedokumente. Behandelt werden also (nur) nationale Identifikationsdokumente. Biometrische Kartenlösungen ohne Chip werden nur am Rande erwähnt.
- Sektorielle Karten im Gesundheitswesen (beispielsweise Teillösungen für bestimmte Patientengruppen) bleiben außen vor.[482] Gleiches gilt für Chipkarten, die wie die bisherige Krankenversichertenkarte in Deutschland lediglich administrative Daten speichern,[483] und für allgemeine Projekte zur Einführung von Telematik im Gesundheitswesen (insbesondere elektronische Patientenakten oder „Electronic Health Records").[484]
- International werden bisweilen reine Signaturkarten, die in Deutschland schon länger angeboten werden, als „Electronic Identity Cards" bezeichnet. Daran ist richtig, dass mit den Funktionalitäten dieser Karten ein elektronischer Identitätsnachweis möglich ist. Thema dieser Arbeit sind jedoch Chipkartenausweise, die über eine reine Signaturfunktion hinausgehen, nicht allgemeine Strategien zur Einführung von Signaturkarten.
- Es erfolgt keine ausführliche Darstellung der technischen Details und Funktionsweise. Soweit ersichtlich, entsprechend die Ausweiskarten durchgängig der ISO/IEC 7816-Serie und international gültigen Normen zu Signaturen und Zertifikaten.[485]

---

480 S. für den Personalausweis zum Folgenden bereits *Hornung*, DuD 2005, 62 ff.; *ders*., in: Reichl/Roßnagel/Müller 2005, 17 ff. (Stand Januar 2004).

481 Deutschland war auch bei der aktuellen Krankenversichertenkarte weltweit Vorreiter, s. *BSI* 1995, 14.

482 Schon vor 1995 gab es hierzu in Europa (überwiegend in Frankreich) etwa zwei Dutzend Feldversuche, s. *BSI* 1995, X; zum Stand Ende 2002 vgl. *eESC/TB11 Health* 2003, 49 ff.; zu frühen Bsp. aus dem Ausland s.a. *Wellbrock*, DuD 1994, 70, 71 f.; *Stark/Wohlmacher*, DuD 1997, 595; *Iwansky* 1999, 46 ff.; *Fuest* 1999, 167 f. m.w.N.

483 Das ist bei einer Vielzahl europäischer Krankenversichertenkarten der Fall, s. die Übersichten der *Europäischen Kommission*, KOM(2003) 73, 5 f., 18 ff. und von *eESC/TB11 Health* 2003, 49 ff.

484 S. etwa für den Stand des Jahres 2001 *Goetz* 2001, 129 ff. Verallgemeinernd lässt sich festhalten, dass Staaten mit zentral organisierten Gesundheitssystemen und ohne Selbstveraltungsmechanismen bei der Einführung von Telematik schneller voranschreiten.

485 S. insoweit unten 6.1.2.

Auch unter diesen Einschränkungen erhebt der folgende Überblick keinen Anspruch auf Vollständigkeit. Hierzu sind Vorhaben, Pläne, Pilotprojekte, Auftragsvergaben und Implementierungsprozesse zu schnelllebig. Basis für die Untersuchung waren zum einen eine Auswertung einschlägiger Berichte aus Literatur und Internet, zum anderen (für die Teile zu Personalausweisen) ein ausführlicher Fragebogen, der im Laufe des Jahres 2003 an Ansprechpartner in 15 Staaten versandt und von diesen beantwortet wurde.[486] Der Überblick gibt den Stand Mai 2005 wieder.

3.1 Überstaatliche Aktivitäten

3.1.1 Die internationale Vereinheitlichung von Reisedokumenten

Weltweit gibt es eine Vielzahl von Aktivitäten zur Vereinheitlichung von Reisedokumenten und ihrer Erweiterung um biometrische Daten. Die wichtigste internationale Organisation für die Vereinheitlichung von Reisedokumenten ist die International Civil Aviation Organisation (ICAO).[487] Die Convention on International Civil Aviation (oder Chicago Convention) wurde am 7. Dezember 1944 von 52 Staaten unterzeichnet. Da sie erst nach der Ratifikation durch 26 Staaten in Kraft treten konnte, wurde für eine Übergangszeit die Provisional International Civil Aviation Organization (PICAO) eingerichtet. Nachdem am 5. März 1947 die 26. Ratifikation erfolgte, nahm die ICAO am 4. April 1947 in Montreal ihre Arbeit auf. Im Oktober desselben Jahres wurde sie zu einer Unterorganisation der Vereinten Nationen und ist dort dem Economic and Social Council (ECOSOC) zugeordnet. Heute gehören der ICAO 187 Vertragsstaaten an; die Bundesrepublik Deutschland ist seit dem Jahre 1956 Mitglied.

Die Aufgabe der ICAO ist die Erarbeitung und Weiterentwicklung von einheitlichen Regelungen für die Sicherheit, Regelmäßigkeit und Wirtschaftlichkeit des internationalen Luftverkehrs, dessen Planung und Entwicklung gefördert werden sollen (Art. 44 Chicago Convention). Zur Erreichung dieser Ziele beschließt die Organisation Richtlinien (Standards) und Empfehlungen (Recommendations), die zum überwiegenden Teil in den 18 Anhängen zum Abkommen enthalten sind. Nach Art. 37 (j) Chicago Convention beschäftigt sich die ICAO auch mit Zoll- und Einreisebestimmungen.

Für ihre Aktivitäten im Bereich von Reisedokumenten beruft sich die ICAO auf Art. 13, 22 und 37 (j) Chicago Convention.[488] Es ist überaus zweifelhaft, ob hieraus eine rechtliche Grundlage abgeleitet werden kann. Art. 13 Chicago Convention schafft keine Kompetenz, sondern verpflichtet lediglich Staaten und Individuen (unter anderem dazu, die Passvorschriften jedes Unterzeichnerstaats einzuhalten). Art. 22 Chicago Convention verbietet den Staaten unnötige Verzögerungen bei der Einreise. Auch hieraus kann keine Befugnis für die ICAO abgeleitet werden. Damit verbleibt als normative Basis Art. 37 (j) Chicago Convention, der jedoch Reisepapiere zumindest nicht ausdrücklich nennt. Im Ergebnis spricht einiges dafür, dass sich mit der ICAO und ihren Gremien lediglich ein faktisches Plenum zur Vereinheitlichung dieser Papiere gefunden hat. Da die Organisation jedoch mittlerweile auf eine mehr als fünfzigjährige Tradition der Standardisierung in diesem Bereich zu-

---

486 Der Fragebogen ist im Anhang abgedruckt.

487 Nähere Informationen unter http://www.luftrecht-online.de/einzelheiten/verwaltung/icao.htm; http://www.icao.int/mrtd/Home/Index.cfm; s.a. *LSE* 2005, 21 ff. Daneben hat bspw. die Gruppe der Acht (G8) unter der Führung der USA und Frankreichs eine Arbeitsgruppe zur Bewertung der Verwendbarkeit von Biometrie im Rahmen der Terrorismusbekämpfung ins Leben gerufen, s. http://www.heise.de/newsticker/meldung/32991.

488 S. *ICAO* 2004c, 5.

rückblickt und nahezu ausnahmslos alle Staaten weltweit ihre Richtlinien befolgen, schmälert das die Wichtigkeit der ICAO nicht. Sie ist vielmehr die entscheidende Instanz für die weitere Entwicklung aller internationalen Reisedokumente.

Die ICAO ist in eine Versammlung (Assembly) und einen Rat (Council) organisiert. Darüber hinaus gibt es Ausschüsse, die Beschlussvorlagen erarbeiten. Die Versammlung, in der jedes Mitglied über eine Stimme verfügt (Art. 48 Chicago Convention), wählt den Rat, der aus Vertretern von 33 Vertragsstaaten besteht. Die entsendenden Staaten repräsentieren nach Art. 50 (b) Chicago Convention drei Gruppen, nämlich die wichtigsten Staaten im Bereich des Luftverkehrs, die Staaten mit den größten Beiträgen zur Vorhaltung von Luftfahrteinrichtungen und andere Staaten, deren Mitwirkung im Rat die Vertretung aller wichtigen Regionen der Welt sicherstellen soll. Diese Aufteilung hat dazu geführt, dass Deutschland seit 1959 im Rat vertreten ist und aktiv in seinen verschiedenen Ausschüssen mitarbeitet.

Die Richtlinien und Empfehlungen der ICAO wirken nicht unmittelbar, sondern nur nach einer Umsetzung durch die Mitgliedstaaten. Nach Art. 38 Chicago Convention sind nationale Abweichungen von den Richtlinien der ICAO anzuzeigen. Es besteht keine durchsetzbare Verpflichtung, Richtlinien und Empfehlungen umzusetzen. Allerdings haben sich die Mitgliedstaaten in Art. 37 Chicago Convention verpflichtet, zu einem Höchstmaß an Einheitlichkeit beizutragen.

Das grundlegende Dokument der ICAO für Reisepapiere ist das dreiteilige ICAO DOC 9303 on Machine Readable Travel Documents, welches seit dem Jahre 1980 ständig fortentwickelt wird und Vorgaben für maschinenlesbare Reisedokumente enthält.[489] Nach den Anschlägen des 11. September 2001 hat die ICAO ihre Aktivitäten zur Einführung biometrischer Daten beschleunigt.[490] Ihre New Technology Working Group empfahl anlässlich eines Treffens in Berlin im Juni des Jahres 2002 den Staaten, das Gesichtsbild als verpflichtendes Merkmal zu speichern und es jedem Land zu überlassen, zusätzlich Fingerabdruck und/oder Irisdaten aufzunehmen.[491] Dies wurde in der so genannten „New Orleans Resolution" vom März des Jahres 2003 bestätigt.[492]

Aufgrund der höheren Übertragungsrate und der geringeren Verschleißerscheinungen sollen kontaktlose Schnittstellen verwendet werden.[493] Außerdem spricht sich die ICAO für die Speicherung biometrischer Volldatensätze aus, weil proprietäre Templates eine weltweite Prüfbarkeit der Daten verhindern würden.[494] Überlegungen gibt es auch zum Aufbau einer weltweiten PKI zur Absicherung der elektronisch gespeicherten Ausweisdaten.[495] Ein Technical Report beschäftigt sich mit der logischen Struktur dieser Daten, um ihre Interoperabilität mit allen Lesegeräten weltweit sicherzustellen.[496] Die ICAO ist bei ihren Aktivitäten eng mit der International Organization of Standardization (ISO) verflochten. Frühere Versionen des DOC 9303 wurden als ISO-Standards (ISO/IEC 7501-1, -2, -3) verabschiedet; umgekehrt bezieht die ICAO die Standardisierungsbemühungen des ISO SC 37 in ihre Arbeiten mit ein.

489 *ICAO* 1994, 2002, 2003a.
490 S. zu den Aktivitäten der ICAO den Überblick bei *Hornung* 2004b, 48 f. und näher unten 6.1.2.
491 Vgl. *ICAO* 2004a, 17.
492 S. http://www.icao.int/mrtd/download/documents/TAG%2014%20-%20Report.pdf, Nr. 3.3.3.
493 S. *ICAO* 2004e, 35; ausführlich *ICAO* 2004b.
494 *ICAO* 2004a, 31 ff.
495 S. *ICAO* 2004d; näher zum Konzept unten 6.2.1.1.
496 *ICAO* 2004c. Der Bericht behandelt auch die Speicherung auf optischen Speichern und Barcodes.

3.1.2 Europäische Initiativen

Die Europäische Union befasst sich sowohl mit den Entwicklungen im Bereich von Personalausweisen als auch von Gesundheitskarten. Der Europäische Rat hatte zunächst am 17. Oktober 2000 Mindest-Sicherheitsstandards für fälschungssichere Reisedokumente beschlossen.[497] Im Anschluss daran legte die Kommission einen Vorschlag für eine Verordnung über Normen für Sicherheitsmerkmale und Biometrie in Pässen der EU-Bürger vor.[498] Dieser sah vor, entsprechend den Plänen der ICAO Gesichtsdaten in den Pässen zu speichern; jeder Staat sollte daneben beschließen können, zusätzliche biometrische Merkmale zu benutzen.[499] Der Rat entschied sich jedoch, den Mitgliedstaaten sowohl die Speicherung von Gesichts- als auch von Fingerabdrucksdaten verbindlich vorzuschreiben.[500] Die entsprechende Verordnung (EG) Nr. 2252 wurde am 13. Dezember 2004 beschlossen.[501] Dem ging gemäß Art. 67 Abs. 1 EGV eine Anhörung des Europäischen Parlaments voraus. Dieses hatte sich für eine Beschränkung auf Gesichtsdaten ausgesprochen.[502] Es besitzt im Verfahren nach Art. 67 Abs. 1 EGV jedoch keine weiteren Befugnisse, sodass der Rat sein Votum unbeachtet lassen konnte. Die Verordnung ist in Deutschland unmittelbar geltendes Recht und verpflichtet zu einer Änderung des Reisepasses.[503] Dagegen hat die Europäische Union derzeit keine Regelungskompetenz für den Personalausweis; Art. 62 Nr. 2 lit. a EGV ist auf den Pass beschränkt.[504] Allerdings enthält Art. III-125 Abs. 2 des Vertrages für eine Verfassung für Europa[505] eine Kompetenznorm auch für Personalausweise. Nach der – derzeit noch unsicheren – allseitigen Ratifizierung des Vertrages könnte der Rat einstimmig nach Anhörung des Europäischen Parlaments durch ein Europäisches Gesetz oder Rahmengesetz „Maßnahmen, die Pässe, Personalausweise, Aufenthaltstitel oder diesen gleichgestellte Dokumente betreffen", beschließen.

Außer den neuen Reisepässen wird in Europa auch ein einheitliches EU-Visum mit biometrischen Daten eingeführt.[506] Pilotverfahren hierzu gibt es unter anderem in Deutschland,[507] Großbritannien[508] und Frankreich.[509] Zur Vermeidung von Doppelanträgen werden die Daten in der zentralen Datenbank EURODAC gespeichert.[510]

---

497 Anhang 1 zur Entschließung des Rats v. 17.10. 2000, ABl. EG C 310/1.

498 S. *Europäische Kommission*, KOM(2004) 116.

499 Vgl. Art. 1 Abs. 2 des Entwurfs.

500 Auch die internationale Entwicklung scheint zur Kombination von Gesichts- und Fingerabdrucksdaten zu gehen; s. etwa für die USA http://europa.eu.int/idabc/en/document/3827/194.

501 ABl. EG 2004 L 385/1; s. *Roßnagel/Hornung*, DÖV 2005, i.E.; s.a. *LSE* 2005, 25 f.; *Kügler*, c't 5/2005, 84 ff.; *Der Bundesbeauftragte für den Datenschutz* 2005, 81.

502 Vgl. die Stellungnahme des Berichterstatters *Coelho*, Doc. A6-0028/2004, abrufbar unter http://www2.europarl.eu.int/omk/sipade2?L=DE&OBJID=90292&LEVEL=4&MODE=SIP&NAV=X&LSTDOC=N; s.a. den Standpunkt der *Art. 29 DPWP* (2004).

503 S. dazu unten 4.2.2.2 (Fn. 1034); zum Inhalt der Verordnung vgl. *Roßnagel/Hornung*, DÖV 2005, i.E.

504 Das ist auch die Position der *Europäischen Kommission*, s. KOM(2004) 116, 5; die Verordnung (EG) Nr. 2252 findet dementsprechend gemäß Art. 1 Abs. 3 Satz 2 keine Anwendung auf Personalausweise.

505 ABl. EU C 310 v. 16.12.2004, S. 1.

506 http://www.heise.de/newsticker/meldung/37870.

507 Bisher in Lagos (Fingerabdruck) und Manila (Iris), s. http://www.heise.de/newsticker/meldung/38877.

508 Vgl. http://www.heise.de/newsticker/meldung/39821.

509 In sieben Städten weltweit, s. http://europa.eu.int/idabc/en/document/3794/194.

510 Beschlossen durch Verordnung (EG) Nr. 2725/2000 des Rates v. 11.12.2000 über die Einrichtung von „Eurodac" für den Vergleich von Fingerabdrücken zum Zwecke der effektiven Anwendung des Dubliner Übereinkommens, ABl. EG L 316, 15.12.2000, weiter ausgeführt durch Verordnung (EG) Nr. 407/2002 v. 28.2.2002 zur Festlegung von Durchführungsbestimmungen zur Verordnung (EG) Nr. 2725/2000, ABl. EG L 62, 5.3.2002; s. z.B. *Golembiewski/Probst* 2003, 10 f.; *TAB* 2004, 11 ff.

Auf Aufforderung des Europäischen Rates[511] hat die Kommission am 17. Februar 2003 eine Mitteilung zur Einführung einer europäischen Krankenversicherungskarte vorgelegt.[512] Ziel ist die Förderung der Mobilität der europäischen Bürger und die Vereinfachung der Verwaltungsabläufe bei der Kostenerstattung. Beides wird bislang durch nicht miteinander kompatible Systeme der Mitgliedstaaten behindert.[513] Geplant war ein dreistufiges Vorgehen:

- Im ersten Schritt wird eine europäische Krankenversichertenkarte als Sichtausweis eingeführt. Die Ausgestaltung soll den Mitgliedstaaten überlassen bleiben; denkbar wäre eine Kombination mit nationalen Versicherungskarten oder die Einführung einer einheitlichen europäischen Karte. Die Kommission spricht sich – vorsichtig – für die zweite Lösung aus.[514] Zunächst wird der Vordruck E 111 (für Reisen) ersetzt. Diese Phase sollte am 1. Juni 2004 beginnen. Zu diesem Zeitpunkt wurde der Start des Projekts in zwölf Mitgliedstaaten offiziell bekannt gegeben.[515] Allerdings geben diese noch nicht alle entsprechende Karten aus. Die Planungen sind indes weit fortgeschritten.
- Bis Ende des Jahres 2005 sollen auch die weiteren Formulare ersetzt werden. Dabei handelt es sich um die Vordrucke E 128 (Studium, Entsendung von Arbeitnehmern), E 110 (internationales Verkehrswesen) und E 119 (Arbeitssuche). Gleichzeitig soll die Übergangsphase enden, in der noch papierne Vordrucke akzeptiert werden.
- Im dritten Schritt ist Ende des Jahres 2008 die Speicherung aller Vordrucke auf elektronischen Trägern geplant. Außerdem sollen die Ansprüche aller Versicherten angeglichen werden, die sich in einen anderen Mitgliedstaat begeben.[516]

Neben diesen spezifischen Aktivitäten gibt es innerhalb der Europäischen Union eine Reihe von Organisationen, die sich mit der Förderung und Verbreitung von Chipkarten und Signaturverfahren beschäftigen. Die Initiative „eEurope“ wurde 1999 auf Betreiben der Europäischen Kommission gegründet. Eine ihrer Unterinitiativen ist eEurope SmartCards. Diese hat das Ziel der „Förderung der intelligenten Chipkarten in der EU“.[517] Eine Arbeitsgruppe hat Minimalanforderungen an einen amtlichen digitalen Ausweis beschrieben.[518]

Die European Electronic Signature Standardisation Initiative (EESSI)[519] führt Standardisierungsaktivitäten durch, um die Umsetzung der Signaturrichtlinie[520] zu unterstützen. Unter der Leitung eines Steering Committees bringt die Initiative Industrie, Nutzergruppen, nationale Behörden und interessierte Organisationen zusammen. Im Standardisie-

511 Dieser hatte im März 2002 in Barcelona die Einführung einer europäischen Krankenversichertenkarte beschlossen, s. *eESC/TB11 Health* 2003, 50.

512 *Europäische Kommission*, KOM(2003) 73.

513 Allerdings gibt es bereits grenzüberschreitenden Initiativen wie das deutsch-französische „Netzlink“ oder die deutsch-niederländische „GesundheitsCard international“, s. *eESC/TB11 Health* 2003, 63 ff.

514 *Europäische Kommission*, KOM(2003) 73, 13 f.

515 Vgl. http://europa.eu.int/idabc/document/2589/194.

516 Bislang haben einige Gruppen von Personen Ansprüche auf alle „unmittelbar erforderlichen“, andere auf alle „erforderlichen“ Leistungen; s. näher *Europäische Kommission*, KOM(2003) 73, 11 f.

517 S. http://eeurope-smartcards.org/ und http://www.electronic-identity.org/.

518 http://www.fineid.fi/download/scc/TB1-reqs06.02.02ver_0.14.pdf.

519 S. http://www.ictsb.org/EESSI_home.htm.

520 Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates v. 13.12.1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen, ABl. EG L 13 v. 19.1.2000, 12.

rungsbereich ist der CEN/ISSS Electronic Signature Workshop tätig.[521] Daneben besitzt das European Telecommunications Standards Institute (ETSI) eine Arbeitsgruppe zum Thema Infrastruktur für elektronische Signaturen, die sich mit technischen Standards und Sicherheitsanforderungen befasst.[522] Weitere Organisationen sind das European Biometric Forum (EBF),[523] das internationale PKI-Forum,[524] die IETF-PKIX Working Group[525] und die European Smart Card Industry Association (EUROSMART).[526] Das Projekt „Digital Passport", das teilweise durch das IST Programm der Europäischen Kommission finanziert wird, strebt die Entwicklung einheitlicher europäischer Lösungen für Reisepässe mit Biometrie an.[527]

3.2 Staaten mit eingeführten Chipkartenausweisen

Mit Finnland, Estland und Belgien gibt es mittlerweile drei europäische Staaten mit Personalausweisen, die über einen Chip verfügen.[528] Im Nahen Osten und in Asien lassen sich fünf weitere Beispiele (Brunei, Oman, Hongkong, Macao und Malaysia) finden. Elektronische Gesundheitskarten wurden in Frankreich und in Taiwan eingeführt.

3.2.1 Europäische Staaten

3.2.1.1 Finnland

Die Finnish Electronic Identification (FINEID) ist das weltweit erste Beispiel für eine Verbindung von Personalausweis und Signaturkarte.[529] Nach einem Pilotprojekt, das im Jahre 1998 begann, wurden zunächst bis Mitte des Jahres 2001 30.000 Karten an Beamte und danach bis Ende November des Jahres 2004 ca. 53.000 Karten an Privatleute ausgestellt. Die FINEID ist ein vollgültiger Ausweis und EU-Reisedokument. Ausländer können die Karte nach sechs Monaten Aufenthalt erhalten. Ihre Rechtsgrundlagen bilden der Population Information Act 1993, der Act on Electronic Service in the Administration 1998 und der Identity Card Act 1999.[530]

In Finnland besteht keine Personalausweispflicht. Außerdem wurde der bisherige Ausweis zunächst parallel zur FINEID angeboten. Um die Verwendung auch für Personen zu ermöglichen, die nicht über einen Kartenleser oder Internetanschluss verfügen, wurden über 300 Informationskioske im öffentlichen Raum installiert.

Das Ausgabeverfahren beginnt mit einem Antrag, der bei der lokalen Polizeibehörde gestellt wird. Diese gibt die Daten in ein zentrales Personeninformationssystem ein und sendet den Antrag an die Karten herstellende Firma (Setec). Setec bestellt mit den Angaben des Informationssystems beim Population Register Centre das Zertifikat, erstellt die

---

521 S. http://www.cenorm.be/isss; zu den verschiedenen Standardisierungsaktivitäten s.a. unten 6.1.2.
522 S. http://www.etsi.org/.
523 S. hierzu *Albrecht*, DuD 2003, 571; http://www.eubiometricforum.com/.
524 http://www.pkiforum.org/.
525 S. http://www.ietf.org/html.charters/pkix-charter.html.
526 Vgl. http://www.eurosmart.com.
527 S. näher http://www.eudigitalpassport.com/ und http://europa.eu.int/ida/en/document/3451/194.
528 Vgl. zur folgenden Staatenübersicht (für den Personalausweis) schon *Hornung*, in: Reichl/Roßnagel/Müller 2005, 17 ff.; *ders*., DuD 2005, 62 ff.
529 Für allgemeine Informationen vgl. http://www.fineid.fi; s.a. *Marzetta/Stöckle/Vaterlaus* 2001, 26 ff., 65 ff.; zu Pilotprojekten http://www.tml.hut.fi/Opinnot/Tik-110.501/1999/papers/legislation/legislation.html. Fragen zur FINEID wurden von *M. Pohjolainen* vom finnischen Population Register Centre beantwortet.
530 Die Gesetze sind abrufbar unter http://www.fineid.fi (in finnischer Sprache).

Karte und schickt sie zurück an die Polizeibehörde. Die PIN geht mit der Abholaufforderung dem Antragsteller direkt zu. Das gesamte Verfahren dauert etwa zehn Tage. Das (staatliche) Population Register Centre ist der einzige Zertifizierungsdiensteanbieter im System, hat aber nahezu alle Funktionen (Kartenproduktion, Zertifikatserstellung, Help-Desk, Verzeichnis- und Sperrdienst) an private Anbieter abgegeben. Außerdem gibt es weitere private Zertifizierungsdiensteanbieter in Finnland, die eigene Karten vertreiben. Die FINEID kostet für den Inhaber 29,- Euro für drei Jahre (im Vergleich dazu betrug die Gebühr des herkömmlichen Ausweises 26,- Euro für zehn Jahre). Außerdem fallen Zusatzkosten von ca. 70,- Euro an, um den häuslichen Arbeitsplatz mit der benötigten Hard- und Software auszustatten. Das Pilotprojekt kostete den Staat ca. 340.000 Euro, der Aufbau der PKI später etwas über 2 Millionen Euro. Die Betriebskosten betragen ca. 4 Millionen Euro pro Jahr.

Auf der Kartenoberfläche befinden sich Name, Geschlecht, Nationalität, Geburtstag und Sozialversicherungsnummer des Inhabers. Diese Daten sind aber nicht elektronisch auf dem Kartenchip gespeichert, dieser dient vielmehr nur als Aufbewahrungsort für die Signatur- und Authentisierungsschlüssel und das Zertifikat. Letzteres enthält den Namen und den FINUID (Finnish unique identifier, die staatliche Personenkennziffer) des Inhabers. Für die Zukunft ist daran gedacht, eine Email-Adresse optional aufzunehmen. Es werden bislang keine biometrischen Daten verwendet. Die Regierung plant jedoch, ab dem Jahre 2007 wie beim Reisepass Gesichts- und Fingerabdrucksdaten zu speichern.

Bei der Einführung der FINEID gab es so gut wie keine Akzeptanzprobleme. Gründe hierfür werden in der Gestaltung des Einführungsprozesses gesehen. Von Beginn an fand eine fortwährende Information der Bevölkerung statt. Außerdem wurde die politische Opposition intensiv an der Entscheidungsfindung beteiligt. Der Ombudsmann für den Datenschutz nahm am Verfahren teil, und seine Anmerkungen wurden für die Gestaltung des Projektes berücksichtigt. Schließlich wurden wichtige Persönlichkeiten des öffentlichen Lebens wie der Premierminister und führende Personen aus Regierung und Wirtschaft in die Vermittlung des Pilotprojekts mit einbezogen.

Trotz der Position Finnlands als Vorreiter einer neuen Generation von Ausweisen und der reibungslosen Einführung wird das Projekt inzwischen kritisch gesehen. Der niedrige Verbreitungsgrad der Karte wird auf eine Reihe von Gründen zurückgeführt, insbesondere auf die zunächst parallele Existenz des alten Personalausweises. Das Land stellt deshalb mittlerweile den Ausweis nur noch mit Chip aus. Außerdem schrecken die Zusatzkosten potentielle Nutzer ab, solange es zu wenige Einsatzmöglichkeiten für die Signaturfunktion gibt. Allgemein scheint die Nachfrage nach Anwendungen im Bereich des Electronic Government geringer zu sein als erwartet. Bemängelt wird aber auch eine unzureichende Unterstützung des Projekts durch die staatlichen Behörden.

Für die Zukunft gibt es Pläne, die Strategie des Population Register Centre grundlegend zu ändern. Die Arbeit soll mehr auf den Bürger zugeschnitten werden. Außerdem werden eine Vereinfachung des Antragsverfahrens und eine Erhöhung der Anwendbarkeit der Karte im öffentlichen Raum angestrebt. Aufgrund der geringen Verbreitung wurde im Frühjahr 2004 ein Online-Identifikationssystem für den Zugang zu Electronic Government-Anwendungen eingerichtet, das nicht auf der FINEID basiert.[531] Entgegen anders lautenden Berichten[532] bedeutet dies jedoch keinen Abbruch des Chipkartenprojekts.[533]

531 S. http://europa.eu.int/idabc/document/2434/194.

532 Vgl. OMNICARD-Newsletter August/2003.

533 Auskunft von *M. Pohjolainen*, Population Register Center; s.a. die Richtigstellung in OMNICARD-Newsletter September/2003.

Schließlich besteht seit Juni des Jahres 2004 die Möglichkeit, die Daten der finnischen Sozialversicherungskarte auf der FINEID zu speichern und so nur eine statt zwei Karten besitzen zu müssen.[534] Auf Intervention des Ombudsmanns für den Datenschutz wurde in das entsprechende Gesetz allerdings eine Norm aufgenommen, nach der jedermann entscheiden kann, ob Daten der Sozial- und Gesundheitsverwaltung in die Karte integriert werden.[535]

3.2.1.2 Estland

In Estland werden nach Abschluss einiger Pilotprojekte seit dem 28. Januar 2002 Personalausweise im Chipkartenformat mit Signaturfunktion an Bürger ab dem 16. Lebensjahr ausgegeben.[536] In Estland herrscht Ausweispflicht, und diese wird auf die Signaturfunktion erstreckt. Das Land ist damit neben Macao[537] das einzige weltweit, welches den Weg einer verpflichtenden Einführung einer Signaturkarte geht.

Neben Esten erhalten Ausländer mit einer Aufenthaltsgenehmigung von mindestens einem Jahr die Karte. Die Rechtsgrundlagen für das Projekt finden sich im Identity Documents Act vom 15. Dezember 1999 und in der Verordnung Nr. 370 der Regierung über Format, technische Einzelheiten und Daten der Karte vom 4. Dezember 2001. Auf die Signaturfunktion des Ausweises findet das estische Signaturgesetz vom 8. März 2000 Anwendung. Auch wenn bislang noch nicht viele Anwendungen zur Verfügung stehen, gibt es doch bereits ein Gerichtsurteil, das die Rechtsverbindlichkeit elektronischer Signaturen in Estland bestätigt.[538] Die Zahl der abgegebenen Karten betrug Mitte Mai des Jahres 2005 760.000 Stück.[539]

Als Besonderheit enthält das Authentifizierungszertifikat eine durch die Regierung vergebene offizielle Email-Adresse,[540] die von jeder öffentlichen Stelle, aber auch von jeder Privatperson genutzt werden kann, um Emails an den Inhaber zu senden. Seit Mitte des Jahres 2003 besteht ein Portal im Gesundheitswesen, über das unter Verwendung des Ausweises medizinische Daten online eingesehen werden können.

Am Verfahren sind drei Akteure beteiligt: das Estonian Citizenship and Migration Board (CMB) als staatliche Behörde, AS Sertifitseerimiskeskus (SK) als einziger Zertifizierungsdiensteanbieter im System[541] und die TRÜB Baltic AS als Kartenhersteller. Der Bürger füllt den Antrag aus und benennt eine Bankfiliale, bei der er die Karte erhalten möchte. CMB erhält den Antrag (dieser verbleibt dort) und übermittelt die Daten zur TRÜB. Diese stellt die Karte her, generiert in ihr die geheimen Schlüssel, bereitet die Umschläge mit den beiden PINs und der PUK vor und bestellt die Zertifikate. SK stellt diese aus, nimmt sie in ihr Verzeichnis auf und übersendet sie an die TRÜB, wo sie zusammen mit dem Personendatensatz auf den Chip aufgespielt werden. Die TRÜB bereitet dann den Übergabeumschlag mit der Karte, den PIN-Umschlägen und einer Einführungs-

534 S. http://europa.eu.int/idabc/document/2649/194.
535 http://www.e.finland.fi/netcomm/news/showarticle.asp?intNWSAID=9958.
536 Informationen sind unter http://www.id.ee und unter http://www.mig.ee erhältlich. Der Fragebogen wurde von *J. Kase* von AS Sertifitseerimiskeskus (s. im Folgenden) beantwortet.
537 S.u. 3.2.2.4.
538 V. 26.6.2003, s. http://www.id.ee/pages.php/030307,473.
539 Davon wurden ca. 156.000 Karten an Ausländer abgegeben. Der jeweils aktuelle Stand kann unter http://www.id.ee/pages.php/03030102 abgerufen werden.
540 In der Form vorname.nachname_NNNN@eesti.ee; NNNN sind Nummern für den Fall von Namensdoppeln.
541 SK wurde von zwei großen estischen Banken (Hansapank und Eesti Ühispank) sowie zwei Telekommunikationsunternehmen (Eesti Telefon und Eesti Mobiiltelefon) gegründet.

broschüre vor. Dieser wird an CMB übergeben, die ihn an SK weiterreicht (welche im Rahmen eines Outsourcing-Projekts die Übergabe betreut). SK bringt den Übergabeumschlag per Sicherheitsdienst zu der vom Bürger benannten Bank, die die Identifizierung bei der Übergabe vornimmt. Im Anschluss daran werden die Zertifikate aktiviert.

Die Produktion einer Karte kostet 280 EEK (ca. 18,- Euro). Für die erste Projektentwicklung wurden 1 Millionen EEK (ca. 64.000 Euro) aufgewendet, während die Investitionen für die elektronische Infrastruktur und Anwendungen mit bislang 40 Millionen EEK (ca. 2,56 Millionen Euro) veranschlagt werden. Das Geschäftsmodell sieht wie folgt aus: Die Karte kostet für den Inhaber 150 EEK (ca. 9,6 Euro), bei einer auf 25 EEK (ca. 1,6 Euro) reduzierten Gebühr für Kinder unter 15 Jahren und Senioren. Um den Einsatz der Signaturfunktion zu fördern, wurde die hierzu benötigte Software für jedermann kostenlos zur Verfügung gestellt. Der Staat finanzierte die Entwicklung, während die Privatwirtschaft die Infrastruktur- und Anwendungskosten übernahm. TRÜB und SK werden für die Kartenherstellung von der Regierung bezahlt, daneben wird SK Gebühren (maximal 60 EEK, ca. 3,80 Euro) für die Erneuerung der Zertifikate erheben, die nach drei Jahren erforderlich ist. Außerdem müssen Organisationen, die die Onlinedienste von SK in großem Umfang nutzen, monatliche Gebühren bezahlen.

Die Karte beinhaltet in visueller wie elektronischer Form Namen, nationale Identifikationsnummer, Geburtstag, Geschlecht, Staatsangehörigkeit, Geburtsort, Ausstellungsdatum, Kartennummer und Gültigkeitsdauer, bei Ausländern auch die Aufenthaltsberechtigung. Auf die Karte werden außerdem ein Photo und eine Unterschrift des Inhabers aufgedruckt. Die Zertifikate für die Signatur und Authentisierung enthalten von den genannten Personendaten nur den Namen und die Identifikationsnummer; das Authentisierungszertifikat enthält darüber hinaus die offizielle Email-Adresse. Die Zertifikate sind drei Jahre gültig, während der Datensatz mit den Personendaten für die gesamte Laufzeit des Ausweises von zehn Jahren verwendet wird. Der noch verfügbare Speicher der Karte wäre in der Lage, biometrische Daten aufzunehmen; es gibt bislang aber keine entsprechenden Pläne.

Die Einführung des neuen Ausweises in Estland stieß nicht auf nennenswerte Akzeptanzschwierigkeiten. Kritik wurde lediglich an mangelnder Information über das Projekt geübt. Dies hat sich jedoch im Laufe der Zeit und mit Fortschreiten des Einführungsprozesses gelegt. Das Fehlen von Akzeptanzproblemen wird zum einen darauf zurückgeführt, dass die estische Gesellschaft allgemein aufgeschlossen gegenüber neuen Technologien ist; zum anderen wurden bei der Einführung die Ergebnisse der relativ langen Diskussion in der Öffentlichkeit (sechs bis sieben Jahre) berücksichtigt. Wichtige Entscheidungen wurden vom Innenministerium in Zusammenarbeit mit einer Arbeitsgruppe getroffen, die mit Spezialisten aus dem öffentlichen und privaten Bereich (unter anderem Telekommunikationsbehörden, Banken und Multimediakonzerne) besetzt war.

3.2.1.3 Belgien

In Belgien wurde Anfang April des Jahres 2003 in elf Gemeinden ein sechsmonatiges Pilotprojekt für einen neuen Personalausweis gestartet und im Anschluss die Entscheidung gefällt, diesen innerhalb von fünf Jahren jedem der etwa 11 Millionen Bürger zur Verfügung stellen.[542] Die entsprechende Rechtsgrundlage trat am 15. September 2004 in

542 Basis war eine Machbarkeitsstudie von Computer Sciences Corporation (CSC). CSC hat auch die Ausschreibung für das Projekt erarbeitet, die unter http://www.registrenational.fgov.be/rrn_fr/cccie/CDCFABRICATIONCID__def_F100402.pdf abrufbar ist. Die Fragen zu Belgien wurden beantwortet von *D. Frauman* (CSC), *Y. De Meester* (Ubizen) und *B. Sijnave* (Federale Overheidsdienst ICT).

Kraft.[543] Nachdem zunächst aus Kostengründen auch eine Verteilung der Karten durch die belgische Post diskutiert wurde, wird die Ausgabe nun doch durch die Gemeinden erfolgen.

Seit Februar des Jahres 2005 werden monatlich 120.000 neue Ausweise ausgegeben. Mitte April desselben Jahres betrug ihre Zahl 350.000.[544] Wie bisher sind alle belgischen Bürger ab dem Alter von elf Jahren ausweispflichtig. Bei Kindern hat die Karte allerdings keine Signaturfunktion. Erwachsene können der Aktivierung der Zertifikate widersprechen, diese werden aber in jeden Fall generiert. Ein Einsatz des Ausweises ist zu Hause an einem PC mit Kartenleser,[545] aber auch an öffentlichen Kiosken oder in Behörden möglich. Zu Beginn wird der Personalausweis lediglich als Identitäts- und europäisches Reisedokument, sowie zur Signaturerstellung dienen. Es ist aber vorgesehen, die Sozialversicherungskarte zu integrieren. Entsprechend den Empfehlungen einer Machbarkeitsstudie wurden dagegen Pläne verworfen, den Ausweis auch als Führerschein einzusetzen oder auf ihm Gesundheitsdaten zu speichern.

Im Rahmen der Signaturfunktion tritt der Staat selbst als Zertifizierungsdiensteanbieter auf, arbeitet aber mit einer Vielzahl von privaten Firmen (Belgacom, Ubizen) zusammen, die die Zertifikatserstellung und weitere Dienstleistungen übernehmen.[546] Die privaten Schlüssel werden während der Personalisierungsphase oder danach durch den Chip selbst generiert. Die Produktionskosten betragen inklusive Personalisierung und Bereitstellung der beiden Zertifikate 9,- Euro. Das Pilotprojekt wird mit 10 Millionen Euro, das Gesamtprojekt mit 100 Millionen Euro veranschlagt. Geplant ist eine Gebühr von 10,- Euro für den Inhaber. Die Karte wird dieselbe Gültigkeitsdauer wie die Zertifikate haben, nämlich fünf Jahre.

Alle auf der Karte sichtbaren Persönlichkeitsdaten, inklusive der Unterschrift und des Bildes, werden auch auf dem Chip gespeichert. Es ist nicht vorgesehen, das Bild zur biometrischen Erkennung zu verwenden, eine Erweiterung um biometrische Daten ist jedoch technisch möglich. Die Wohnadresse des Trägers wird nur elektronisch abgelegt, um zu verhindern, dass bei einem Wohnortwechsel des Inhabers ein neuer Ausweis ausgestellt werden muss. Die Identitätsdaten werden nicht verschlüsselt, sind also für jedermann lesbar, der physischen Zugang zur Karte hat. Eine Änderung der Daten ist jedoch nur durch die Behörden, und nur mit Zustimmung des Inhabers (das heißt nach dessen vorheriger PIN-Eingabe) möglich.

Die Akzeptanz der entwickelten Lösung soll auf der Basis des Pilotprojekts evaluiert werden. Bislang gibt es dazu keine eindeutigen Erkenntnisse, allerdings wurden wegen eines möglichen Zugriffs privater Anbieter auf staatlichen Daten Bedenken gegen die Outsourcing-Lösung mit der Firma Ubizen laut. Daneben gibt es grundsätzliche Kritik an der Verwendung einer Multiapplikationskarte. Der Staat hofft, durch positive Ergebnisse des Pilotprojekts negative Reaktionen in der Bevölkerung vermeiden zu können.

543 S. http://europa.eu.int/ida/en/document/3301/194.

544 Vgl. http://europa.eu.int/idabc/en/document/4098/194.

545 Die Firma Microsoft plant offenbar, die Karte zur Identifikation im Rahmen des MSN Messenger einzusetzen, vgl. http://europa.eu.int/idabc/en/document/3854/194. Eine Zusammenarbeit gibt es auch mit der Firma Adobe, s. http://europa.eu.int/idabc/en/document/4098/194.

546 Für weitere Einzelheiten zum Geschäftsmodel s. http://www.rijksregister.fgov.be/slides/EN/intro/intro.htm.

3.2.1.4 Frankreich

Im Bereich der Telematik im Gesundheitswesen ist Frankreich im europäischen Vergleich weit entwickelt.[547] Bei der „Carte Vitale“[548] handelt es sich um eine allgemein eingeführte Mikroprozessorkarte im Gesundheitswesen. Sie soll nach und nach zu einem ähnlichen Modell wie dem in Deutschland geplanten ausgebaut werden, wobei aber ganz überwiegend serverbasierte Datenspeicherungen geplant sind. Vorgesehen ist die Speicherung von Notfallinformationen, europäischen Berechtigungsnachweisen und Pointern zur Ablage von Gesundheitsdaten in Serversystemen. Zu Identifikationszwecken wird es ein Datenfeld für biometrische Daten auf der Karte geben.[549]

Bis zum Jahre 2007 soll außerdem ein allgemeines System einer elektronischen Patientenakte aufgebaut werden.[550] Für Fachkräfte im Gesundheitswesen wurde ein Heilberufsausweis (Carte de Professionnnel de Santé) eingeführt, der zum Zugriff auf die Gesundheitskarte erforderlich ist.[551] Dabei erfolgt eine gegenseitige Authentisierung der beiden Karten. Bereits derzeit wird die Hälfte aller monatlich anfallenden 60 Millionen Behandlungsscheine in elektronischer Form ausgestellt und zur Abrechnung an die Versicherungsträger übermittelt.

In Frankreich wurde im Oktober des Jahres 2003 außerdem ein Vorhaben der Regierung bekannt gegeben, bis zum Jahre 2006 einen Personalausweis im Chipkartenformat („Identité Nationale Electronique Sécurisée“) einzuführen.[552] Dieser soll Möglichkeiten für elektronische Signatur und Authentisierung bieten. Für die Aufnahme biometrischer Merkmale wird eine einheitliche Lösung auf der Basis der ICAO-Kriterien favorisiert, die sowohl für den Personalausweis als auch für den Reisepass gelten soll (Gesichts- und Fingerbilder).[553] Es ist noch nicht entschieden, ob die Daten nur auf dem Ausweis, oder auch in zentralen staatlichen Datenbanken gespeichert werden.[554] Als Trägermedium wird im Moment ein Dual Interface-Chip bevorzugt in Erwägung gezogen. Am 1. Februar 2005 startete das Innenministerium ein Internet-Diskussionsforum, um den französischen Bürgern die Möglichkeit zu geben, ihre Meinung zu dem Projekt zu äußern.[555] Die Regierung plant, bis zum Juni des Jahres 2005 einen Gesetzesentwurf vorzulegen.[556] Der neue Ausweis soll – anders als das bisherige Modell – nach einer Übergangszeit verpflichtend ausgegeben werden.

3.2.2 Außereuropäische Staaten

3.2.2.1 Brunei

In Brunei werden seit August des Jahres 2000 Chipkartenausweise mit Fingerabdruckdaten verwendet.[557] Sie werden für Staatsangehörige und Personen mit ständiger Aufenthaltserlaubnis als Personalausweis ausgestellt, ausländische Arbeitnehmer erhalten eine Variante als Green Card. Die Verteilung der insgesamt etwa 350.000 Karten ist mittlerwei-

547 S. *eESC/TB11 Health* 2003, 55 ff.; *Europäische Kommission*, KOM(2003) 73, 23 ff.
548 S. http://www.sesam-vitale.fr.
549 Vgl. http://www.heise.de/newsticker/meldung/49266.
550 S. http://europa.eu.int/idabc/document/2570/194.
551 Vgl. näher http://www.gip-cps.fr/.
552 S. http://www.cardtechnology.com/cgi-bin/readstory.pl?story=20031002CTDN621.xml.
553 Vgl. http://europa.eu.int/ida/en/document/3249/194.
554 S. http://europa.eu.int/ida/en/document/3312/194.
555 S. http://europa.eu.int/idabc/en/document/3839/194.
556 Vgl. http://europa.eu.int/idabc/en/document/4100/194.
557 Allgemeine Informationen sind unter http://www.immigration.gov.bn/registration.htm verfügbar.

le abgeschlossen. Brunei war damit der erste Staat mit einer biometrischen Identifikationschipkarte. Sie wird bisher für Einwanderungszwecke und als Rentenausweis eingesetzt, weitere Anwendungen (wie Signatur- und Bezahlfunktion) sind in naher Zukunft geplant.

Die Ausgabe der Ausweise erfolgt durch die Einwohnermeldeämter. Die Karte kostet ca. 6,- Euro für Bürger von Brunei und ca. 12,- Euro für ausländische Arbeitnehmer. Die Gesamtkosten für Hardware, Software und Karten werden mit ca. 3 Millionen Euro angegeben. Anscheinend wirft das System aufgrund der Gebühren mittlerweile für den Staat sogar Profit ab.

Neben den üblichen Identifikationsdaten sind auf der Karte die Templates beider Daumenabdrücke gespeichert. Diese werden auch in einem neuen zentralen Melderegister aufbewahrt. Beim Ausweisantrag werden die abgenommen Daumendaten mit der zentralen Datenbank abgeglichen, um Doppel- und Falschanträge zu verhindern. Soweit ersichtlich, gab es bei der Einführung des neuen Ausweises keine Akzeptanzschwierigkeiten.

3.2.2.2 Oman

Oman hat im Januar des Jahres 2004 mit der Vergabe von Personalausweisen mit biometrischem Merkmal an seine 1,2 Millionen Bürger über 15 Jahren begonnen.[558] Nachdem die erste Karte an den Sultan des Landes ausgestellt wurde, erhielten bis zum 1. August 2004 100.000 Bürger den neuen Ausweis. Der Staat hat eine Komplettlösung von Gemplus International eingekauft. Die Rechtsgrundlage für das Programm bildet das königliche Dekret Nr. 66/99.

In einem ersten Schritt übernimmt der neue Ausweis nur Identifikationsfunktionen. Eine Kontrolle soll vor allem an der Grenze, aber auch durch portable Geräte möglich sein. Oman will dann eine dreistufige Implementierung einer PKI durchführen. Zunächst soll diese nur für den Datenaustausch zwischen Behörden und Verwaltungsbeamten eingesetzt werden. Gleichzeitig wird ein Programm zur Entwicklung von Electronic Government Anwendungen aufgelegt. In einem zweiten Schritt können Unternehmen und Organisationen, die mit der Regierung regelmäßig kommunizieren (etwa für Arbeitnehmerregistrierung, Arbeitserlaubnisse oder Importfragen), die PKI nutzen. In der letzten Stufe wird diese dann auch den Bürgern angeboten werden.

Der Ausweis ist verpflichtend für jeden Bürger ab 18 Jahren, ausländische Einwohner und Ausländer, die sich mehr als 14 Tage im Land aufhalten. Das entspricht der bisherigen Regelung. Der Ausweis wird damit auch Visumfunktionen übernehmen. Er ist an 16 Ausgabezentren der Royal Oman Police erhältlich. Das Verfahren läuft wie folgt ab: Im Ausgabezentrum werden die Daten erhoben und elektronisch an das zentrale Register gesendet. Dort werden die Fingerabdruck-Templates berechnet, die an die Ausgabestelle zurückgeschickt werden. Vor Ort erfolgen in einem geschützten Bereich die Personalisierung und ein Test der Funktionsfähigkeit der Karte und der gespeicherten Templates. Ist dieser nicht erfolgreich, wird eine neue Karte produziert. Der gesamte Prozess zwischen Antrag und Kartenausgabe dauert lediglich 30 Minuten.

Gemplus ist neben Software und Chipkarten auch für Beratung, Projektmanagement und Integration sowie für weitere Dienstleistungen zuständig. Dabei wird das Unternehmen ein nationales Registrierungssystem aufbauen, welches bislang nicht existiert. Die Kosten des Systems werden zunächst von der Royal Oman Police getragen.

---

558 Zur Situation in Oman gibt es wenig offizielle Informationen. Zuständig in der Regierung ist die Royal Oman Police Force (http://www.rop.gov.om). Die Fragen zu Oman beantwortete *C. Norell* (Gemplus); s.a. http://www.kablenet.com/kd.nsf/Frontpage/042AD43D56E2E36E80256C5D00376555?OpenDocument.

Die Chips enthalten Namen, Adresse, Geburtstag, Photo und zwei Fingerabdrucks-Templates in digitaler Form. Mittelfristig ist ein Einsatz als Führerschein und für die automatisierte Einreise geplant, langfristig auch die Speicherung medizinischer Notfalldaten und eine Verwendung als elektronische Geldbörse und zum Electronic Voting. Aus Datenschutzgründen ist vorgesehen, bei einer Ausdehnung auf derartige Bereiche separate technische Zugriffsrechte für die jeweils zuständigen Behörden zu vergeben.

3.2.2.3 Hongkong

In der Hong Kong Special Administrative Region (HKSAR) werden seit dem 23. Juni 2003 Ausweise mit Fingerabdrucksdaten und Signaturfunktion ausgegeben.[559] Basis für das Projekt war ein Machbarkeitsgutachten einer Beratungsfirma.[560] Im Rahmen einer groß angelegten Umtauschaktion sollen innerhalb von vier Jahren alle 6,8 Millionen Bürger über elf Jahren einen neuen Ausweis erhalten.[561] Dieser ist für jeden Einwohner der HKSAR verpflichtend.[562]

Der Personalausweis fällt in Hongkong unter die Registration of Persons Ordinance und die zugehörige Registration of Persons Regulation.[563] Ein Ergänzungsgesetz – Registration of Persons (Amendment) Bill – schuf die Grundlage für die neue Karte. Aus staatlicher Sicht ist ihr Hauptnutznießer das Immigration Department. Dessen Vollzugsbeamte sollen mit mobilen Lesegeräten für Maßnahmen gegen illegale Einwanderer ausgerüstet werden. Außerdem wird die Karte den Weg für ein automatisches Personen- und Kraftwagenabfertigungssystem an Grenzübergängen bereiten.[564] Die Verwendung dieser Systeme soll zwar nicht verpflichtend sein, wegen des damit verbundenen Zeitgewinns wird aber mit einer hohen Zahl von Nutzern gerechnet. Der Ausweis wird eine Vielzahl von weiteren Anwendungen ermöglichen, wobei diese strikt freiwillig ausgestaltet werden sollen:

- Der Personalausweis verfügt derzeit bereits über eine Signaturfunktion. Die Bürger können an 20 Poststellen der Hongkong Post ihr Zertifikat beantragen und Kartenlesegeräte erhalten. Die (staatliche) Post bietet bereits seit einigen Jahren Signaturkarten an, für die es auch schon eine Reihe von Anwendungen im Electronic Government gibt. Sie tritt als einziger Zertifizierungsdiensteanbieter auf. Das höhere Vertrauen der Bürger in einen staatlichen Anbieter überwog die Bedenken wegen der Gefahr einer unumkehrbaren Monopolbildung. Die Zulassung weiterer Anbieter wird allerdings für die Zukunft erwogen. Dabei würden die Zertifikate nachträglich auf den Chip aufgespielt werden.

---

559 Für allgemeine Informationen vgl. http://www.smartid.gov.hk/en/index.html; s. im Übrigen v.a. die Legislative Council Papers No. CB(1)666/01-02(01) und CB(2)2433/01-02(06), abrufbar unter http://www.legco.gov.hk/yr01-02/english/panels/itb/papers/itbse1220cb1-666-1e.pdf bzw. http://www.legco.gov.hk/yr01-02/english/panels/se/papers/se0710cb2-2433-6e.pdf; vgl. ferner http://www.info.gov.hk/gia/general/200112/20/1220190.htm; http://asia.cnet.com/newstech/security/0,39001150,39080241,00.htm. *S. Law*, Industry and Technology Bureau der HKSAR, war so freundlich, den Fragebogen zu beantworten.

560 Der Gang der Arbeiten ist dargestellt im Legislative Council Paper No. CB(2)2433/01-02(08), abrufbar unter http://www.legco.gov.hk/yr01-02/english/panels/se/papers/se0710cb2-2433-8e.pdf.

561 Der Umtausch erfolgt jahrgangsweise, s. http://www.smartid.gov.hk/en/replace/who.html.

562 Aufgrund der speziellen verfassungsrechtlichen Situation zwischen der Volksrepublik China und der HKSAR ist die Abgrenzung der verschiedenen Personengruppen, ihre Aufenthaltsberechtigung und Personalausweispflicht sehr kompliziert; s. näher http://www.info.gov.hk/immd/english/sitemap/index.htm.

563 Verfügbar unter http://www.justice.gov.hk/index.htm und http://www.legco.gov.hk.

564 Vgl. http://www.cardtechnology.com/cgi-bin/readstory.pl?story=20030911CTDN266.xml.

- Ebenfalls umgesetzt ist der Einsatz im öffentlichen Bibliothekenwesen. Die 2,5 Millionen Dauernutzer erhalten die Option, ihre Benutzernummer elektronisch auf dem Ausweis abzulegen und diesen zum Zugang zu gebrauchen. Die bisherigen Plastikkarten mit Barcode werden für Besucher, aber auch für Bürger weiterhin erhältlich sein, die den Ausweis hierzu nicht benutzen möchten.
- Ab dem Jahre 2006 soll der Ausweis Teil eines neuen Führerscheinsystems werden. Dabei geht Hongkong aber nicht den Weg einer Speicherung der Daten in visueller oder elektronischer Form auf dem Ausweis. Eine elektronische Variante hätte einen zu großen Investitionsbedarf für Lesegeräte bei Verkehrspolizisten, Arbeitgebern und Autoverleihern verursacht. Außerdem gab es Zweifel an der Akzeptanz in der Volksrepublik China. Eine visuelle Speicherung wurde wegen des Platzbedarfs verworfen. Außerdem wollte man aus Datenschutzgründen einen Entzug der Fahrerlaubnis nicht öffentlich machen und hätte deshalb zweimal (bei Beginn und Ende des Entzugs der Fahrerlaubnis) einen neuen Ausweis ausstellen müssen. Stattdessen plant Hongkong, die Pflicht zum Mitführen eines Führerscheins abzuschaffen und in einer zentralen Datenbank alle Führerscheininhaber mit ihren Personalausweisnummern zu speichern. Anhand der Nummer kann dann bei Kontrollen eine Abfrage der Führerscheindaten erfolgen. Es soll aber weiterhin die Option eines separaten Führerscheins für berufliche und private Zwecke geben, etwa für Auslandsreisen.
- Auf der Karte gibt es außerdem freien Speicherplatz für zukünftige Anwendungen, beispielsweise für eine elektronische Geldbörse.

Der Personalausweis wird beim Immigration Department beantragt, dort personalisiert und ausgestellt. Die Behörde ist gehalten, über die Signaturfunktion aufzuklären. Nach der Antragstellung kann zusätzlich ein Signaturzertifikat beantragt werden. Erfolgt dies, so wird das Zertifikat vor der Ausgabe auf die Karte aufgespielt und die PIN bei der Abholung des Ausweises durch Mitarbeiter der Post übergeben.

Der neue Ausweis ist für die Bürger kostenlos, lediglich bei einer Neuausstellung nach Verlust oder Beschädigung fallen Gebühren an. Darüber hinaus bietet Hongkong jedem Ausweisinhaber das Signaturzertifikat (das eine Gültigkeit von drei Jahren besitzt) für das erste Jahr umsonst an. Davon verspricht man sich, die kritische Masse von Nutzern zu erreichen, die für die Entwicklung einer neuen Generation von Signaturanwendungen notwendig ist. Erwartet wird, dass die überwiegende Zahl der Nutzer aufgrund der gewonnenen Erfahrungen und der sich abzeichnenden neuen Möglichkeiten das Zertifikat nach einem Jahr gebührenpflichtig (für 50 HKD, also ca. 5 Euro pro Jahr) weiternutzen wird. Um Bürger ohne eigenen PC oder Kartenleser nicht zu benachteiligen, wird es eine erhebliche Aufstockung der Zahl öffentlicher Computer und Selbstbedienungskioske im ganzen Land geben, von denen zurzeit etwa 100 an gut zugänglichen Knotenpunkten installiert sind. Hier können die gespeicherten Daten eingesehen und die PIN geändert werden. Der Staat rechnet mit Kosten von etwa 2,8 Milliarden HKD (ca. 280 Millionen Euro) für das gesamte Projekt. Man hofft allerdings auf eine erhebliche Förderung von Electronic Government und Electronic Commerce.

Auf dem Chip werden Name, Geburtstag, Geschlecht, Kartennummer, ein digitalisiertes Gesichtsbild und die Templates von beiden Daumenabdrücken gespeichert, bei Ausländern mit Dauerwohnsitz außerdem der Einwanderungsstatus (Student, Arbeitnehmer, etc.). Das biometrische Merkmal wurde entsprechend dem Rat der Machbarkeitsstudie gewählt. Die Ausweise werden lediglich die Templates der Daumen enthalten; allerdings wird auch eine zentrale Datei mit Volldatensätzen angelegt. Die allgemeine Abnahme von Fingerabdrü-

cken erfolgt in Hongkong bereits seit der Einführung des Personenregistersystems in den 60er Jahren des vorigen Jahrhunderts. Derzeit werden Matching-Einheiten mit Lebenderkennungssystemen an Grenzübergängen installiert. Ein Matching auf der Karte wurde in Betracht gezogen, aus technischen Gründen jedoch verworfen. Bei entsprechendem technischem Fortschritt soll diese Option jedoch erneut erwogen werden.

Datenschutzregeln zum Ausweis finden sich in der Personal Data (Privacy) Ordinance und den erwähnten Rechtsgrundlagen des Ausweises. Diese wurden für den neuen Ausweistyp ergänzt. So ist der unbefugte Umgang mit den Ausweisdaten strafbar. Außerdem findet eine strikte Trennung nach Applikationen statt, womit Zugriffe des Immigration Departments auf die Zertifikatsdaten und anderer Anwender auf die Einwanderungsdaten verhindert werden. Dazu werden Secure Access Module (SAM) Schlüssel verwendet. Auch vor einem Datentransfer zu einem Backend-System erfolgt eine gegenseitige Authentisierung zwischen der Karte und einem zertifizierten Lesegerät. Darüber hinaus werden alle Daten zwischen der Karte und Backend-Datenbanken stets verschlüsselt übertragen.

In Zusammenarbeit mit dem Datenschutzbeauftragten der Regierung wurde ein Code of Practice für den Umgang mit dem neuen Ausweis erarbeitet. Die Datenschutzsituation soll überdies regelmäßig intern, aber auch unter Einbeziehung des Beauftragten, evaluiert werden. Außerdem erfolgte eine Schulung der Mitarbeiter der Einwanderungsbehörde über die neuen Datenschutzregeln. Vor der Entscheidung über die Einführung des neuen Personalausweises wurde ein ausführlicher Konsultationsprozess durchgeführt.[565] Es gab öffentliche Ausstellungen, Veranstaltungen und Diskussionen mit Bürgern. Die Funktionsweise der Karte, insbesondere im Hinblick auf die biometrischen Merkmale, wurde der Öffentlichkeit vorgestellt. Die Reaktionen waren generell positiv, es wurden aber auch Sicherheits- und Datenschutzbedenken aus der Bevölkerung und von Datenschützern laut. Diese führten zu einer strikten Freiwilligkeit weiterer Anwendungen. Jede weitere, auch freiwillige, Anwendung des Ausweises würde außerdem eine gesetzgeberische Entscheidung erfordern. Als Ergebnis des Diskussionsprozesses wurde der Fingerabdruck der Iris unter anderem deshalb vorgezogen, weil befürchtet wurde, die Bürger könnten wegen vermuteter Gesundheitsrisiken der Iriserkennung den Ausweis ablehnen.

Da die Karte für weitere Anwendungen vorausgerüstet ist, wird die Entwicklung der Einsatzmöglichkeiten von Chipkarten intensiv beobachtet. Verantwortliche in der Volksrepublik China sehen die Karte in Hongkong als Testlauf für das gesamte Land.

3.2.2.4 Macao

Ähnlich wie Hongkong hat auch die Macao Special Administrative Region (Macao SAR) mit der Einführung von Chipkartenausweisen begonnen, die signaturfähig sind und Fingerabdrucksdaten beinhalten.[566] Die Verteilung an die 460.000 Einwohner begann am 4. Dezember 2002 und damit bereits elf Monate, nachdem Siemens Business Services den Auftrag erhalten hatte. Bis zum Frühjahr 2005 wurden ca. 200.000 Macao Special Administrative Region Electronic Identity Cards (MEID) ausgegeben. Der Umtausch des alten Ausweises soll innerhalb von vier Jahren abgeschlossen werden.

565 S. hierzu LC Paper No CB(2)2433/01-02(07), abrufbar unter http://www.legco.gov.hk/yr0102/english/panels/se/papers/se0710cb2-2433-7e.pdf.

566 Allgemeine Informationen sind unter http://www.dsi.gov.mo/documents/sar_id_index_e.html abrufbar; s.a. http://www.heise.de/newsticker/meldung/34493; http://www.golem.de/0301/23587.html. Der Fragebogen zu Macao wurde von *I. Lai*, Identification Department of the Macao SAR, beantwortet.

In Macao herrscht seit dem Jahre 1952 eine allgemeine Ausweispflicht. Laut Artikel 24 des Grundgesetzes der Macao SAR ist jeder Einwohner mit dauerhaftem Aufenthalt vom fünften Lebensjahr an verpflichtet, die Macao SAR Permanent Resident Identity Card zu besitzen. Für eine Vielzahl von Personen mit anderem Aufenthaltsstatus gibt es die Macao SAR Resident Identity Card. Beide Versionen haben dieselben Funktionen. Die Gültigkeit der Karte der Dauereinwohner richtet sich nach dem Alter. Der Ausweis ist entweder fünf Jahre (für unter 18jährige), zehn Jahre (für 18-60jährige) oder unbegrenzt (für über 60jährige) gültig.

Die Einführung der MEID ist in der Macao Resident Identity Card Bill und einer entsprechenden Rechtsverordnung mit Ausführungsbestimmungen geregelt.[567] Die Karte ist – wie in Estland[568] – verpflichtend signaturfähig, die erforderliche Infrastruktur ist aber noch nicht sehr weit entwickelt. Es gibt nur einen Zertifizierungsdiensteanbieter im System. Fest eingeplant sind für die Zukunft bereits eine Verwendung als Führerschein, Krankenversichertenkarte, Sozialversicherungsausweis und Studentenausweis. Daneben gibt es Überlegungen für einen Einsatz als elektronische Geldbörse. Art. 9 Abs. 4 des Einführungsgesetzes legt fest, dass der Inhaber das Recht hat, den Chip für andere Zwecke als zur Identifikation zu verwenden, hierzu aber nicht verpflichtet werden kann.

Das Verfahren vom Antrag bis zur Ausgabe dauert zwölf Tage. Es gibt auch einen Dreitages-Expressservice. Für den Antrag wurden ein zentrales Büro mit zehn Enrolment-Stationen und mobile Erfassungsmöglichkeiten eingerichtet. Der Ausweis wird vom Identification Department abgegeben. Die Gesamtkosten inklusive der Ausweisproduktion, der Anschaffung der Hard- und Software sowie der Projektentwicklungskosten belaufen sich auf ca. 1,5 Millionen USD (ca. 1,175 Millionen Euro). Dazu kommen Verwaltungskosten und laufende Ausgaben. Der Ausweis kostet bei der Erstbeantragung für den Bürger 80 Patacas (ca. 8,15 Euro); die Erneuerung ist etwa ein Drittel billiger. Senioren, Minderjährige, Schüler, Studenten, Sozialhilfeempfänger und Arbeitslose sind von der Zahlung befreit.[569] Das Gebührenaufkommen wird bei weitem nicht kostendeckend sein.

Die Kartenoberfläche enthält Namen, Photo, Unterschrift, Geschlecht und Geburtstag des Inhabers. Dieselben Daten, sowie Namen der Eltern, Ehestatus und Fingerabdruck werden in digitaler Form auf der Karte gespeichert. Darüber hinaus kann der Inhaber wählen, ob er eine Kontaktperson oder -organisation in den elektronischen Datensatz aufnehmen möchte. Die Fingerabdrucksdaten sind auch in einem zentralen System gespeichert, das Matching findet aber nur gegen den Referenzdatensatz auf dem Ausweis statt. Bereits der alte Ausweis enthielt Fingerabdrücke in optischer Form.[570]

Die auf der Kartenoberfläche enthaltenen Daten werden als „offen“ betrachtet und unterliegen auch auf dem Chip keinen besonderen Sicherheitsvorkehrungen, sind also immer auslesbar. Die übrigen Datensätze sind je nach Befugnis der zuständigen Stelle zugänglich. So kann ein Arzt beispielsweise im Notfall auf die (freiwilligen) Daten einer Kontaktperson zugreifen, jedoch nur nach einer Authentisierung mittels eines Security Access Moduls. Der Karteninhaber hat die Möglichkeit, den gesamten auf dem Personalausweis gespeicherten Datensatz über seine PIN oder per Fingerabdrucksidentifikation einzusehen. Hierfür wurden öffentliche Kioske in Behörden installiert.

---

567 Law No. 8/2002 und Administrative Regulation No. 23/2002 regulating the implementation of the MEID regime. Beide sind bislang nur in den offiziellen Landessprachen Chinesisch und Portugiesisch erhältlich.

568 S.o. 3.2.1.2.

569 Art. 33 und 34 Administrative Regulation No. 23/2002.

570 Dies ist auch in Portugal der Fall und wurde in der Zeit der portugiesischen Verwaltung (bis 1999) eingeführt.

Das lokale Parlament in Macao hat Gesetze zum Datenschutz und Straftatbestände für einen Missbrauch von geheim zu haltenden Daten verabschiedet. In der Macao SAR gibt es bislang keine unabhängigen Datenschutzbeauftragten. Die Überprüfung der Einhaltung der entsprechenden Gesetze ist Sache der zuständigen Ministerien, der Staatsanwaltschaft und der Antikorruptionskommission. Daneben sieht Art. 10 des Gesetzes Nr. 8/2002 die Einrichtung eines „Data Management Committee for Other Uses of the Resident ID" vor. Dieses soll Vorschläge für zukünftige Applikationen der MEID untersuchen und der Lokalverwaltung der Macao SAR Empfehlungen darüber geben, ob diese im öffentlichen Interesse sind. Dabei werden Datenschutzgesichtspunkte eine Rolle spielen.

Die Einführung der Karte war nur von wenigen Akzeptanzproblemen begleitet. Das wird vor allem auf die seit langem bestehende Ausweispflicht zurückgeführt, die bereits bisher ein Dokument mit Fingerabdrücken beinhaltete. Datenschutzbedenken wurden mit strikter Freiwilligkeit für Zusatzapplikationen, Auskunftsrechten und der Einführung von Straftatbeständen für den Datenmissbrauch ausgeräumt. Auf Widerstände wegen der Höhe der Gebühr reagierte man mit der beschriebenen sozialen Staffelung. Die Verwaltung reklamiert, seit der Einführung keine einzige negative Reaktion erhalten zu haben.

3.2.2.5 Malaysia

Malaysia hat im September des Jahres 2001 einen neuen Ausweis im Chipkartenformat eingeführt.[571] Die „MyKad" wurde bis Mitte April des Jahres 2003 an 4,1 Millionen der 23 Millionen Einwohner ausgegeben. Die Verteilung soll bis Ende des Jahres 2005 abgeschlossen werden. Die rechtliche Grundlage sind der National Registration Act 1950 und die National Registration Regulation 1990 (ergänzt 2001). Die neue Karte ist bislang für alle Bürger und Ausländer mit Dauerwohnrecht ab dem Alter von zwölf Jahren verpflichtend. Es ist daran gedacht, sie in Zukunft mit der Geburt auszustellen.

Die Karte hat zurzeit acht Anwendungen, wobei zwei unterschiedliche Chips (je einer mit kontaktorientierter und kontaktloser Schnittstelle) verwendet werden. Möglich ist eine Speicherung von Ausweis-, Führerschein-, Pass- und Visumsdaten und von Angaben zur Krankengeschichte. Darüber hinaus ist die Karte einsetzbar zur elektronischen Signatur, Bezahlung von Autobahn-, Park- und Transportgebühren, zum Abheben an Geldautomaten und als elektronische Geldbörse. Die Signaturfunktion wird sowohl im privaten Bereich als auch im Electronic Government genutzt. Die Zertifikate werden nachträglich auf der Karte gespeichert. Hierfür sind private Zertifizierungsdiensteanbieter und deren Subunternehmer zuständig. Im Sommer des Jahres 2003 gab es zwei staatlich zugelassene Anbieter und eine Reihe von Unterorganisationen. Die Zahl der Signaturzertifikate betrug im Sommer des Jahres 2004 3.000.[572]

Die Ausgabe des Personalausweises erfolgt durch das National Registration Department. Die PKI wurde in Zusammenarbeit mit privaten Anbietern und Nutzern entwickelt. Die Herstellung der Karte selbst kostet umgerechnet ca. 4,50 Euro. Da weitere Kosten auf eine Vielzahl von staatlichen und privaten Beteiligten verteilt werden, ist eine Gesamtkostenrechnung nicht verfügbar. Der Staat stellt die Karte, während die Infrastruktur durch den privaten Sektor (Banken, Mautstellen, Transportunternehmen) betrieben wird. Um die

571 Vgl. die malaysische Seite http://www.jpn.gov.my/kppk1/index.htm (leider ohne englische Informationen); *Woodward/Orlans/Higgins* 2003, 296 ff. sowie den Bericht unter http://www.plesman.com/index.asp?theaction=61&lid=1&sid=50449. Der Fragenkatalog wurde von Herrn *Ariffin*, Project Director für die Government Multipurpose Card im National Registration Department, beantwortet.

572 S. http://biz.thestar.com.my/news/story.asp?file=/2004/8/9/business/8607468&sec=business.

Verbreitung des neuen Personalausweises zu fördern, wird dieser bis zum Jahre 2005 kostenlos abgegeben.

Neben allgemeinen Persönlichkeitsdaten (Namen, Adresse, Geschlecht, Personennummer, Photo in visueller und digitaler Form) werden Templates des Fingerabdrucks gespeichert. Dieser wurde gewählt, weil er auch im bisherigen Ausweis in visueller Form enthalten war. Für die biometrischen Daten existiert eine zentrale Datenbank. Der Zugriff auf diese ist nur mit Zustimmung des Generaldirektors für das Einwohnermeldewesen möglich, die im Regelfall für Strafverfolgungsmaßnahmen und für Identifikationen durch Notare gewährt wird. Bestimmte Datenbereiche der Karte, insbesondere die Gesundheitsdaten, sind so gesichert, dass nur die jeweils Berechtigten Zugriff haben. Dies wird durch eine Berechtigungskarte nebst Secure Access Module sichergestellt. Nach einer groß angelegten Werbekampagne gab es anscheinend keine Akzeptanzprobleme. Es mangelt jedoch noch an Lesegeräten sowohl im öffentlichen wie im privaten Bereich.[573]

Es gibt Pläne, den Gebrauch der Karte auf den Zutritt zu Gebäuden und Parkplätzen, die Benutzung öffentlicher Verkehrsmittel, den Einsatz als Studentenausweis und zum ticketlosen Flugverkehr zu erweitern. Malaysia unterstützt derzeit Burma mit einem vergleichbaren Projekt. Außerdem hat Indonesien eine Absichtserklärung zum Kauf von 500.000 Karten abgegeben. Interesse besteht auch von Seiten der Philippinen, Laos und Kambodschas.

3.2.2.6 Taiwan

Taiwan ist eines der wenigen Länder, in denen bereits eine Gesundheitskarte im Einsatz ist, die in etwa dem für Deutschland geplanten Modell entspricht. Auf dem Chip sind neben den Identifikationsdaten des Karteninhabers Notfallinformationen, Organspendeausweis, Impfpass, elektronisches Rezept, Medikamentendokumentation, Anamnesedaten und Informationen zur Kostentransparenz gespeichert.[574] Mit der Karte sind die symmetrische und asymmetrische Verschlüsselung von Daten, eine elektronische Authentisierung und der sichere Transport von Gesundheitsinformationen möglich. Seit dem Juli des Jahres 2002 wurden mittlerweile 24 Millionen Gesundheitskarten und 350.000 elektronische Heilberufsausweise ausgegeben. Die Anlaufinvestitionen von 170 Millionen USD (ca. 190 Millionen Euro) amortisierten sich bereits innerhalb eines Jahres.

Auf dem Kartenkörper ist ein Bild des Inhabers aufgedruckt. Dies ersetzt die bis dahin vor der Behandlung erforderliche Identifikation mittels Personalausweis.[575] Zum Jahreswechsel 2003/2004 verlor die bisherige papierne Version, die für eine Übergangszeit weiter eingesetzt werden konnte, ihre Gültigkeit.

Die Einführung der Gesundheitskarte wird von Protesten einer Organisation von etwa 50 sozialen Gruppen begleitet.[576] Diese befürchten Gefahren für die sensiblen Daten und weisen auf Sicherheitsrisiken hin. So führte ein Softwarefehler Ende Dezember des Jahres 2003 dazu, dass die Daten von 30.000 Asthmapatienten auf der Homepage des Bureau of National Health Insurance frei zugänglich waren. Abrufbar waren die vollständigen Krankengeschichten, die nationalen Identifikationsnummern, die Namen von Verwandten und die Adressen und Telephonnummern der Betroffenen. Bemängelt wird auch ein zu geringer Schutz gegen Zugriffe durch Privatpersonen, insbesondere Arbeitgeber.

---

573 Vgl. http://www.centerdigitalgov.com/international/story.php?docid=49229.

574 S. http://www.gi-de.com/portal/page?_pageid=42,55000&_dad=portal&_schema=PORTAL; *BITKOM/VDAP/VHitG/ZVEI* 2003, 147.

575 S.a. http://www.taiwanheadlines.gov.tw/20011205/20011205s2.html.

576 Vgl. http://www.taiwanheadlines.gov.tw/20040102/20040102s1.html.

Taiwan plant außerdem, ab dem Sommer des Jahres 2005 eine neue Personalausweisgeneration einzuführen, die auch biometrische Daten des Fingers enthalten soll.[577] Gestaltung und Technologie der Karte werden sich an die der Gesundheitskarte anlehnen.

3.3 Staaten mit Pilotprojekten

Pilotprojekte für Chipkartenausweise finden sich praktisch nur in Europa, während die übrigen Staaten im Interesse einer schnellen Einführung auf größere Tests verzichten.

3.3.1 Italien

Nach einem Pilotprojekt in der Lombardei und im Veneto hat sich Italien dazu entschieden, einen Personalausweise im Chipkartenformat mit Signaturfunktion (Carta d'identità Elettronica – CIE) auszugeben.[578] Das Projekt verläuft bislang aber schleppend. Geplant ist ein größerer Feldversuch in 130 Gemeinden, der jedoch seit dem Jahre 2002 bereits mehrfach verschoben wurde. Zwischenzeitlich war der Start für den Dezember des Jahres 2003 geplant. Aufgrund von Softwareproblemen und Unklarheiten über das Ausgabeverfahren wurde dann mit einem Beginn um die Jahresmitte 2004 gerechnet.[579] Auch dieser Termin konnte jedoch nicht eingehalten werden.

In Italien gibt es keine umfassende Personalausweispflicht. De facto ist dieser jedoch allgemein verbreitet.[580] Die Rechtsgrundlagen für die neue Karte bestehen seit Anfang des Jahres 2002.[581] Geplant ist, die Ausgabe der Ausweise wie bisher durch die Kommunen abzuwickeln. Die endgültige Personalisierung (nach zentraler Vor-Personalisierung) könnte in den Gemeinden erfolgen. Als Alternative käme aber auch ein Postversand in Frage. Über die Ausgabe der Zertifikate ist noch nicht letztgültig entschieden. Vermutlich wird das Innenministerium als einziger Zertifizierungsdiensteanbieter auftreten. Das Verhältnis zu den bisher existierenden Anbietern ist unklar.

Die Aufnahme biometrischer Daten wird technisch möglich sein, aber nicht von Anfang an umgesetzt werden. Eine politische Entscheidung über die Aufnahme steht noch aus. Die sichtbaren Identifikationsdaten sollen dagegen von Beginn an auch im Chip gespeichert werden. Datenänderungen werden nur mittels einer speziellen Software möglich sein, die das Innenministerium bereitstellt. Sie sind außerdem zu protokollieren und dürfen nicht ohne Kenntnis des Inhabers durchgeführt werden. Dieser hat das Recht, jederzeit den Dateninhalt des Chips zu erfahren. Es ist angedacht, freie Speicherbereiche der Karte dem Inhaber zur Verfügung zu stellen, etwa zur freiwilligen Speicherung medizinischer Notfalldaten.

Im Gesundheitswesen wurde in der Lombardei eine umfassende Testregion für den Einsatz von Chipkarten eingerichtet. Das System heißt Carta Regionale di Servizi della Lombardia – Sistema Informativo Socia Sanitario Lombardia (CRS-SISS). In einem Feldversuch mit 320.000 Bürgern werden seit dem September des Jahres 2003 über zwei Jahre hinweg Karten an Bürger, Ärzte, Apotheker und Angestellte ausgegeben.[582] Auf der Ge-

---

577 S. http://www.taipeitimes.com/News/taiwan/archives/2005/01/28/2003221245.

578 S. http://www.anci.it/cie/ und http://www.cartaidentita.it/cie/reader/index.html (in italienischer Sprache); *Gentili* 2001. Die Fragen wurden von *R. Camilli* und *G. De Carlo*, Baker & McKenzie, beantwortet.

579 S. http://europa.eu.int/idabc/document/1708/194.

580 *Medert/Süßmuth* (1998, 97) sprechen von einer „faktischen" Ausweispflicht.

581 Gesetz Nr. 10 v. 15.2.2002.

582 Vgl. *Braun/Kollack/Mund* 2004, 234 ff.; s.a. http://www.cardtechnology.com/cgi-bin/readstory.pl?story=20041201CTMI661.xml.

sundheitskarte der Bürger werden Notfallinformationen und Verweise für Behandlungsdaten gespeichert. Die Leistungserbringer erhalten einen elektronischen Heilberufsausweis. Das Projekt ist auf sieben Jahre angelegt.

3.3.2 Tschechische Republik

In der Tschechischen Republik wurde im Jahre 1997 ein Pilotprojekt mit 30.000 Gesundheitskarten für Versicherte und 100 Heilberufsausweisen gestartet.[583] Neben Versicherungsinformationen werden auch der Aufbewahrungsort der elektronischen Patientenakte und ausgewählte medizinische Daten auf dem Chip gespeichert. Die Karte ist durch eine PIN geschützt. Geplant ist eine Ausdehnung auf das gesamte Land. Es wurde eine Zusammenarbeit mit den Betreibern der französischen Carte Vitale vereinbart.

3.3.3 Slowenien

Auch Slowenien begann im Jahre 1998 mit einem Pilotprojekt für eine Gesundheitskarte.[584] Mittlerweile ist diese an die gesamte Bevölkerung ausgegeben worden, verfügt allerdings bislang noch nicht über Funktionalitäten, die über die Identifizierung hinausgehen. Der Chip ist hierfür aber vorausgerüstet, sodass ein nachträgliches Update der Karten möglich wäre, ohne diese auszutauschen. Geplant ist die Speicherung von Allergie- und Impfdaten, eines freiwilligen Organspendeausweises und weiterer Gesundheitsinformationen. In diesem Fall wird der Zugriff nur mit einem elektronischen Heilberufsausweis und nach gegenseitiger Authentisierung mit der Gesundheitskarte möglich sein. Bereits in der ersten Phase erfolgte eine serverbasierte Vernetzung der beteiligten Leistungserbringer im Gesundheitswesen.

3.4 Staaten mit grundsätzlichen Entscheidungen für eine Einführung

3.4.1 Europäische Staaten

3.4.1.1 Großbritannien

In Großbritannien[585] gibt es bislang keinen Personalausweis. Dies war nicht immer so: In der Zeit des zweiten Weltkriegs wurde unter der Regierung *Churchill* ein allgemeiner Ausweis eingeführt, der bei sich getragen werden musste und auf Verlangen den Vollzugsbehörden vorzulegen war.[586] Damit sollte die Identifikation von Ausländern erleichtert werden. Die Personalausweispflicht bestand nach Ende des Krieges zunächst weiter, bis ein Urteil des House of Lords im Jahre 1951 zu dem Ergebnis kam, eine allgemeine Pflicht zur Vorlage gegenüber der Polizei entspreche nicht dem ursprünglichen Einführungszweck der Karte und sei damit rechtswidrig.[587] Diese Entscheidung führte, zusammen mit öffent-

583 Vgl. *eESC/TB11 Health* 2003, 53 ff.; *Europäische Kommission*, KOM(2003) 73, 33 ff.
584 S. *eESC/TB11 Health* 2003, 75 ff.; *Europäische Kommission*, KOM(2003) 73, 33 ff.
585 Zur besseren Lesbarkeit wird im Folgenden dieser Terminus anstelle der offiziellen Staatsbezeichnung „Vereinigtes Königreich Großbritannien und Nordirland“ verwendet.
586 Zu den Hintergründen s. *Agar* 2001, 101 ff.; dort auch zu noch früheren Vorläufern während des ersten Weltkriegs; s.a. *Thomas*, MLR 1995, 702, 703 ff.
587 *Willcock v Muckle*, decision of 26 June 1951 (by Acting Lord Chief Justice, Lord Goddard); s. näher *Agar* 2001, 110 f.; *Thomas*, MLR 1995, 702, 705 f. und unten 4.2.2.1.1.

lichen Protesten gegen zu häufige Kontrollen,[588] im Jahre 1952 zur Aufhebung des National Registration Act und zum Ende des Personalausweiswesens.

Im Zuge der Debatte um die Verbesserung von Sicherheitsmaßnahmen plant die britische Regierung nunmehr die (Wieder-)Einführung eines allgemeinen Personalausweises für das Jahr 2007 oder 2008.[589] Ein entsprechender Vorstoß des Premierministers *Major*[590] war im Jahre 1995 noch am Widerstand der Bevölkerung und des Kabinetts gescheitert. Das Home Office legte am 3. Juli 2002 ein Consultation Paper über „Entitlement Cards and Identity Fraud" vor.[591] Eine separate Machbarkeitsstudie untersuchte die Möglichkeit der Verwendung biometrischer Merkmale.[592] Die nachfolgende Diskussion wurde kontrovers geführt, und die Berichte über das Meinungsbild in der Bevölkerung sind widersprüchlich.[593] Das Home Affairs Committee des House of Commons unterstützte das Vorhaben der Regierung prinzipiell, forderte jedoch eine stärkere Beteiligung der Öffentlichkeit.[594] Der Information Commissioner *Thomas* äußerte große Bedenken gegenüber der bisherigen Behandlung von Datenschutzfragen, weil es keine Sicherheitsvorkehrungen gegen Zweckentfremdungen gebe.[595]

Das Consultation Paper zog drei Varianten eines Personalausweises in Erwägung, nämlich die Abgabe an die gesamte Wohnbevölkerung, an Staatsbürger und gewisse Wohnbevölkerungsgruppen oder an freiwillige Inhaber. Die Regierung plant nunmehr ein zweistufiges Vorgehen.[596] In einem ersten Schritt sollen ein landesweites Personenregister (unter Einschluss biometrischer Daten) aufgebaut und Reisepässe und Führerscheine um biometrische Daten ergänzt werden. Gleichzeitig wird ein zunächst freiwilliger Personalausweis eingeführt. Nach einer Evaluation und unter erneuter Zustimmung beider Häuser des Parlaments könnte dieser in einem zweiten Schritt verpflichtend werden.

Am 29. November 2004 brachte die Regierung einen Gesetzesentwurf für das neue Personenregister und den Personalausweis ein, der noch vor Weihnachten in erster Lesung beraten und am 10. Februar 2005 endgültig beschlossen wurde.[597] Allerdings stimmte das House of Lords dem Gesetz nicht mehr vor den Wahlen 5. Mai 2005 zu, sodass es in der nächsten Legislaturperiode neu eingebracht werden muss. Die Regierung erhofft sich neben der Terrorismusbekämpfung auch eine Verringerung von Straftaten im Zusammen-

---

588 *Sobel*, B.U. J. Sci. & Tech. L. 2002, 37, 52.

589 Die Fragen zu Großbritannien wurden von *S. Harrison* (Home Office) beantwortet. Kritische Anmerkungen zu den Plänen der Regierung finden sich unter http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-89872&als[theme]=National%20ID%20Cards und http://www.liberty-human-rights.org.uk/privacy/id-cards.shtml; s.a. *Smith*, Law Society Gazette 2004, No 24, 17; *Home Affairs Committee* 2004, 20 ff. m.w.N.; zur Vorgeschichte auch ebd., 8 ff.

590 Vgl. das damalige Grundsatzpapier, abrufbar unter http://www.totse.com/en/privacy/privacy/idconslt.html; s. dazu *Thomas*, NLJ 1995, 1254 ff.; *ders*., MLR 1995, 702 ff., insbes. 706 ff.

591 Abrufbar unter http://www.homeoffice.gov.uk/docs/entitlement_cards.pdf.

592 S. *Mansfield/Rejman-Greene* 2003.

593 Nach einer Umfrage unterstützen 80 % der Bevölkerung die Pläne, s. http://www.silicon.com/news/500022-500001/1/2672.html). Sie wurde allerdings vom Kartenhersteller SchlumbergerSema finanziert. Nach anderen Berichten war zumindest die überwiegende Zahl der Reaktionen auf das Consultation Paper ablehnend, vgl. http://www.heise.de/newsticker/meldung/37863; http://news.bbc.co.uk/2/hi/technology/3004376.stm; s.a. *Home Affairs Committee* 2004, 36 f. m.w.N.; *LSE* 2005, 56 f.

594 S. *Home Affairs Committee* 2004, 4 f.

595 http://www.vnunet.com/News/1138740. In einer parlamentarischen Anhörung kritisierte der Commissioner überdies das Fehlen datenschutzrechtlicher Auskunftsrechte und den Inhalt des geplanten nationalen Registers, s. http://europa.eu.int/idabc/document/2620/194; http://europa.eu.int/ida/en/document/3241/194.

596 Vgl. http://www.homeoffice.gov.uk/docs2/identity_cards_nextsteps_031111.pdf.

597 Der Gesetzesentwurf und die Begründung sind unter http://www.publications.parliament.uk/pa/cm200405/cmbills/008/2005008.htm abrufbar; s. zum Inhalt z.B. *LSE* 2005, 10 ff.

hang mit Identitätsmissbrauch, illegaler Einwanderung und Schwarzarbeit.[598] Eine kritische Einschätzung des Vorhabens kommt unter anderem von der London School of Economics & Political Science (LSE).[599]

Die Möglichkeit einer Signaturfunktion wird im Consultation Pater aus dem Jahre 2002 nur am Rande behandelt.[600] Dagegen beschäftigt sich dieses sehr detailliert mit den Kosten des Projekts.[601] Die Anschubfinanzierung wird auf 136 Millionen Pfund (ca. 198 Millionen Euro), die laufenden Kosten werden über einen Zeitraum von 13 Jahren je nach Kartentyp auf 1,182 bis 3,009 Milliarden Pfund (ca. 1,718 bis 4,372 Milliarden Euro) geschätzt.[602] Im Frühjahr 2005 wurden allerdings von der Regierung bereits Gesamtkosten von 5,5 Milliarden Pfund für zehn Jahre genannt.[603] Im Gutachten finden sich auch Überlegungen zu Kosteneinsparungen, die allerdings teilweise darauf beruhen, dass Großbritannien bislang noch nicht über einen Ausweis verfügt und deshalb durch die Einführung Verwaltungsabläufe kostensparender durchgeführt werden könnten. Die verbleibenden Kosten werden wohl über Gebühren aufgebracht werden. Der mittlerweile zurückgetretene Innenminister *Blunkett* plädierte für eine Gebühr von 25 bis 30 Pfund (ca. 36 bis 44 Euro) pro Karte, um finanzielle Vorbehalte in der Regierung auszuräumen.[604] Eine Einführung von Personalausweisen im Zusammenhang mit der Umstellung des Reisepasses entsprechend den neuen Normen der ICAO scheint wahrscheinlich. In diesem Fall könnte die Gebühr 122 Euro für die kombinierte Beantragung der beiden Dokumente betragen.[605]

Der Personalausweis soll Namen, Geburtstag und -ort, Adresse, Identifikationsnummer (die es bislang nicht gibt), Nationalität, Geschlecht, Photo, Unterschrift, Gültigkeitsdauer und Beschäftigungsstatus enthalten. Die Frage der Speicherung biometrischer Daten wurde bereits in dem Consultation Paper ausführlich diskutiert.[606] Aller Voraussicht nach wird der Ausweis diejenigen biometrischen Daten enthalten, die im nationalen Personenregister gespeichert werden. Das würde – entsprechend den Vorgaben der EU – die Speicherung von Gesichts- und Fingerabdrucksdaten bedeuten. Ein spezieller „National Identity Scheme Commissioner" soll über den Aufbau des Systems und die Einhaltung der gesetzlichen Bestimmungen wachen.

Des Weiteren hat die Regierung im Frühjahr 2004 zwei mit insgesamt 2 Milliarden Pfund (ca. 2,9 Milliarden Euro) dotierte Aufträge zur Modernisierung des Gesundheitswesens in Auftrag gegeben.[607] Stellen des Gesundheitswesens in Nordostengland sollen elektronisch so miteinander verbunden werden, dass Arzttermine online gebucht und Rezepte elektronisch an die Apotheken geschickt werden können. In den nächsten zehn Jahren werden für derartige Projekte ca. 15 Milliarden Euro bereitstehen. Ein flächendeckender Einsatz von Chipkarten ist bislang aber nicht geplant.

---

598 Vgl. zu den Motiven auch den Bericht "Identity Cards Bill Regulatory Impact Assessment", abrufbar unter http://www.homeoffice.gov.uk/docs3/ria_251104.pdf; s.a. *LSE* 2005, 13 f.; 32 ff.

599 Diese bezeichnet die Pläne als „neither safe nor appropriate" (*LSE* 2005, 3). Die überwiegende Mehrheit der befragten Experten kam zu dem Ergebnis, das Vorhaben sei „too complex, technically unsafe, overly prescriptive and lack a foundation of public trust and confidence" (ebd.).

600 S. etwa die kurze Erwähnung auf S. 60 und 66 des Consultation Papers (Fn. 591).

601 Vgl. die Überlegungen in Annex 5 des Consultation Papers (Fn. 591).

602 S. 141. Grundsätzliche Kritik kommt vom Institute for Applied Health and Social Policy am King's College in London. Dort geht man von wesentlich höheren Ausgaben aus, s. http://www.vnunet.com/News/1138042.

603 S. *LSE* 2005, 15.

604 Vgl. *Brown/Elliott* 2003.

605 Vgl. http://www.heise.de/newsticker/meldung/52899.

606 S. 51 ff. und 104 ff. des Consultation Papers (Fn. 591).

607 S. http://www.heise.de/newsticker/meldung/43266.

3.4.1.2 Spanien

Die spanische Regierung hat beschlossen, einen digitalen Personalausweis mit Signaturfunktion einzuführen. Erste Tests waren zunächst im Laufe des Jahres 2004 geplant, wurden mittlerweile jedoch auf die ersten Monate des Jahres 2006 verschoben.[608] An ihrem Ende sollen alle staatlichen Ausgabestellen in der Lage sein, das neue Dokument auszugeben.[609] Vorgesehen ist, als biometrische Merkmale den Fingerabdruck und das Gesichtsbild zu speichern.[610] Der momentane Zeitplan sieht die vollständige Ausgabe der neuen Karte an 29 Millionen Bürger ab dem Jahre 2007 oder 2008 vor. Die Kosten des Gesamtprojekts werden auf 148,9 Millionen Euro veranschlagt.

Im spanischen Implementierungsgesetz zur europäischen Signaturrichtlinie findet sich auch ein Abschnitt über den digitalen Personalausweis.[611] Der neue Ausweis wird danach alle Funktionen des bisherigen Papiers übernehmen und zusätzlich die Möglichkeiten der elektronischen Signatur und Authentisierung bieten. Die Zertifikate werden zweieinhalb Jahre gültig sein. Behörden sind verpflichtet, den Einsatz des neuen Ausweises zu akzeptieren. Die ausgebende Stelle hat den Bürger über die Arbeitsweise der Signaturfunktion zu informieren. Anscheinend bieten die bisherigen Normen allerdings noch keine hinreichende Basis für die Einführung des neuen Personalausweises.[612]

Ein weiteres groß angelegtes Chipkartenprojekt in Spanien ist die neue Sozialversicherungskarte,[613] die gerade in einem Pilotprojekt in der Region Andalusien ausgegeben wird und die automatisierte Verarbeitung der Daten durch die Verwaltung und den persönlichen Zugriff durch den Karteninhaber ermöglichen soll. Sie speichert Fingerabdrucksdaten zur Identifizierung, wobei darauf verzichtet wurde, diese zusätzlich außerhalb des Chips aufzubewahren.[614]

3.4.1.3 Niederlande

In den Niederlanden bestand bis Ende des Jahres 2004 keine allgemeine Ausweispflicht.[615] Dies hat sich am 1. Januar 2005 geändert. Seitdem muss jeder Bürger ab dem 15. Lebensjahr ein Identifikationsdokument besitzen und bei sich führen.[616] Akzeptiert werden Reisepass, Führerschein und ein – bislang nicht verpflichtender – Personalausweis. Dieser soll in Zukunft im Chipkartenformat ausgegeben werden und signaturfähig sein. Die Regierung plant überdies, ihn mit einem kontaktlosen Chip auszustatten und auf diesem biometrische Daten zu speichern. Beide Änderungen könnten im Jahre 2007 eintreten. Eine Reihe von Gutachten zum Einsatz von PKI und Biometrie in Ausweispapieren hat diese Entwicklung vorbereitet.[617] Eine der Studien empfiehlt die Einführung einer eindeutigen

608 S. http://europa.eu.int/ida/en/document/3651/194.
609 Vgl. http://europa.eu.int/idabc/document/1088/194.
610 http://europa.eu.int/idabc/document/1552/194; http://europa.eu.int/idabc/en/document/4216/194.
611 Titel IV, Artikel 25 und 26.
612 S. http://europa.eu.int/idabc/document/1896/194.
613 Vgl. *Ferreiro* 2004, 278 ff.
614 *Ferreiro* 2004, 289.
615 *M. van Dellen* und *S. Nouwt* vom Centre for Law, Administration & Informatization der Universität Tilburg waren so freundlich, Auskunft über das Personalausweiswesen zu geben.
616 Vgl. http://www.edri.org/edrigram/number3.1/ID. Dem Bericht zufolge wurden im ersten Monat nach der Gesetzesänderung 3.300 Bußgelder wegen Verstößen gegen die Mitführungspflicht verhängt.
617 S. etwa http://www.bprbzk.nl/downloads/020703.Brief%20TK%20biometrie.pdf; http://www.pkioverheid.nl/asp/get.asp?xdl=../views/pki/xdl/Page&VarIdt=00000001&SitIdt=00000002&ItmIdt=00000044 (in holländischer Sprache).

Identifikationsnummer, der so genannten „Burger Service Nummer“. Diese soll zum 1. Januar 2006 eingeführt werden .[618] Die Verteilung der Kosten für die künftige Ausweisgeneration ist noch unklar. Bislang beträgt die Gebühr für den freiwilligen Personalausweis 28,73 Euro.

Der neue Ausweis soll (wie der neue Reisepass) biometrische Daten des Gesichts und der Finger des Inhabers enthalten.[619] Diese werden zusammen mit den übrigen Angaben in dezentralen staatlichen Datenbanken gespeichert werden. Eine Verwendung von Templates wird aus Datenschutzgründen bevorzugt. Gleichzeitig soll sich der Reisepass an den Empfehlungen der ICAO orientieren, die sich jedoch für die Speicherung von Volldatensätzen ausgesprochen hat.[620] Es ist unklar, wie dieser Widerspruch aufgelöst werden wird. Anfang Juli des Jahres 2004 startete das niederländische Ministerium für innere Angelegenheiten und auswärtige Beziehungen einen Testlauf für die Integration biometrischer Daten in Reisepässe mit 15.000 freiwilligen Teilnehmern.[621]

3.4.2 Außereuropäische Staaten

3.4.2.1 Vereinigte Arabische Emirate

Die Vereinigten Arabischen Emirate (VAE) haben im Frühjahr 2003 mit der französischen SAGEM einen Vertrag über den Aufbau eines Einwohnermelde- und -verwaltungssystems abgeschlossen, das auch einen Personalausweis im Chipkartenformat mit biometrischen Daten enthalten wird.[622] Die Multiapplikationskarte soll an 22 Standorten ausgegeben werden und für Bürger und Einwohner der VAE verpflichtend sein. Daraus resultiert eine Gesamtzahl von 2 Millionen Ausweisen. Die ersten Karten sollten im Sommer 2004 des Jahres verfügbar sein und speichern die Fingerabdrucksdaten der Inhaber. Der Ausweis könnte in Zukunft auch im Rahmen des Electronic Government Anwendung finden. Er hat überdies Kapazitäten für weitere Applikationen; gedacht ist an den Führerschein und medizinische Notfalldaten.

3.4.2.2 Bahrain

Bahrain wollte im Laufe des Jahres 2004 einen multifunktionalen Chipkartenausweis einführen.[623] Die Karte soll als Ausweis, Führerschein, Krankenversichertenkarte, elektronische Geldbörse, sowie im Ausbildungswesen eingesetzt werden. Gespeichert werden etwa Gesundheitsinformationen wie Allergien und Angaben für den medizinischen Notfall. Geplante Electronic Government Anwendungen sind die Beantragung von Geburts- und Heiratszertifikaten, Genehmigungen im Bereich der Wirtschaft und Electronic Voting.

Als biometrisches Merkmal wird der Fingerabdruck verwendet werden. Dieser dient zum einen der Identifikation des Ausweisinhabers, zum anderen der Zugriffssicherung zu den nichtstaatlichen Speicherbereichen der Karte, auf die Behörden keinen Zugriff haben.

---

618 Vgl. http://europa.eu.int/idabc/document/2556/194.
619 http://europa.eu.int/idabc/document/1977/194.
620 S.o. 3.1.1.
621 S. http://www.heise.de/newsticker/meldung/48809; http://www.cardtechnology.com/cgi-bin/readstory.pl?story=20040906CTDN975.xml.
622 Vgl. http://www.kommune21.de/meldung.php?id=2219.
623 S. http://www.solutions.gc.ca/pki-icp/pki-in-practice/efforts/2003/05/scan-analyse14_e.asp#_Toc43877370.

3.4.2.3 Saudi-Arabien

Saudi-Arabien treibt ein Projekt zur Einführung eines Personalausweises im Chipkartenformat voran. Dieses unterliegt jedoch in weiten Teilen der Geheimhaltung. Deshalb sind so gut wie keine Informationen verfügbar.[624] Der Start wurde bereits mehrmals verschoben. Es ist beabsichtigt, den Ausweis an alle männlichen Staatsbürger abzugeben und auf ihm Gesichtsdaten für die biometrische Erkennung zu speichern mit der Option einer Erweiterung auf andere Merkmale. Zu einem späteren Zeitpunkt ist auch der Einsatz einer PKI geplant.

3.4.2.4 Thailand

Thailand hat im Jahre 2003 durch das Bureau of Registration Administration einen Chipkartenausweis getestet und sich im Anschluss daran für eine Einführung im Laufe des Jahres 2004 entschieden.[625] Probleme traten auf, weil die zuständigen Stellen sich nicht darüber verständigen konnten, ob die Kontrolle durch eine staatliche Behörde oder eine unabhängige Organisation vonstatten gehen sollte.[626] Weitere Verzögerungen entstanden offenbar durch eine mangelhafte Vorbereitung des Projekts.[627] Auch gab es Widerstand in der Bevölkerung wegen datenschutzrechtlicher Bedenken.[628] Ende September des Jahres 2004 war immer noch keine endgültige Entscheidung über den Hersteller der Karte gefallen.

Auf dem Ausweis sollen Name, Adresse, Geburtstag, Blutgruppe und andere medizinische Angaben gespeichert werden. Geplant ist daneben eine Vorausrüstung für elektronische Signatur, Führerschein, Geldkartenfunktion und andere Applikationen. Das National Electronics and Computer Technology Centre (Nectec) wird die Karten produzieren und hat die Vorbereitungen hierfür abgeschlossen.[629] Die Ausgabe soll an 61 Millionen Bürger ab dem ersten Lebensjahr erfolgen. Als biometrisches Merkmal wird die Karte Fingerabdrucksdaten enthalten. Jedes Ministerium soll unabhängig entscheiden können, welche Daten darüber hinaus gespeichert werden. Das führt zu Einwänden aus der Sicht des Datenschutzes. Die Karte soll nicht verpflichtend sein und 100 Baht (ca. 2,- Euro) kosten.

3.4.2.5 Japan

Die japanische Regierung plante im Sommer des Jahres 2002, innerhalb von zwei Jahren 15 bis 20 Millionen Ausweise mit Chip und Signaturfunktion kostenlos ausgeben und die Kosten von ca. 150 Millionen Euro staatlicherseits zu tragen.[630] Das Projekt wurde jedoch bislang nicht in Angriff genommen. Nunmehr ist für das Jahr 2005 die Einführung eines Personalausweises im Chipkartenformat mit biometrischen Daten (Gesicht oder Fingerabdruck) beabsichtigt.[631]

Grundlage für den neuen Ausweis ist das Datenbankprojekt Juki Net. Dabei handelt es sich um ein neues Identifikationssystem, das auch eine allgemeine Personennummer bein-

---

624 S. etwa http://www.cardtechnology.com/cgi-bin/readstory.pl?story=20030828CTDN054.xml.
625 Vgl. http://www.cardtechnology.com/cgi-bin/readstory.pl?story=20030814CTDN861.xml.
626 Vgl. http://www.solutions.gc.ca/pki-icp/pki-in-practice/efforts/2003/05/scan-analyse10_e.asp.
627 S. http://asia.cnet.com/newstech/personaltech/0,39001147,39154781,00.htm.
628 S. http://www.cardtechnology.com/cgi-bin/readstory.pl?story=20040826CTDN912.xml.
629 http://www.enn.ie/news.html?code=9173057.
630 S. den Bericht unter http://www.taz.de/pt/2002/08/01/a0224.nf/text. Fragen wurden von Prof. *S. Fujiwara* beantwortet.
631 Vgl. http://www.heise.de/newsticker/meldung/44266.

haltet.[632] Diese soll für 93 Behörden zur Verfügung stehen und zunächst in 26 Verwaltungsabläufen eingesetzt werden. Die Einführung (und dabei auftretende technische Fehler) wurde von Protesten begleitet. Hauptkritikpunkt ist die fehlende datenschutzrechtliche Absicherung und die Ausgestaltung der elfstelligen Personennummer, die über Namen, Alter, Geschlecht und Wohnort Aufschluss gibt.

3.4.2.6 Volksrepublik China

In der Volksrepublik China starteten im Laufe des Jahres 2004 Feldversuche für die Einführung eines Chipkartenausweises.[633] Bis Mitte April des Jahres 2005 wurden ca. 8 Millionen neue Ausweise ausgegeben.[634] Wegen der hohen Kosten, der enormen Stückzahl und der benötigten Infrastruktur kommt eine kontaktlose Karte ohne Mikroprozessor und mit lediglich vier Kilobyte Speicher zum Einsatz.[635] Ein digitalisiertes Photo wird im Chip gespeichert, aber nicht zum automatisierten Abgleich verwendet werden. Selbst in dieser Version wird mit Kosten von 50 Milliarden Yuan (ca. 4,74 Milliarden Euro) gerechnet. Mittelfristig könnte eine zweite Generation des Personalausweises auch Fingerabdrucksdaten speichern.

3.5 Diskussionsprozesse

3.5.1 Diskussionen in europäischen Staaten

3.5.1.1 Schweiz

Die schweizerische Regierung hatte sich auf der Basis einer Bedarfsanalyse aus dem Jahre 2001[636] zunächst Mitte des Jahres 2002 für die Einführung eines digitalen Ausweises mit Signaturfunktion, aber ohne biometrische Daten entschieden.[637] Geplant war eine Konzeptionsphase bis Ende des Jahres 2003, ein Pilotprojekt zu Beginn des Jahres 2005 und die allgemeine Ausgabe des Ausweises ab Mitte desselben Jahres. Mittlerweile ist das Projekt jedoch vorläufig gestoppt worden. Nachdem mit Wirkung zum 1. Januar 2005 die Rechtsgrundlagen für den Betrieb privater Zertifizierungsdiensteanbieter geschaffen wurden, will man zunächst deren Erfolg abwarten.

Lediglich dann, wenn diese Anbieter keine hinreichende Versorgung der Bevölkerung mit Signaturkarten bewirken sollten, würden die Pläne wieder aufgenommen. Für diesen Fall wäre eine Abgabe der neuen Karte an die gesamte Wohnbevölkerung und die Auslandsschweizer vorgesehen. Für Personen mit schweizerischem Bürgerrecht würde es dabei wie bislang keine Personalausweispflicht geben, wohl aber für Ausländer, die auch bislang einen Ausländerausweis mit sich führen müssen.

Der gesamte Fokus der schweizerischen Planungen lag – unter dem Gesichtspunkt der Wirtschaftsförderung – sehr stark auf der Signaturfunktion des Ausweises und der damit verbundenen denkbaren staatlichen Infrastrukturaufgabe. Die Bedarfsanalyse konzentriert

---

632 Das System startete im August 2003, s. http://www.heise.de/newsticker/meldung/39765.

633 S. http://www.heise.de/newsticker/meldung/39354; http://www.heise.de/newsticker/meldung/39932. Eine Testphase fand in Shanghai, Shenzhen und Huzhou statt, s. http://europa.eu.int/idabc/document/2365/194.

634 S.http://www.cardtechnology.com/cgi-bin/readstory.pl?story=20050425CTDN469.xml.

635 http://www.cardtechnology.com/cgi-bin/readstory.pl?story=20030911CTDN261.xml.

636 *Marzetta*/*Stöckle*/*Vaterlaus* 2001. Fragen der Machbarkeit wurden explizit ausgeklammert.

637 Für allgemeine Informationen s. *Bürge* 2003; *Marzetta*/*Stöckle*/*Vaterlaus* 2001. Die Fragen wurden von *U. P. Holenstein* vom schweizerischen Bundesamt für Justiz beantwortet.

sich auf den Electronic Commerce, hält aber staatliche Anwendungen für erforderlich, um hinreichend Anreize für die Signatur zu schaffen. Sie rät – unter dem Gesichtspunkt unterschiedlicher Gültigkeitszeiträume von elektronischem und physischem Ausweis – von einer Kombination mit einem allgemeinen Personalausweis ab.[638]

Die Studie kalkuliert die Kosten für zwei unterschiedliche Varianten. Bei 100.000 Ausweisen sollen sie sich gerechnet auf einen Zehnjahreszeitraum auf ca. 9 Millionen SFR (etwa 5,77 Millionen Euro) pro Jahr belaufen, bei 1 Million Ausweisen auf ca. 30 Millionen SFR (etwa 19,24 Millionen Euro). Der Initialaufwand für die Projektentwicklung, Ausbildung, zentrale und dezentrale Infrastruktur beträgt jeweils ca. 14 Millionen SFR (etwa 8,98 Millionen Euro). Inzwischen werden die laufenden Kosten aber wohl deutlich geringer (je nach Variante ca. 5-10 Euro pro Ausweis und Jahr) veranschlagt. Das Gutachten spricht auch erhebliche Kostendegressionseffekte an. Es gibt noch keine Entscheidung über mögliche Gebühren für die Karte, falls diese doch noch signaturfähig ausgestaltet werden sollte.

Der Ausweis würde vermutlich von den Gemeinden ausgegeben werden, wobei mit privaten Zertifizierungsdiensteanbietern zusammengearbeitet werden soll. Gleichzeitig wird überlegt, bestimmte Bereiche (wie Electronic Voting,[639] elektronische Strafregisterauszüge oder Geschäfte, die für das organisierte Verbrechen von Interesse sind) einem staatlichen Zertifikat vorzubehalten. Der Ausweis würde zunächst keine biometrischen Daten enthalten, aber so vorausgerüstet sein, dass dies bei späterem Bedarf nachgeholt werden kann. Weitere Anwendungen, beispielsweise im Gesundheitswesen, sind nicht geplant. Der Datenschutzbeauftragte der Schweiz ist zur Zusammenarbeit im Projekt eingeladen, Akzeptanzschwierigkeiten soll mit einer rechtzeitigen und adäquaten Information der Öffentlichkeit entgegengewirkt werden.

In der Schweiz bestehen auch Pläne für die Einführung einer elektronischen Gesundheitskarte.[640] Ein Feldversuch hierzu wurde am 8. November 2004 im Raum Lugano im Kanton Tessin gestartet.[641] Wie in Deutschland wird eine lebenslang gültige Versicherungsnummer eingeführt werden. Auch ansonsten ähneln sich die Pläne: auch die schweizerische Karte wird einen verpflichtenden und einen freiwilligen Speicherbereich enthalten. In der Schweiz ist außerdem der Einsatz als elektronische Geldbörse geplant. Ein wichtiger Unterschied besteht hinsichtlich der Personalisierung: anders als in Deutschland wird die Gesundheitskarte kein Photo, sondern einen biometrischen Fingerabdruck enthalten. Die Karte könnte im Jahre 2006 allgemein ausgegeben werden.

3.5.1.2 Österreich

Österreich kennt keine Personalausweispflicht. Deshalb sind weniger als 20 % der Bevölkerung im Besitz eines Personalausweises. Dieser hat eine Gültigkeitsdauer von zehn Jahren und wird seit dem 9. Januar 2002 im Scheckkartenformat ausgegeben, allerdings bislang ohne Chip.[642]

---

638 Dabei wurde wohl die Möglichkeit der Erneuerung des Zertifikats übersehen; s. dazu unten 5.2.5.

639 Dieses hat in den schweizerischen Überlegungen zum Electronic Government wegen der basisdemokratischen Elemente der schweizerischen Verfassung einen viel höheren Stellenwert als in anderen Staaten.

640 S. etwa *v. Below* 2001, 4 ff.; *Denz/v. Below*, Schweizerische Ärztezeitung 2002, 2026 ff.

641 Vgl. zum Folgenden http://www.heise.de/newsticker/meldung/56328.

642 Für allgemeine Informationen zum Personalausweis in Österreich s. http://www.help.gv.at/3/Seite.030000-10006.html. Fragen wurden von Prof. *R. Posch*, Wissenschaftlicher Gesamtleiter des Zentrums für sichere Informationstechnologie in Wien, und seinem Mitarbeiter *G. Karlinger* beantwortet.

Nach § 3 Abs. 4 Passgesetz[643] können Personalausweise mit „einem Datenträger versehen werden, auf dem der Inhaber automatisationsunterstützt ihn betreffende personenbezogene Daten für seinen persönlichen Gebrauch im Rechtsverkehr verarbeiten darf". Auf dieser Grundlage wird angedacht, den Personalausweis in das offene Konzept „Bürgerkarte" einzubinden, mit dem die elektronische Signatur in Österreich gefördert werden soll. Es versucht, gewisse Mindestkriterien für eine Vielzahl von Chipkarten des öffentlichen und privaten Bereichs zu definieren, auf denen Signaturverfahren ablaufen können.[644] Ziel ist die Interoperabilität der Karten mit allen angebotenen Anwendungen des elektronischen Geschäftsverkehrs. Die ersten Bürgerkarten sind mittlerweile erhältlich. So gibt die österreichische Computergesellschaft OCG ihre Mitgliedskarten kostenlos als Bürgerkarten aus.[645] Auch das Produkt a-sign premium des Zertifizierungsdiensteanbieters A-TRUST entspricht dem Konzept.[646] Schließlich gibt es seit dem 31. Januar 2005 die Möglichkeit, EC-Karten mit Bürgerkartenfunktion zu erhalten.[647]

Einer der größten Anwendungsbereiche der Bürgerkarte wird die Sozialversicherungskarte der österreichischen Sozialversicherungsträger sein.[648] Sie wird im ersten Schritt in ihrer Funktionalität in etwa der deutschen Krankenversichertenkarte entsprechen und den bisherigen papiernen Krankenschein ersetzen. Auf die Aufnahme eines Lichtbildes wurde aus Kostengründen verzichtet.[649] Für die Verwendung im Gesundheitswesen werden lediglich administrative Daten gespeichert werden, also keine Angaben über die Gesundheit. Geplant ist allerdings, die Karte als Authentisierungsinstrument für den Zugriff auf elektronischen Gesundheitsdaten einzusetzen.[650] Der Chip wird außerdem für elektronische Signaturverfahren eines beliebigen Zertifizierungsdiensteanbieters vorbereitet und so in das Konzept Bürgerkarte eingebunden werden. Im Oktober des Jahres 2004 wurde eine Einigung über die Finanzierung des Projekts erzielt.[651] Am 13. Dezember 2004 startete ein Test mit zunächst 2.500 Karten.[652] Er wurde am 28. Februar 2005 auf 86 Arztpraxen und 104.000 Patienten erweitert.[653] Im Erfolgsfall war flächendeckende Einführung ab Mai des Jahres 2005 geplant.[654]

Gegenüber der Sozialversicherungskarte hat der Personalausweis einen wesentlich geringeren Verbreitungsgrad in der Bevölkerung. Dennoch gibt es Konzepte für eine Zusammenarbeit zwischen Personalausweisbehörden und privaten Zertifizierungsdiensteanbietern. Der Ausweis soll weiterhin von den Behörden ausgestellt werden. Wie bei anderen Karten im Konzept „Bürgerkarte" hätte der Inhaber die Wahlfreiheit hinsichtlich der Zertifizierungsdiensteanbieter. Die Behörde könnte die einmalige Identitätsüberprüfung des Antragstellers im Rahmen der Registrierung gemäß Signaturgesetz, die privaten Anbieter die Personalisierung der Karte und den Verzeichnis- und Sperrdienst übernehmen. Der

643 Abrufbar unter http://www.bmi.gv.at/downloadarea/kunsttexte/Passgesetz.pdf.
644 S. http://www.buergerkarte.at; zu diesem Konzept gibt es auch ein Weißbuch (*Posch* 2002).
645 S. http://www.members.ocg.at/.
646 Vgl. http://www.a-trust.at; zu weiteren geplanten Karten s. http://www.buergerkarte.at/de/was_ist_die_buergerkarte/auspraegungen_der_buergerkarte.html.
647 S. http://europa.eu.int/idabc/en/document/3857/194.
648 Vgl. dazu *Otter* 2001; *eESC/TB11 Health* 2003, 51; *Posch* 2002, unter 3.1.
649 S. http://www.heise.de/newsticker/meldung/58304.
650 S. OMNICARD-newsletter März 2004/2; vgl. zum Konzept des Datenflusses und der Kritik daran durch Datenschutzbehörden und Softwareunternehmen http://www.heise.de/newsticker/meldung/57959; s.a. http://europa.eu.int/idabc/en/document/4074/194.
651 Vgl. http://europa.eu.int/idabc/en/document/3422. Die Ausgabe der Karte soll 116 Mio. Euro kosten.
652 S. http://www.aerztezeitung.de/docs/2005/04/13/066a1406.asp?cat=/politik/gesundheitssystem_and.
653 Vgl. http://www.heise.de/newsticker/meldung/57412.
654 S. http://www.heise.de/newsticker/meldung/54198.

Anbieter würde zwei getrennte Umschläge (einen mit dem Ausweis, einen mit der PIN) per Post dem Karteninhaber zustellen. Dieses Verfahren entspricht der Zusendung von Kredit- und Bankkarten.

Gegenwärtig enthält der Ausweis Namen, Geburtsdatum und -ort, Augenfarbe, Größe, Lichtbild und Unterschrift des Karteninhabers. Nach Abschluss der entsprechenden internationalen Normung ist die Speicherung biometrischer Daten geplant. Falls in Zukunft ein signaturfähiger Chip in den Ausweis integriert werden sollte, würden die Zertifikatsdaten den Spezifikationen des Konzepts „Bürgerkarte" entsprechen. Dabei kommt für jeden Bürger zur Verwendung der Karte im Electronic Government ein einmaliges Identifikationsmerkmal zum Einsatz. Diese Personenbindung der öffentlichen Schlüssel an den Ausweisinhaber wird durch das zentrale Melderegister bewerkstelligt, das eine einmalige Ordnungsnummer (so genannte ZMR-Zahl) jedes Bürgers enthält.[655] Das Verfahren wurde mit dem Datenschutzbeauftragten evaluiert. Das Identifikationsmerkmal der Personenbindung darf nur in auf das Verfahren abgestimmter abgeleiteter Form in Datenbanken der Verwaltung gespeichert werden. Dadurch ist die automatische Durchsuchung verschiedener Datenbanken nach einzelnen Personen effektiv schwieriger als das Durchsuchen nach Namen. Langfristig ist angedacht, auf das Speichern der Namen in den Verfahren zu verzichten und dadurch einen weiteren Datenschutzeffekt zu erzielen.

Die Kosten der Karte belaufen sich derzeit für den Staat auf 15,72 Euro. Dabei ergaben sich erhebliche Einsparungen durch eine teilweise mit der Sozialversicherungskarte einheitliche Konzeption. Dem Bürger wird allerdings eine erheblich höhere Gebühr in Rechnung gestellt. Diese beträgt, obwohl die Karte noch keinen Chip enthält, 56,- Euro.

3.5.1.3 Schweden

In Schweden gibt es keinen amtlichen Personalausweis.[656] Stattdessen werden Karten von Banken, der Post und der staatlichen Verkehrsverwaltung (Führerschein) landesweit als Identifikationsdokumente akzeptiert. Einige dieser Karten – Schätzungen belaufen sich auf 100.000 bis 200.000 – sind signaturfähig, die Zertifikate benutzen die staatliche Personenkennziffer als einheitliches Ordnungskriterium.

Ausgelöst durch die bevorstehende EU-weite Einführung von Reisepässen mit biometrischen Daten bestehen auch Planungen, einen staatlichen Personalausweis mit denselben Daten auszugeben.[657] Es gibt noch keine Entscheidung darüber, ob der Ausweis signaturfähig sein wird.

3.5.1.4 Russland

In Russland gibt es Pläne für die Einführung eines neuen Ausweises ab dem Jahr 2006.[658] Dieser soll im Chipkartenformat ausgegeben werden und zunächst vermutlich keine biometrischen Daten enthalten. Über eine Signaturfunktion ist noch nicht entschieden, geplant sind aber die Aufnahme von Gesundheits- und Sozialversicherungsinformationen sowie ein Einsatz im Steuerbereich. Ein Testlauf soll in der Enklave Kaliningrad stattfinden. In der Region Moskau gibt es überdies Pläne zum Aufbau einer Multifunktionskarte, die im Sozialversicherungs-, Gesundheits- und Transportwesen eingesetzt wer-

655 Vgl. http://www.cio.gv.at/it-infrastructure/sz-bpk/.
656 Fragen zu diesem Bereich wurden von *M.-L. Farnes* (Trust2You) beantwortet.
657 S. http://europa.eu.int/ida/en/document/3247/194.
658 Vgl. http://main.izv.info/community/14-07-03/news53344 (in russischer Sprache).

den könnte. Man rechnet in Russland für das gesamte Land mit Einführungskosten von mehreren Milliarden Euro.

3.5.2 Diskussionen in außereuropäischen Staaten

3.5.2.1 USA

In den USA gibt es – wie in Großbritannien – kein allgemeines Identifikationsdokument. Die amerikanische Gesellschaft steht der Idee eines Personalausweises seit jeher skeptisch gegenüber. Bereits im Jahre 1971 wurde ein Plan verworfen, die Sozialversicherungsnummer zu einer Art Personalausweissystem auszubauen.[659] Die Regierungen der Präsidenten *Carter* und *Reagan* ließen keinen Zweifel daran, dass sie ein solches Projekt ablehnten. Präsident *Clinton* verhinderte die Erweiterung der Einsatzfelder der Sozialversicherungsnummer, als dies im Rahmen seiner Gesundheitsreform diskutiert wurde.

Nach den Anschlägen des 11. September 2001 hat die Diskussion um ein nationales Identifikationspapier zwar neue Impulse erhalten. Die technischen und politischen Fragen der Einführung eines Personalausweises werden diskutiert.[660] Die öffentliche Meinung, die Umfragen zufolge eine Woche nach den Terrorattacken zu 70 % einen Ausweis unterstützte, lehnt diesen jedoch nunmehr mit großer Mehrheit wieder ab.[661] Die Zahl der kritischen Veröffentlichungen in Wissenschaft, Presse und Internet ist unübersehbar.[662] Befürchtet werden eine allgemeine Verhaltenskontrolle, die Vernetzung bisher verteilter Datenbanken, die Verschlechterung der Lebens- und Arbeitsbedingungen von Ausländern und Diskriminierungen gegenüber fremdländisch erscheinenden Bürgern durch stärkere und intensiver Kontrollen.[663] Die ablehnende Haltung der Mehrheit der Bevölkerung dürfte der Grund dafür sein, dass es im Kongress keine Pläne für die Einführung eines Personalausweises gibt und die Regierung im Weißen Haus verlauten lässt, sie ziehe einen solchen noch nicht einmal in Erwägung. Eine kurz- und mittelfristige Änderung dieser Politik ist sehr unwahrscheinlich. Möglicherweise wird es aber in Teilbereichen andere Entwicklungen geben. In diese Richtung weisen etwa Pläne, für „trusted travellers“ ein staatliches Papier einzuführen, das den Inhabern eine schnellere Abfertigung an Flughäfen ermöglichen würde.[664]

Trotz der ablehnenden Haltung der amerikanischen Gesellschaft gegenüber Identifikationspapieren verfügt diese über Äquivalente zu einem Personalausweis. Eingesetzt werden die Sozialversicherungsnummer, der Führerschein und Betriebs- und Dienstausweise.[665] Insbesondere die Sozialversicherungsnummer hat sich mittlerweile zu einer Art Ausweis entwickelt, obwohl dies nach der Rechtslage explizit unzulässig ist.

Für den Führerschein, der bislang in unterschiedlichen Varianten von den Bundesstaaten ausgegeben wird, gibt es Pläne für einen einheitlichen nationalen Standard, der auch

---

659 S. zum Folgenden http://www.epic.org/privacy/id_cards/.

660 Vgl. etwa *Kent/Millet* 2002; *Woodward/Orlans/Higgins* 2003, 353 ff.; s.a. *Eaton* 2003, insbes. 23 ff., 139 ff.

661 S. http://www.wired.com/news/print/0,1294,51000,00.html.

662 Vgl. bspw. *Sobel*, B.U. J. Sci. & Tech. L. 2002, 37 ff.; *ders*., Harv. J. Law & Tec 2002, 319 ff., jeweils m.w.N.; s.a. die Übersichten des Electronic Privacy Information Centre (http://www.epic.org/privacy/d_ards/) und von Privacy International (http://www.privacyinternational.org/issues/idcard/).

663 *Kent/Millet* 2002, 7, 16 f.

664 S. näher http://www.davidmbrown.com/columns/060202.html.

665 Zum Problem der oftmals zirkulären Vertrauensbasis bei der Ausstellung der verschiedenen Identifikationspapiere (ein Dokument wird bei Vorlage eines anderen ausgestellt) vgl. *Kent/Millet* 2003, 155 ff.; s.a. *Eaton* 2003, 1 ff.

biometrische Daten enthalten könnte. Im Mai des Jahres 2002 wurde ein entsprechender Gesetzesentwurf in den Kongress eingebracht und dort im Februar des Jahres 2005 verabschiedet.[666] Gleichzeitig gibt es Initiativen auf einzelstaatlicher Ebene. Mindestens sechs Staaten (Texas, Kansas, Kalifornien, Hawaii, Oklahoma und Georgia) verwenden bereits Fingerabdrücke zur Ausstellung der Führerscheine oder stehen unmittelbar davor, solche Systeme einzuführen. In Kalifornien sollen die bislang dezentral gespeicherten Fingerabdrucksdaten digitalisiert und zentral gespeichert werden, um die Vergabe von Mehrfachidentitäten zu verhindern.[667] Dagegen hat sich die Organisation der Führerschein ausgebenden Stellen in Gesamtnordamerika (AAMVA) gegen eine Einführung biometrischer Daten zum jetzigen Zeitpunkt ausgesprochen, weil technische Details noch unklar seien.[668]

Auf der betrieblichen und behördlichen Ebene werden zurzeit Betriebs- und Dienstausweise in sehr großen Stückzahlen geplant oder bereits ausgegeben. Zumindest die staatlichen Ausweise könnten mittelfristig ebenfalls Bausteine in einem System von Personalausweissurrogaten werden. Das größte derartige Projekt ist die Common Access Card des US-Verteidigungsministeriums.[669] Diese wurde mittlerweile an insgesamt über vier Millionen Armee- und Zivilbedienstete, deren Familienangehörige und Reservisten ausgeben.[670] Ihre zweite Version, mit deren Einführung bald gerechnet wird, soll Fingerabdrucksdaten enthalten. Entsprechende Programme werden in einer Vielzahl von Behörden und Privatfirmen geplant.[671] Sollte diese kaum überschaubare Masse von Projekten[672] ganz oder überwiegend Realität werden, könnte eine Situation entstehen, in der nahezu jeder US-Bürger aufgrund von Arbeitsstelle, Behördenkontakten, Freizeitverhalten oder Reisen ein offizielles oder halboffizielles Identitätsdokument besitzt, rein formal jedoch keine Ausweispflicht besteht. Die Koordination und Sicherstellung der Interoperabilität dieser Systeme dürfte einen enormen Aufwand verursachen.

Im Unterschied zu der emotionalen Debatte um einen Personalausweis werden diese Vorhaben in der Bevölkerung weitgehend akzeptiert. Das gilt auch dann, wenn biometrische Daten verwendet werden. In vielen Betrieben ist es schon seit langem üblich, die Abdrücke aller zehn Finger in die Personalakte aufzunehmen.[673] Die so genannten „civil files" der Criminal Justice Information Services Division beinhalten die Fingerabdrucksdaten von über 40 Millionen aktuellen oder ehemaligen Staatsbediensteten.[674] Auch in rechtlicher Hinsicht bestehen keine so hohen Anforderungen an die Erhebung biometrischer Daten wie in Deutschland: Seit einer Entscheidung des Supreme Courts aus dem Jahre 1973 ist es grundsätzlich zulässig, geheime Aufnahmen des Gesichts und der Stimme anzufertigen.[675]

Neben diesen Entwicklungen im Bereich allgemeiner Identifikationsdokumente gibt es in den USA weitreichende Vorhaben zum Aufbau einer Telematik-Infrastruktur im Gesundheitswesen. Der Bericht einer Expertengruppe (eHealth Initiative) vom Frühjahr des

---

666 S. *LSE* 2005, 29 f.; mittlerweile hat auch der Senat der Vorlage zugestimmt, s. http://www.heise.de/newsticker/meldung/59455; vgl. aus technischer Sicht *Woodward/Orlans/Higgins* 2003, 171.

667 Vgl. http://www.heise.de/newsticker/meldung/39630.

668 S. http://www.cardtechnology.com/cgi-bin/readstory.pl?story=20030922CTDN420.xml.

669 http://www.computeruser.com/news/02/05/07/news2.html; zu früheren Bsp. s.a. *Albrecht* 2001, 78 f.

670 Vgl. http://www.gcn.com/23_3/dodcomputing/24840-1.html.

671 Etwa im Homeland Security Department, s. http://www.fcw.com/fcw/articles/2003/0707/news-smart1-07-07-03.asp. Die Regierung plant eine Koordination der Projekte, s. http://www.theregister.co.uk/2003/07/22/one_us_gov_smartcard_id/.

672 S. etwa http://www.cardtechnology.com/cgi-bin/readstory.pl?story=20040401CTMC126.xml.

673 *Albrecht* 2001, 75.

674 S. näher *Woodward/Orlans/Higgins* 2003, 315 ff.

675 *US v. Dionisio* 410 US 1 (1973).

Jahres 2004 kommt zu dem Ergebnis, dass mit Hilfe der Einführung eines elektronischen Rezepts im US-Gesundheitswesen jährlich 29 Milliarden USD eingespart werden könnten.[676] Chipkarten für Patienten oder Leistungserbringer finden jedoch keine Erwähnung.

3.5.2.2 Kanada

Auch in Kanada gibt es kein allgemeines Identifikationsdokument. Im Alltag werden ähnliche Äquivalente wie in den USA verwendet. Seit dem Februar des Jahres 2003 läuft eine parlamentarische Debatte über die Einführung eines Personalausweises.[677] Im Oktober desselben Jahres legte das Standing Committee on Citizenship and Immigration unter dem Vorsitz des Abgeordneten *Fontana* einen Bericht vor,[678] der als biometrisches Merkmal Fingerabdrucks-, Iris- oder Handflächendaten in Erwägung zieht. Die Diskussion wird teilweise heftig geführt. Der kanadische Bundesdatenschutzbeauftragte wollte sie bereits im Keim ersticken. Die Befürworter führen die Terrorismusgefahr und eine zunehmende Zahl von „Identitätsdiebstählen" – im Jahre 2001 12.000 Fälle mit einem Schaden von ca. 2,5 Milliarden CAD (ca. 1,57 Milliarden Euro) – an.[679] Ein weiteres Argument ist die Verwendungsmöglichkeit im Grenzverkehr mit den USA. Hierzu ist bislang lediglich die Vorlage eines Führerscheins erforderlich. In den USA gibt es aber Überlegungen, von Personen mit bestimmtem kulturellem Hintergrund bei der Einreise unabhängig von ihrer Nationalität biometrische Daten zu erheben. Das könnte auch kanadische Bürger betreffen, die beispielsweise in arabischen Ländern geboren wurden. Um eine derartige Diskriminierung an der Grenze zu den USA zu verhindern, möchte Kanada biometrische Merkmale in ein eigenes Legitimationspapier aufnehmen. Allerdings gab es im Frühjahr 2004 des Jahres Meldungen, die kanadische Regierung habe die entsprechenden Pläne wieder aufgegeben.[680]

Ähnlich wie in den USA bestehen auch Pläne für einen Führerschein mit biometrischen Daten. Ferner laufen Pilotprojekte für ein „trusted travellers" Programm mit biometrischer Erkennung (CANPASS-Air und NEXUS-Air). Teilnehmer zahlen 50,- CAD (ca. 31,40 Euro) jährlich, können die normalen Kontrollen umgehen und sich stattdessen an einem Selbstbedienungskiosk identifizieren.[681] Vorbestrafte Personen dürfen nicht partizipieren. Beabsichtigt ist eine jährliche Sicherheitsüberprüfung.

Weitere Pläne zur Einführung allgemeiner Chipkartenausweise gibt es in den einzelnen Provinzen. Ontario verfolgte bereits im Jahre 1999 die Idee, eine Multifunktionskarte auszugeben. Auf ihr sollten der Führerschein, das Geburtszeugnis und Gesundheitsinformationen gespeichert werden.[682] Das Projekt wurde zu Beginn des Jahres 2002 wegen öffentlichen Widerstands und der erwarteten zu hohen laufenden Kosten für die PKI gestoppt. Derzeit gibt es in Quebec Überlegungen zur Einführung einer Gesundheitskarte, die mit biometrischen Identifikationsmerkmalen ausgestattet werden könnte. Alberta plant eine Verbindung von Führerschein und Gesundheitsdaten auf einer Karte. Hier wird außerdem bereits ein Gesichtserkennungssystem bei der Beantragung des Führerscheins eingesetzt.[683]

---

676 Abrufbar unter http://www.ehealthinitiative.org/initiatives/erx/document.aspx?Category=249&Document=270; s.a. http://www.heise.de/newsticker/meldung/46541.

677 S. die Stellungnahmen des kanadischen Einwanderungsministers unter http://www.cic.gc.ca/english/press/speech/id-card.html; http://www.cic.gc.ca/english/press/speech/id-card-2.html.

678 *Canadian Standing Committee on Citizenship and Immigration* 2003.

679 Zu vergleichbaren Problemen in den USA vgl. *Albrecht* 2001, 71.

680 Vgl. http://www.canoe.ca/NewsStand/CalgarySun/News/2004/04/09/414457.html.

681 S. http://www.itbusiness.ca/index.asp?theaction=61&sid=53445.

682 S. http://www.itbusiness.ca/index.asp?theaction=61&sid=47573.

683 S. OMNICARD-Newsletter August 2003.

3.5.2.3 Indien

Indien erwägt die Einführung eines Personalausweises in Kombination mit einem allgemeinen Personenregister.[684] Da beides derzeit nicht existiert, ist das Projekt eine große Herausforderung für das Land, in dem ca. 600 Millionen Menschen in 600.000 Städten und Dörfern wohnen. Im Laufe des Jahres 2005 soll ein Pilotprojekt mit 3 Millionen Bürgern stattfinden.

Geplant ist eine Chipkarte, die Fingerabdrücke und Photos der Inhaber sowie eine nationale Identifikationsnummer speichern wird, die es bislang nicht gibt. Die Regierung verspricht sich eine Zusammenführung der bislang verwendeten Karten (beispielsweise zur Wählerregistrierung und im Gesundheitswesen) sowie eine effektivere Grenzkontrolle.

3.5.2.4 Exkurs: Australien

Australien verfügt nicht über einen Personalausweis. Pläne zu seiner Einführung wurden im Jahre 1987 aufgrund öffentlicher Proteste gestoppt. Dagegen ist das nationale Programm zur Einführung von Biometrie in Reisepässen weltweit führend.[685] Ein Pilotprojekt zur Gesichtserkennung (SmartGate) startete im November des Jahres 2002 mit bislang 4.000 Bediensteten der Fluggesellschaft Quantas.[686] Das Matching dauert ungefähr 10 Sekunden. Als Gründe für die Wahl der Gesichtserkennung werden Nutzerfreundlichkeit, die Verbindung mit bisherigen Photodatenbanken und die Empfehlungen der ICAO genannt.

3.6 Staaten mit biometrischen Lösungen ohne Chip; Staaten in der ersten Phase der Überlegungen

Neben den bisher beschriebenen eingeführten oder geplanten Projekten gibt es weitere Personalausweise mit einfachen Speicherchips beispielsweise in Namibia und Botswana. Gleiches gilt für die von den Vereinten Nationen im Kosovo ausgegebenen Identitätspapiere. Mehrere vor allem außereuropäische Staaten besitzen Lösungen mit 2D-Barcodes, auf denen Fingerabdrucksdaten gespeichert sind. In Europa hat Bosnien-Herzegowina seit dem Jahre 2002 2,5 Millionen solcher Karten ausgegeben.[687] Der brasilianische Bundesstaat Rio de Janeiro betreibt seit dem November des Jahres 2000 eine entsprechende Lösung für seine Staatsangehörigen und speichert beide Daumen in abgerollter Form. Das System arbeitet mit einer zentralen Datenbank, die eine Reihe von Betrugsversuchen aufdecken konnte. Nach offiziellen Angaben gab es keine Akzeptanzprobleme, was wohl daran lag, dass auch der vorherige Ausweis (in visueller Form) den Daumenabdruck enthielt. Weitere Beispiele sind Argentinien, die Elfenbeinküste, Botswana, Guatemala, Honduras, Jemen, Kambodscha, Kolumbien, Libanon und Nigeria.[688]

Ansätze und Diskussionen um Identitätskarten mit PKI oder Biometrie gibt es daneben in einer Vielzahl weiterer Länder. In Portugal möchte man den aktuellen Ausweis, der ein

684 Vgl. http://www.cardtechnology.com/cgi-bin/readstory.pl?story=20040903CTDN965.xml.

685 *J. Churchill* (Australian Customs Service) und *J. Osborne* (Department of Foreign Affairs and Trade) waren so freundlich, einige Fragen zu beantworten.

686 S. etwa http://www.zdnet.com.au/newstech/security/story/0,2000024985,20268126,00.htm; http://asia.cnet.com/newstech/security/0,39001150,39082933,00.htm; http://www.cardtechnology.com/cgi-bin/readstory.pl?story=20030911CTDN265.xml.

687 S. http://europa.eu.int/idabc/en/document/1854/194; *TAB* 2004, 25.

688 S.a. *TAB* 2004, 25 ff.; *LSE* 2005, 27 ff.

Fingerabdrucksbild auf der Oberfläche enthält, durch eine Chipkarte ersetzen.[689] Vietnam plant eine kontaktlose Chipkarte als Ausweis für seine 67 Millionen Einwohner.[690] Auf dem vier Kilobytes großen Chip sollen der Fingerabdruck sowie Standardangaben wie Name, Adresse und Geburtsdatum gespeichert werden. Weitere Beispiele sind Lettland, Bulgarien,[691] Israel, die Philippinen, Südafrika und Libyen.[692] Hier sind aber noch keine Entscheidungen über Systeme, Kartentypen, Anbieter und konkrete Ausgestaltung gefallen.

Auf eine Aufstellung der Staaten, die Fingerabdrücke in visueller Form auf Identitätskarten eingeführt haben, wird an dieser Stelle verzichtet.

3.7 Tabellarische Zusammenfassung der wichtigsten Projekte

Die Übersicht hat gezeigt, dass es im Personalausweisbereich bereits eine Vielzahl von internationalen Projekten gibt, von deren Erfahrungen ein deutscher digitaler Personalausweis profitieren könnte. Die nachfolgende Tabelle fasst die wichtigsten Projekte in diesem Bereich zusammen.[693] Dies ist für die Gesundheitskarte angesichts der nur geringen Zahl der – überdies noch nicht weit fortgeschrittenen – Vorhaben nicht möglich.

Bei den ausgegebenen Karten handelt es sich durchgängig im Polykarbonatkarten im Scheckkartenformat. Die Angaben in der Spalte „Kosten" sind mit Vorsicht zu betrachten, da die Gesamtkosten sehr unterschiedlich verteilt werden und bisweilen nicht alle Kostenpunkte (Entwicklungs-, Anschaffungs- und laufende Kosten) in die Angaben der Staaten einfließen.[694] In der folgenden Spalte wurde die Kaufkraft der Bürger des jeweiligen Staates ins Verhältnis zur deutschen Kaufkraft gesetzt. Das Ergebnis gibt an, wie hoch die Gebühr oder der Preis im Verhältnis für einen deutschen Bürger wäre. Die Angabe erfolgt nur, soweit sich erhebliche Abweichungen ergeben. Bei den Darlegungen zur Biometrie ist darauf hinzuweisen, dass sich auch die Staaten, die bislang keine biometrischen Daten in den Ausweis aufgenommen haben, sich regelmäßig für eine Vorausrüstung in dieser Richtung entschieden haben.

689 S. http://europa.eu.int/idabc/en/document/3769/194; http://europa.eu.int/idabc/en/document/4298/194.

690 Vgl. OMNICARD-Newsletter Juli 2003.

691 Dort soll bis 2007 ein Ausweis eingeführt werden, der in Bezug auf biometrische Daten dem künftigen europäischen Reisepass entspricht, s. http://europa.eu.int/ida/en/document/3496/194.

692 Südafrika plant einen Chipkartenausweis, auf dem Photo, Fingerabdrücke, Identifikationsnummer und Adresse digital gespeichert werden sollen. Der Start der Ausgabe ist für Ende 2005 geplant, s. http://www.cardtechnology.com/cgi-bin/readstory.pl?story=20040823CTDN878.xml. Zum Projekt in Libyen vgl. http://www.cardtechnology.com/cgi-bin/readstory.pl?story=20050613CTDN983.xml.

693 S. zum Stand Januar 2004 bereits *Hornung*, in: Reichl/Roßnagel/Müller 2005, 29 ff.

694 Soweit Kosten in Euro umgerechnet wurden, wurde der Wechselkurs vom 10.2.2005 zugrunde gelegt.

Land	Abgabe an wen	Stand / ausgegebene Karten	Funktion der PKI; Modell für ZDAs	Kosten für Staat und Bürger	Nach deutscher Kaufkraft	Weitere Anwendungen	Biometrie
Finnland	Auf freiwilliger Basis an Bürger und Ausländer ab 6 Monaten Aufenthalt	53.000 im November 2004	PKI für Signatur und Authentisierung; Freiwilligkeit der PKI-Funktion; staatlicher ZDA	Bürger: 29,- € für drei Jahre + 70,- € für Leser und Software; 2 Mio. € für den Aufbau der PKI; laufende Kosten z.Z. ca. 4 Mio. € pro Jahr	Vergleichbar	Optional Sozialversicherungsdaten	Geplant
Estland	Verpflichtend an Bürger und Ausländer mit Aufenthaltsrecht von mindestens einem Jahr	760.000 Mitte Mai 2005	PKI für Signatur und Authentisierung; PKI verpflichtend für jedermann, kein opt-out; privater Monopolist als einziger ZDA	Bürger: 9,60 €, soziale Ermäßigung auf 1,60 €. Kosten für Zertifikatsabfragen; Infrastruktur bislang ca. 2,56 Mio. €, geteilt zwischen Staat und Wirtschaft	40,00 €; ermäßigt: 6,50 €	Online-Zugang zu Patientendaten, freier Speicher verfügbar	Nein
Belgien	Verpflichtend an Bürger	350.000 im April 2005; Kartenausgabe 120.000 pro Monat	PKI für Signatur und Authentisierung; PKI für jedermann mit opt-out; Staat tritt als ZDA auf, aber Outsourcing	Gebühr von 10,- € für fünf Jahre; Produktionskosten für Karte und Zertifikate 9,- €	Vergleichbar	Geplant als Sozialversicherungskarte, explizit nicht als Führerschein	Gesicht, aber kein automatisierter Abgleich
Brunei	Verpflichtend für Bürger und Ausländer mit Dauerwohnrecht; Greencard für Gastarbeiter	350.000; vollständige Ausgabe an gesamte Bevölkerung	Karte ist für elektronische Signatur ausgerüstet, bislang aber kein Einsatz; staatliche Organisation	6,- € für eigene Bürger; 12,- € für Gastarbeiter; Gesamtkosten des Staates für Hardware, Software und Karten ca. 3 Mio. €	k. A.	Rentenausweis und für Immigrationszwecke; Geldkarte	Templates von beiden Daumen

Oman	Verpflichtend für Bürger und Ausländer mit über 14-tägigem Aufenthalt	Start der Ausgabe im Januar 2004; 100.000 Karten bis August 2004	3-stufiges PKI-Aufbauprogramm: verwaltungsintern – Großkunden – Private; Karte ist signaturfähig; privater Monopolist	k. A. zu Gebühr und Gesamtkosten		Mittelfristig als Führerschein; langfristig medizinische Notfalldaten, Geldkarte, E-Voting	Templates von beiden Daumen
Hongkong	Verpflichtend für jeden Bewohner (auch Ausländer) ab 180 Tage Aufenthalt	Start der Ausgabe im Juni 2003, Austausch nach Geburtsjahrgängen	PKI für Signatur und Authentisierung; PKI freiwillig; staatlicher Monopolist	Zertifikate sind für jeden Bürger im ersten Jahr kostenlos, danach 5,- € / Jahr; Gesamtkosten des Staates ca. 280 Mio. €	Zertifikat 9,20 €	Bibliothekskarte; ab 2006 Einbindung in online-Führerscheinsystem und an automatischen Übergängen in die Volksrepublik; Geldkarte angedacht	Templates von beiden Daumen
Macao	Verpflichtend für Bürger und Großzahl von Bewohnern	200.000 im Frühjahr 2005	PKI für Signatur und Authentisierung; PKI verpflichtend für jedermann; privater Monopolist	8,15 € für Bürger, soziale Gebührenermäßigung; Anlaufkosten 1,2 Mio. €, k. A. über Verwaltungsaufwand und laufende Kosten	k. A.	Geplant: Führerschein, Kranken- und Sozialversicherungsausweis, Studentenausweis; Geldkarte angedacht; freier Speicherplatz für Bürger	Templates des Fingerabdrucks

Malaysia	Verpflichtend für Bürger und Ausländer mit Daueraufenthaltsrecht	4,1 Mio. im April 2003	PKI für Signatur und Authentisierung; Wettbewerb zwischen privaten Anbietern; nachträgliches Auf-spielen der Zertifikate bei diesen	Abgabe bis 2005 umsonst; Produktionskosten der Karte 4,50 €; k. A. zu Gesamtkosten, da Verteilung auf Vielzahl von staatlichen und privaten Stellen	Produktionskosten 7,40 €	Führerschein; Gesundheitskarte; Bezahlung von Autobahn-, Park- und Transportgebühren, Geldkarte	Template eines Daumens
Italien	Verpflichtend an Bürger	Pilotprojekt mit 130 Gemeinden mehrfach verschoben	PKI für Signatur und Authentisierung; vermutlich Ausgabe der Zertifikate durch das Innenministerium; private PKI vorhanden	k. A.		Freier Speicher, z.B. für Notfalldaten oder private Anwendungen	Entscheidung steht noch aus
Spanien	Verpflichtend an Bürger	Test im Laufe des Jahres 2006 geplant	PKI für Signatur und Authentisierung; noch keine Entscheidung über ZDA	Gesamtkosten auf 143 Mio. € geschätzt	Vergleichbar	Noch keine Entscheidung	Daten von Gesicht und Fingerabdruck
Großbritannien	Zunächst freiwillig an Bürger, evt. verpflichtend nach weiterer Parlamentsentscheidung	Vom Unterhaus beschlossen, Einführung 2007 oder 2008 geplant	Nur wenige Überlegungen zu PKI	36 - 44 € Gebühr (oder 122 zusammen mit Pass); Studie von 2002: 1,7 - 4,3 Mrd. € über 13 Jahre für Staat	Vergleichbar		
Niederlande	Ausweispflicht seit 1.1.2005	Einführung für 2007 geplant	Entscheidung über PKI noch offen; vermutlich für Signatur und Authentisierung	k. A.	(Jedenfalls) Vergleichbar	Noch keine Entscheidung	Daten von Gesicht und Fingerabdruck

Bahrain	Verpflichtend an alle Bewohner	Start der Ausgabe war für 2004 geplant	k. A.	k. A.		Geplant als Führerschein, Krankenversicherungskarte, elektronische Geldbörse	Template des Fingerabdrucks
Thailand	Verpflichtend für Bürger	Testphase ab Mitte 2003; Rollout verschoben	Noch keine Entscheidung; Karte soll für Signatur vorausgerüstet sein	Für den Bürger 2,- €	Bürger: 9,10 €	Führerschein, Sozialversicherung, Geldkarte, Notfalldaten, Steuerinformationen	Template des Fingerabdrucks
China	Verpflichtend für Bürger ab 16	8 Mio. im April 2005	Keine PKI	Erwartete Projektkosten 4,74 Mrd. €		Explizit nein	Erste Generation nein
Schweiz	Freiwillig an Bürger und Auslandsschweizer, verpflichtend für Ausländer mit Dauerwohnrecht	Projekt vorläufig gestoppt, Erfolg privater ZDAs wird abgewartet	PKI für Signatur und Authentisierung; Entscheidung unter privaten Wettbewerbern; möglicherweise staatliche Zertifikate für sensible Bereiche (z.B. E-Voting)	Noch keine Entscheidung über Gebühr; Initialaufwand auf 9 Mio. € geschätzt; laufende Kosten pro Jahr bei 1 Mio. Ausweise auf 19 Mio. € geschätzt	Vergleichbar	Explizit nein	Nein
Österreich	Freiwillig an Bürger	Version mit Chip geplant, inzwischen aber wieder offen	Falls PKI: für Signatur und Authentisierung; PKI freiwillig; freie Entscheidung unter privaten Wettbewerbern	z.Z. Bürger: 56,- € für die Karte	Vergleichbar	PIN-gesicherte Speicherkapazität, über die der Inhaber frei verfügen kann	Geplant (Gesicht und Fingerabdruck)

4 Datenschutzrechtliche Anforderungen und Bewertung

4.1 Regelungssystem und Anwendbarkeit

4.1.1 Normative Grundlagen

Datenschutzrechtliche Anforderungen an Chipkartenausweise und die mit ihnen interagierende Peripheriestruktur finden sich auf unterschiedlichen normativen Ebenen. Grundlage der Analyse bildet das deutsche Verfassungs- und einfache Recht. Im Zuge der fortschreitenden Internationalisierung wird beides durch völker- und europarechtliche Normen beeinflusst und verändert. Darüber hinaus zwingt der – zumindest potentiell – grenzüberschreitende Anwendungscharakter der meisten Chipkarten dazu, die überstaatliche Perspektive sowohl auf der technischen als auch auf der rechtlichen Seite mit im Blick zu haben. Der digitale Personalausweis muss auch in anderen Staaten nutzbar sein, weil er ein europaweit akzeptiertes Reisedokument sein wird. Deshalb ist es für den Inhaber auch wichtig zu wissen, unter welchen Umständen seine Daten im Ausland ausgelesen und verwertet werden. Die elektronische Gesundheitskarte sollte die gespeicherten Daten auch ausländischen Ärzten preisgeben, denn je mehr Möglichkeiten bestehen, medizinische Leistungen im europäischen Ausland in Anspruch zu nehmen,[695] desto wichtiger wird die europaweite Nutzbarkeit der Gesundheitskarte.

Dabei ist auf technischer Seite dem Interoperabilitäts- und Kompatibilitätsproblem durch Standardisierung zu begegnen.[696] In rechtlicher Hinsicht sind die deutschen Anforderungen des Datenschutzes in aller Regel höher und stärker ausdifferenziert als die Anforderungen anderer Staaten und europa- und völkerrechtliche Regelungen.[697] Letztere wirken allerdings normativ und argumentativ verstärkend auf die deutsche Rechtslage ein. So ist es anerkannt, dass nationale Normen (innerhalb der jeweiligen Auslegungs-, insbesondere Wortlautgrenzen) entsprechend internationalen Verpflichtungen auszulegen sind. Wird ein völkerrechtlicher Vertrag nach Art. 59 Abs. 2 Satz 1 GG in nationales Recht umgesetzt, so hat das Umsetzungsgesetz zwar nur den Rang eines einfachen Bundesgesetzes.[698] Im Prinzip gilt deshalb die lex posterior-Regel. Das Bundesverfassungsgericht leitet jedoch aus der Entscheidung des Grundgesetzes für die internationale Zusammenarbeit einen Auslegungsgrundsatz ab, der in Zweifelsfällen einer Deutung Vorrang gibt, die in Übereinstimmung mit dem völkerrechtlichen Vertrag steht.[699] Die Verpflichtung der Ge-

---

695 Zur grundfreiheitlichen Inanspruchnahme von Gesundheitsleistungen im europäischen Binnenmarkt s. EuGH, Rs. C-385/99 – Müller-Fauré und van Riet, EuR 2003, 628 (dazu *Nowak*, EuR 2003, 644 ff.) und Rs. C-56/01 – Patricia Inizan, Entscheidung v. 23.10.2003 (abrufbar unter http://curia.eu.int/jurisp/cgi-bin/form.pl?lang=de); zur Frage der Kostenübernahme *Kraus*, GesR 2004, 37 ff.

696 S. näher unten 6.1.2.

697 Zur Entwicklung nationaler Datenschutzrechte vgl. den Überblick bei Simitis-*Simitis*, Einl. Rn. 112 ff.; zum Stand 1999 ausführlich *Banisar/Davies*, J. Marshall J. Computer & Info. L. 1999, 1, 15 ff.; zur Entwicklung außerhalb Europas Roßnagel-*Burkert*, Kap. 2.3, Rn. 78 ff., 90 ff.; zur Umsetzung der DSRL ebd., Rn. 64 ff.; Roßnagel-*Brühann*, Kap. 2.4, Rn. 64 ff.

698 Das gilt unabhängig vom Streit um die Rechtsnatur der Umsetzung (dazu Sachs-*Streinz*, Art. 59 Rn. 60 ff.; AK GG-*Zuleeg*, Art. 24 Abs. 3/Art. 25 Rn. 10 ff., jeweils m.w.N.). Speziell bei der EMRK gibt es zwar Versuche, einen Übergesetzesrang zu begründen, dieser ist jedoch im Ergebnis abzulehnen, vgl. *Pache*, EuR 2004, 393, 398 ff. m.w.N.

699 S. zuletzt sehr ausdrücklich BVerfG, JZ 2004, 1171 (dazu *Klein*, JZ 2004, 1176 ff.; *Grupp/Stelkens*, JZ 2005, 133 ff.; *Sauer*, ZaörV 2005, 35 ff.); ferner BVerfGE 58, 1 (34); 59, 63 (89); *Rojahn* 2000, 135 ff.; *Bleckmann*, DÖV 1996, 137 ff.; *Tomuschat*, HdbStR VII (1992), § 172 Rn. 27 ff.; AK GG-*Zuleeg*, Art. 24 Abs. 3/Art. 25 Rn. 25, 33 ff.

richte zu einer derartigen Auslegung ergibt sich aus der Bindung an Gesetz und Recht (Art. 20 Abs. 3 GG).[700] Etwas anderes gilt nur dann, wenn der Gesetzgeber klar bekundet hat, vom Vertragsinhalt abweichen zu wollen.[701] Genügt eine Entscheidung diesen Anforderungen nicht, so liegt eine Verletzung des in seinem Schutzbereich berührten Grundrechts in Verbindung mit dem Rechtsstaatsprinzip vor.[702]

Erforderlich ist danach eine Auslegung des deutschen Datenschutzrechts konform mit dem Europäischen Gemeinschaftsrecht[703] und der Europäischen Menschenrechtskonvention.[704] Das Bundesverfassungsgericht hat zwar bislang vergleichsweise wenig Gebrauch von der Möglichkeit gemacht, internationale Menschenrechte ins deutsche Verfassungsrecht zu rezipieren.[705] Gleichzeitig hat es jedoch entschieden, dass bei der Auslegung des Grundgesetzes „Inhalt und Entwicklungsstand der Europäischen Menschenrechtskonvention in Betracht zu ziehen“[706] sind und „die Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte als Auslegungshilfe für die Bestimmung von Inhalt und Reichweite von Grundrechten und rechtsstaatlichen Grundsätzen des Grundgesetzes“[707] dient. Der folgende Überblick gibt eine grobe Orientierung über die internationalen Grundlagen des Datenschutzrechts, während Details bei den einzelnen rechtlichen Anforderungen erörtert werden.

4.1.1.1 Internationale Grundlagen

Ähnlich wie im Grundgesetz[708] wird das Recht auf Datenschutz in aller Regel nicht ausdrücklich in den allgemeinen internationalen Menschenrechtsdokumenten erwähnt. Das gilt für die Allgemeine Erklärung der Menschenrechte,[709] den Internationalen Pakt über bürgerliche und politische Rechte (IPbpR)[710] und die Europäische Menschenrechtskonvention (EMRK)[711] ebenso wie für außereuropäische Verträge wie die Amerikanische Men-

700 BVerfG, JZ 2004, 1171, 1174 f.

701 BVerfGE 74, 358 (370); ebenso BVerwGE 110, 203 (210 ff.); zu Bsp. einer völkervertragskonformen Auslegung s. *Britz*, NVwZ 2004, 173 f.

702 BVerfG, JZ 2004, 1171, 1172.

703 *Lorenz*, DVBl. 2001, 428, 431; allgemein zum Erfordernis der europarechtskonformen Auslegung *Craig/De Búrca* 2002, 218 f.; *Rüthers* 2005, 490 ff. Grundlage ist die mittlerweile zumindest im Grundsatz anerkannte Lehre vom Vorrang des Gemeinschaftsrechts (st. Rspr. des EuGH seit Rs. 6/64 – Costa ./. ENEL, Slg. 1964, 1251); s. näher *Craig/De Búrca* 2002, 275 ff.; *Weatherill/Beaumont* 1999, 433 ff.; *Oppermann* 1999, Rn. 616 ff.; *Streinz* 2003, Rn. 168 ff.

704 S. BVerfGE 74, 358 (370); BVerwGE 94, 35 (48 ff.); 100, 287 (296 f.); vgl. ausführlich *Uerpmann* 1993, 35 ff.; 109 ff.; s.a. *Sommermann*, AöR 1989, 391 ff.; *Grabenwarter* 2003, 21 ff. m.w.N.

705 S. *Bryde*, Der Staat 2003, 61, 68 ff.; für Bsp. bis 1993 vgl. *Uerpmann* 1993, 135 ff.

706 BVerfGE 74, 358 (370).

707 BVerfGE 74, 358 (370); JZ 2004, 1171, 1173 f.; vgl. zur Wirkung von Urteilen des EGMR in der deutschen Rechtsordnung *Pache*, EuR 2004, 393, 402 ff. m.w.N.; s.a. *Sauer*, ZaörV 2005, 35 ff.

708 Die Verfassungen der Bundesländer enthalten zum Teil ausdrückliche Gewährleistungen eines Grundrechts auf Datenschutz, zuerst Art. 4 Abs. 2 LVerf NW (seit 1978), ferner Art. 11 Abs. 1 LVerf Bbg., Art. 6 LVerf MV, Art. 33 LVerf Sachs., Art. 6 Abs. 1 LVerf Sachs.-Anh., Art. 6 Abs. 2 LVerf Thür.; Art. 33 LVerf Bln., Art. 12 Abs. 3 LVerf Brem., Art. 4a LVerf Rh.-Pf.; Art. 2 LVerf Saarl.

709 Resolution 217 A (III) v. 10.12.1948, abrufbar unter http://www.unhchr.ch/udhr/lang/ger.htm; s. näher *Kempfler*, JA 2004, 577 ff.

710 Resolution 220 A (XXI) v. 16.12.1966, BGBl. II 1973, 1553; s. allgemein *Akehurst* 1997, 215 ff.; *Steiner/Alston* 2000, 137 ff.

711 Die EMRK ist in Deutschland geltendes Recht seit dem Gesetz v. 7.8.1952, BGBl. II, 685. Sie trat am 3.9.1953 in Kraft. Der offizielle Text der Konvention ist unter http://conventions.coe.int/treaty/en/Treaties/Html/005.htm abrufbar; s. allgemein zur EMRK *v. Dijk/v. Hoof* 1998, 3 ff.; *Merrills/Robertson* 2001, 1 ff.; Frowein/Peukert-*Frowein*, Einl.

schenrechtskonvention.[712] Eine Ausnahme bildet die am 7. Dezember 2000 vom Rat der Europäischen Union und den Präsidenten des Europäischen Parlaments und der Europäischen Kommission verkündete Charta der Grundrechte der Europäischen Union,[713] die in Art. 8 ein Recht auf den Schutz personenbezogener Daten gewährleistet. Die Charta hat zwar keinen rechtsverbindlichen Charakter. Art. 8 wurde jedoch – wie die meisten anderen Artikel – in die Verfassung der Europäischen Union aufgenommen, die am 17. und 18. Juni 2004 in Brüssel von den 25 Mitgliedstaaten der Europäischen Union verabschiedet wurde.[714] Nach der Ratifizierung durch alle Mitgliedstaaten wird die Europäische Union damit über ein geschriebenes Grundrecht auf Datenschutz verfügen.

Es ist sinnvoll, zwischen den unterschiedlichen Organisationen zu unterscheiden, die datenschutzrechtlich relevante Normen erlassen haben. In aller Regel wird auch ohne ausdrückliche Erwähnung aus denjenigen Bestimmungen, die sich in Menschenrechtsverträgen mit dem allgemeinen Schutz der Privatsphäre befassen,[715] ein Recht auf Datenschutz abgeleitet. Ähnlich wie in Deutschland das Bundesverfassungsgericht waren es meist die mit der Kontrolle der jeweiligen Dokumente betrauten Organe, die durch entsprechende Entscheidungen oder Verlautbarungen die Entwicklung beeinflussten.[716]

Auf der Ebene der Vereinten Nationen hat der Ausschuss für Menschenrechte[717] festgehalten, dass aus Art. 17 IPbpR bestimmte Grundsätze für die Datenverarbeitung folgen, nämlich Gesetzesvorbehalt für den öffentlichen wie den privaten Bereich, Zweckbindung, Verbot von Verarbeitungszwecken, die mit dem Pakt in Widerspruch stehen, Datensicherheit sowie Auskunfts- Kontroll-, Korrektur- und Löschungsrechte des Betroffenen.[718] Des Weiteren beschloss die Generalversammlung der Vereinten Nationen am 14. Dezember 1990 Richtlinien betreffend personenbezogene Daten in automatisierten Dateien.[719] Dabei handelt es sich allerdings lediglich um Empfehlungen. Sie beinhalten die Grundsätze der Richtigkeit und Zweckbindung, ein Auskunftsrecht, Beschränkungen für sensible Daten und Anforderungen zur Datensicherheit.

Auch die Richtlinien der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD) für den Schutz der Privatsphäre und den grenzüberschreitenden Datenverkehr personenbezogener Daten[720] und ihre Leitlinien für den Verbraucherschutz im

---

712 American Convention on Human Rights, oder "Pact of San José, Costa Rica", O.A.S. Treaty Series No. 36, 1144 UNTS 123, abrufbar unter http://www.oas.org/juridico/english/Treaties/b-32. htm.

713 ABl. EG 2000 C 364/01.

714 Die Europäische Verfassung (ABl. EU C 310 v. 16.12.2004, S. 1) enthält sogar zwei Normen zum Datenschutz (Art. I-51 I und Art. II-68).

715 Art. 12 der Allgemeinen Erklärung der Menschenrechte, Art. 17 IPbpR, Art. 8 EMRK, Art. 11 ACHR.

716 Zum System der institutionalisierten Überwachung der Einhaltung von Menschenrechten auf der internationalen Ebene vgl. *Cassese* 2001, 363 ff.; *Akehurst* 1997, 213 ff.

717 Der Ausschuss (Human Rights Committee) nimmt nach Art. 41 ff. IPbpR die Berichte der Staaten zur Umsetzung entgegen und verhandelt staatliche Mitteilungen über Verstöße. Außerdem besteht die Möglichkeit der Individualbeschwerde nach einem Zusatzprotokoll. Der Ausschuss kann nach Art. 40 Abs. 4 IPbpR allgemeine Bemerkungen zur Konvention erstellen; s. näher *Harris* 1998, 647 ff.; *Shaw* 1997, 226 ff. m.w.N.; ausführlich *McGoldrick* 1991; *Steiner/Alston* 2000, 705 ff.

718 *Human Rights Committee* 1994, insbes. Rn. 1, 10; auch nach *Seidel* 1996, 40 ff. und Meyer-*Bernsdorff*, Art. 8 Rn. 4 folgt aus Art. 17 IPbpR eine Pflicht der Vertragsstaaten, Datenerhebungen gesetzlich zu regeln und nur zu bestimmten Zwecken zuzulassen; s.a. *Gridl* 1999, 157 ff.

719 Resolution 44/132-14.12.1990, UN Doc. E/CN.4/Sub.2/1988/22, abrufbar unter http://www.datenschutz-berlin.de/recht/int/uno/gl_pbdde.htm; s. näher Roßnagel-*Burkert*, Kap. 2.3, Rn. 37 ff.; *Gridl* 1999, 182 ff.; Simitis-*Simitis*, Einl. Rn. 177 ff.; *Wuermeling* 2000, 12 f.

720 V. 23.9.1980, OECD-Dokument C (80) 58; s. Roßnagel-*Burkert*, Kap. 2.3, Rn. 22 ff.; *Ellger* 1990, 513 ff.; *Gridl* 1999, 172 ff.; Simitis-*Simitis*, Einl. Rn. 169 ff.; *Viethen* 2003, 24 f.; *Tinnefeld/Ehmann* 1998, 51 f.; zum Hintergrund *Meister*, DuD 1980, 9, 13 ff. Die Richtlinien haben durchaus Einfluss auf die nationale Rechtsentwicklung der OECD-Mitgliedstaaten, s. *OECD* 2004, 7 m.w.N.

elektronischen Geschäftsverkehr[721] stellen nur Empfehlungen dar. Beide sind für diese Untersuchung von geringerem Interesse, könnten aber bei (vor allem grenzüberschreitenden) wirtschaftlich orientierten Anwendungen und Abrechnungssystemen, insbesondere bei der elektronischen Gesundheitskarte, Bedeutung erlangen. Sie fordern das Vorliegen einer gesetzlichen Grundlage oder Einwilligung für die Datenverwendung, die Einhaltung der Grundsätze der Transparenz, Datenqualität und Zweckbindung und die Sicherstellung von Betroffenenrechten. Allerdings ergeben sich insoweit keine rechtlich bindenden Verpflichtungen der Mitgliedstaaten der OECD.

Im europäischen Kontext ist zwischen Normen und Entscheidungen unter dem Dach des Europarats einerseits und der supranationalen Gesetzgebung durch die Europäische Union andererseits zu unterscheiden.

Der Europäische Gerichtshof für Menschenrechte hat anerkannt, dass die Sammlung und Speicherung personenbezogener Daten in die Rechte aus Art. 8 Abs. 1 EMRK eingreift und einer Rechtfertigung bedarf, die ihrerseits den Anforderungen aus Art. 8 Abs. 2 EMRK genügen muss.[722] Damit ist eine gesetzliche Grundlage erforderlich, die ausreichend deutlich und genau sein muss.[723] Ein Eingriff ist nur zulässig, wenn er der nationalen oder öffentlichen Sicherheit, dem wirtschaftlichen Wohl des Landes, der Aufrechterhaltung der Ordnung, der Verhütung von Straftaten, dem Schutz der Gesundheit oder der Moral oder dem Schutz der Rechte und Freiheiten anderer dient. Außerdem ist das Verhältnismäßigkeitsprinzip zu beachten. Vor allem im Gesundheitsbereich sind erhöhte Anforderungen zu stellen.[724] Schließlich bestehen ein Auskunftsrecht und eine Unterrichtungspflicht bei heimlichen Datensammlungen.[725]

Auch die Mitgliedstaaten des Europarats trugen zu der Entwicklung bei. Durch das Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten vom 28. Januar 1981[726] schufen sie erstmals einen rechtsverbindlichen völkerrechtlichen Vertrag zum Datenschutz.[727] Dieser stellt Grundsätze für die Datenverarbeitung auf, die von den Unterzeichnerstaaten intern als Mindeststandards umzusetzen

721 Guidelines for Consumer Protection in the Context of Electronic Commerce, abrufbar unter http://europa.eu.int/comm/internal_market/privacy/instruments/ocdeguideline_en.htm; s. *Scholz* 2003, 117.

722 Grundlegend Leander ./. Schweden, Urteil v. 26.3.1987, ferner Z ./. Finnland, Urteil v. 25.2.1997; Amann ./. Schweiz, Urteil v. 16.2.2000, alle abrufbar unter http://www.echr.coe.int/Eng/Judgments.htm; s.a. den Bericht der Kommission in Rs. 15220/89 (DR 75, 30) und die Entscheidung in Rs. 25099/94 (DR 81, 136), sowie *Reed/Murdoch* 2001, 403 f.; Frowein/Peukert-*Frowein*, Art. 8 Rn. 5; Meyer-*Ladewig*, Art. 8 Rn. 11 ff.; *Seidel* 1996, S. 38 f.; ausführlich *Gridl* 1999, 106 ff.; *Matz* 2003, 108 ff.; zu den frühen Entscheidungen *Breitenmoser* 1986, 239 ff.; vgl. zur Auslegung von „privacy" i.S.v. Art. 8 EMRK *Merrills/Robertson* 2001, 138 ff.; *Harris/Boyle/Warbrick* 1995, 302 ff.; *Gusy*, DVR 1984, 289 ff.

723 Amann ./. Schweiz, Urteil v. 16.2.2000 (abrufbar unter http://www.echr.coe.int/Eng/Judgments.htm), Abs. 50, 55 ff.

724 Z ./. Finnland, Urteil v. 25.2.1997 (abrufbar unter http://www.echr.coe.int/Eng/Judgments.htm), Abs. 95; dazu *Mowbray* 2001, 362 ff.; *Peters* 2003, 161.

725 S. *Breitenmoser* 1986, 246 f.

726 European Treaty Series No. 108, abrufbar unter http://www.datenschutz-berlin.de/recht/eu/eurat/dskon_de.htm. Deutschland hat das Übereinkommen am 19.6.1985 ratifiziert, s. BGBl. II, 1985, 539. Es trat am 1.10.1985 in Kraft; näher *Ellger* 1990, 460 ff.; *Gridl* 1999, 190 ff.; Simitis-*Simitis*, Einl. Rn. 136 ff.; *Viethen* 2003, 31 ff.; *Scholz* 2003, 114 ff. m.w.N; grundlegend *Henke* 1986.

727 *Henke* 1986, 48. Die Konvention hat Vorläufer in den Entschließungen (73) 22 und (74) 29 über den Schutz der Privatsphäre natürlicher Personen gegenüber elektronischen Datenbanken im nichtöffentlichen bzw. öffentlichen Bereich.

sind.[728] Hierzu zählen Zweckbindung, eingeschränkte Erfassung, Datenqualität, Auskunftsrecht und die Verantwortlichkeit des Datenverwenders.[729] Als (nicht verbindliche) Auslegungshilfe existieren Empfehlungen des Ministerkomitees des Europarates zum Übereinkommen, die unbestimmte Rechtsbegriffe bereichsspezifisch konkretisieren.[730] Zur Anpassung an die weitere Entwicklung innerhalb der Europäischen Union wurde am 23. Mai 2001 ein Zusatzprotokoll verabschiedet, das am 1. Juli 2004 in Kraft trat.[731] Es verpflichtet die Staaten in Art. 1 zur Einrichtung einer unabhängigen Kontrollinstanz zur Überwachung des Übereinkommens und des Zusatzprotokolls. Art. 2 des Zusatzprotokolls lässt den Transfer von Daten in Staaten, die keine Parteien des Übereinkommens sind, nur bei Vorliegen eines adäquaten Datenschutzniveaus zu.

Neben dem Übereinkommen und dem Zusatzprotokoll kommt dem Schutz durch Art. 8 EMRK besondere Bedeutung zu, weil das Übereinkommen aus dem Jahre 1981 lediglich die automatisierte Datenverarbeitung erfasst[732] und nur bei Verletzung einer Norm der Konvention selbst die Möglichkeit der Individualbeschwerde eines Bürgers gegen seinen Staat besteht.[733] Andererseits reicht das Übereinkommen insofern weiter, als es ausdrücklich auch die Datenverarbeitung im nichtöffentlichen Bereich erfasst.

Die Entwicklung in der Europäischen Gemeinschaft verlief parallel zu der im Rahmen des Europarats. Auch der Europäische Gerichtshof verfügt über eine Rechtsprechungstradition im Grundrechtsbereich. Bereits lange vor der Proklamation der Charta der Grundrechte der Europäischen Union, aber auch weit vor der Einführung von Art. 6 Abs. 1 und Abs. 2 EUV, die erstmals im Europarecht in allgemeiner Form auf die Menschenrechte und die Rechte aus der Europäischen Menschenrechtskonvention Bezug nahmen, ging das Gericht deutlich über die ausdrücklich in den europäischen Verträgen enthaltenen Grundrechte hinaus.[734] Es ordnet die Grund- und Menschenrechte der Unionsbürger als allgemeine Rechtsgrundsätze in das ungeschriebene primäre Gemeinschaftsrecht ein und findet diese Grundsätze in den gemeinsamen Verfassungsüberlieferungen der Mitgliedstaaten.[735] Hierbei rekurriert der Europäische Gerichtshof maßgeblich auf internationale und europäische Abkommen über Menschenrechte, an denen die Mitgliedstaaten beteiligt sind: in der Ver-

728 Das Übereinkommen ist „non-self-executing“ und verleiht keine direkten Rechte an die Bürger, s. schon den Explanatory Report, Nr. 38. (http://conventions.coe.int/Treaty/EN/cadreprincipal.htm); Simitis-*Simitis*, Einl. Rn. 138; *Ellger* 1990, 463; *Schild*, EuZW 1991, 745, 747.

729 S. im Einzelnen *Henke* 1986, 100 ff., 127 ff., 135 ff.

730 Näher Simitis-*Simitis*, Einl. Rn. 163 ff.; Bsp. bei *Schild*, EuZW 1991, 745, 747.

731 Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows, European Treaty Series No. 181, abrufbar unter http://conventions.coe.int/Treaty/en/Treaties/Html/181.htm; vgl. ausführlich *Hornung*, DuD 2004, 719 ff.

732 Zu Hintergrund und Inhalt dieser Einschränkung vgl. *Henke* 1986, 78 ff.

733 Art. 34 EMRK; zum Verfahren vgl. *Merrills/Robertson* 2001, 297 ff. m.w.N.; *Grabenwarter* 2003, 58 ff.; *Peters* 2003, 223 ff.; zur Rechtslage vor der Reform des Beschwerdeverfahrens *v. Dijk/v. Hoof* 1998, 44 ff.

734 Zur Entwicklung allgemein *Weatherill/Beaumont* 1999, 284 ff.; *Craig/De Búrca* 2002, 317 ff.; *v. Bogdandy*, CMLRev 2000, 1307 ff.; *Jacobs*, E.L.Rev. 2001, 331 ff.; *Oppermann* 1999, Rn. 491 ff.; die Verwendung von Grundrechten durch den EuGH wird kritisch beleuchtet von *Coppel/O'Neill*, CMLRev 1992, 669 ff. (s. aber die Gegenkritik bei *Weiler/Lockhart*, CMLRev 1995, 32 ff. und 579 ff.); zusammenfassend zur gemeinschaftsrechtlichen Begründung von Grundrechten *Nicolaysen*, EuR 2003, 719 ff.

735 S. EuGH, Rs. 4/73, Slg. 1974, 491 – Nold ./. Kommission, Abs. 13; Rs. 44/79, Slg. 1979, 3727 – Hauer ./. Land Nordrhein-Westfahlen, Abs. 14 f.; *Craig/De Búrca* 2002, 323 ff.; *Usher* 1998, 2 ff. Nach *Mähring*, EuR 1991, 369, 370 war das Recht auf informationelle Selbstbestimmung jedenfalls 1991 ein allgemeiner Grundsatz der Verfassungstraditionen der Mitgliedstaaten; s.a. *Schorkopf* 2002, Rn. 14, 35 ff.

gangenheit vor allem die Europäische Menschenrechtskonvention, daneben aber auch die Europäische Sozialcharta und die Allgemeine Erklärung der Menschenrechte.[736] In seiner Rechtsprechung hat der Europäische Gerichtshof bereits im Jahre 1969 die Grundrechtsqualität des Datenschutzes anerkannt[737] und in der Folge bestätigt und ausgebaut.[738]

Nach der Proklamation der Charta der Grundrechte der Europäischen Union zeichnet sich ab, dass diese trotz ihres nicht rechtsverbindlichen Charakters vom Europäischen Gerichtshof für den Zeitraum bis zur allseitigen Ratifizierung der Verfassung der Europäischen Union maßgeblich herangezogen werden wird, weil sie „auf höchster Ebene der Ausdruck eines demokratisch zustande gekommenen politischen Konsenses darüber ist, was heute als Katalog der von der Gemeinschaftsrechtsordnung garantierten Grundrechte gelten kann".[739] Sie dürfte damit – unabhängig von der Unsicherheit über die Ratifizierung der Verfassung – durch die Rechtsprechung des Gerichtshofs faktisch verbindlichen Charakter erlangen und würde dadurch an die Stelle der Europäischen Menschenrechtskonvention treten, die in der Rechtsprechung des Gerichts im Laufe der Zeit einen immer größeren Stellenwert eingenommen hat.[740] Zu beachten ist, dass die Charta der Grundrechte nur für das Handeln der Organe der Europäischen Union und für die Mitgliedstaaten bei der Durchführung des Rechts der Union gilt. Sie enthält in Art. 8 – der wortgleich in Art. II-68 des Vertrages über eine Verfassung für Europa übernommen wurde – ein Grundrecht auf Datenschutz und erlaubt eine Datenverarbeitung nur nach Treu und Glauben zu festgelegten Zwecken.[741] Erforderlich ist wie im deutschen Recht eine Einwilligung oder gesetzliche Ermächtigung. Der Betroffene hat ein Auskunfts- und Berichtigungsrecht, und es ist eine unabhängige Kontrolle vorgesehen. Für Art. 8 der Charta greift die allgemeine Grundrechtsschranke nach Art. 52 Abs. 1 des Dokuments, in dem Gesetzesvorbehalt, Wesensgehaltsperre und Verhältnismäßigkeitsgrundsatz verankert sind.[742]

---

736 *Oppermann* 1999, Rn. 491.

737 EuGH, Rs. 29/69, Slg. 1969, 419 – Stauder ./. Stadt Ulm (allerdings ohne ausdrückliche Nennung), dazu *Craig/De Búrca* 2002, 320 f.

738 S. EuGH, Rs. 145/83, Slg. 1985, 3539 – Adams ./. Kommission; Rs. C-404/92 P, Slg. 1994 I, 4737 (= EuGRZ 1995, 247) – X ./. Kommission.

739 Schlussanträge des Generalanwalts *Mischo* in den verbundenen Rs. C-20/00 und C-64/00, Booker Aquaculture ./. The Scottish Ministers (abrufbar unter http://curia.eu.int/jurisp/cgi-bin/form.pl?lang =de), Abs. 126; zum rechtlichen Status der Charta vgl. *de Witte*, MJ 2001, 81 ff.; *Callies*, EuZW 2001, 261, 267; *Tettinger*, NJW 2001, 1010; s. zum Hintergrund *Weber* 2002, 1 ff.; zur Interpretation der Charta vgl. *Dorf*, JZ 2005, 126 ff.; zur verbindlichen Wirkung nach einer potentiellen Ratifizierung der Verfassung s. *Schmitz*, EuR 2004, 691, 697 f.

740 Der EuGH berücksichtigt mittlerweile die EMRK nicht nur als solche, sondern in der Ausprägung, die sie durch die Rspr. des EGMR gefunden hat, s. EuGH, Rs. C-13/94, Slg. 1996, I-2143 – P ./. S, Abs. 16; Rs. C-74/95 und C-129/95, Slg. 1996, I-6609 – Strafverfahren gegen X, Abs. 25; Rs. C-274/99 P, Slg. 2001, I-1611 – Connolly ./. Kommission, Abs. 39 ff.; s. näher *Kühling*, EuGRZ 1997, 296, 297 f.; *Alber/Widmaier*, EuGRZ 2000, 497, 505; vgl. zur parallelen Frage der Berücksichtigung von Urteilen des EGMR in Deutschland *Pache*, EuR 2004, 393, 402 ff. m.w.N.; s. zur Funktion der Charta als „Konkretisierung gemeinsamer Werte" *Schmitz*, EuR 2004, 691, 704 ff.; zum Verhältnis von Charta und EMRK s. *Lemmens*, MJ 2001, 49 ff.; *Lenaerts/de Smijter*, MJ 2001, 90, 96 ff.; *Tettinger*, NJW 2001, 1010, 1011; *Grabenwarter* 2003, 29 ff.

741 S. im Einzelnen Meyer-*Bernsdorff*, Art. 8 Rn. 1 ff; zum Grundrechtskatalog des Verfassungsvertrages vgl. *Grabenwarter*, EuGRZ 2004, 563 ff.; *Kingreen*, EuGRZ 2004, 570 ff. Der Vertrag enthält in Art. I-51 eine weitere Norm zum Datenschutz.

742 Näher Meyer-*Borowsky*, Art. 52 Rn. 18 ff.; *Schmitz*, EuR 2004, 691, 709 ff.

Im sekundären europäischen Gemeinschaftsrecht[743] finden sich für Chipkartensysteme relevante Normen insbesondere in der allgemeinen Datenschutzrichtlinie der Europäischen Gemeinschaft vom 24. Oktober 1995.[744] Sie schafft Mindeststandards zur Vereinheitlichung des bis dahin stark unterschiedlichen Datenschutzniveaus in den Mitgliedstaaten. Der Europäische Gerichtshof hat mittlerweile entschieden, dass zumindest die Grundsätze in Art. 6 Abs. 1 c) und Art. 7 lit. c, e DSRL unmittelbar durch nationale Gerichte anwendbar sind.[745] Weitere Regelungen zum Datenschutz enthält die Datenschutzrichtlinie für elektronische Kommunikation.[746] Beide Richtlinien sind in Deutschland inzwischen umgesetzt. Sie fordern spezifische Rechtsgrundlagen, Zweckbindung, Transparenz, Verhältnismäßigkeit, Datensicherheit, Betroffenenrechte und unabhängige Kontrollen.[747]

Vom Anwendungsbereich her erfassen die Vorgaben des Europarechts nicht alle Chipkartenausweise. Art. 3 Abs. 2 und Erwägungsgrund 13 DSRL nehmen ausdrücklich Datenverarbeitungen bei Tätigkeiten im Rahmen der Gemeinsamen Außen- und Sicherheitspolitik (Titel V des Vertrages über die Europäische Union) und der Polizeilichen und Justiziellen Zusammenarbeit in Strafsachen (Titel VI) von der Anwendung ebenso aus wie „Verarbeitungen betreffend die öffentliche Sicherheit,..., die Sicherheit des Staates...und die Tätigkeiten des Staates im strafrechtlichen Bereich“. Auch die Grundrechtecharta gilt nicht umfassend, sondern nach Art. 51 Abs. 1 für die Mitgliedstaaten ausschließlich bei der Durchführung des Rechts der Union. Das betrifft im Wesentlichen den Erlass von normativen Akten zur Umsetzung von Richtlinien in das nationale Recht und die administrative Durchführung von Unionsrecht, insbesondere von Verordnungen.[748]

Die Ausnahmen in der Datenschutzrichtlinie gelten insbesondere für den digitalen Personalausweis, wenn und weil dieser als staatliches Identifikationsdokument gerade der Abwehr von Gefahren für die öffentliche Sicherheit dienen soll.[749] In privaten Anwendungsbereichen des Personalausweises (beispielsweise für die Signaturfunktion) und bei Chipkarten im nicht-hoheitlichen Bereich stellt sich dies anders dar. Das Problem ist insoweit entschärft, als der deutsche Gesetzgeber bei der Umsetzung der Richtlinie die Einschränkungen ihres Anwendungsbereiches nicht übernommen, sondern allgemeingültige Normen geschaffen hat. Diese sind auch auf Ausweise anwendbar, die nicht in den Geltungsbereich der Richtlinie fallen.

---

743 Zur Rechtssetzungskompetenz der EG im Bereich des Datenschutzes unter den Gesichtspunkten der Prinzipien der begrenzten Einzelermächtigung, Subsidiarität und Verhältnismäßigkeit vgl. *Viethen* 2003, 70 ff., 122 ff., 130 ff.

744 Richtlinie 95/46/EG des Europäischen Parlaments und des Rates v. 24.10.1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. EG L 281/31 v. 23.11.1995,; s. zum Hintergrund Simitis-*Simitis*, Einl. Rn. 188 ff.; *ders.*, NJW 1997, 281 ff.; Roßnagel-*Burkert*, Kap. 2.3, Rn. 44 ff.; *Dammann/Simitis* 1997, Einl.; *Ehmann/Helfrich* 1999, 49 ff.; *Schild*, EuZW 1996, 549 ff.; *Gounalakis/Mand*, CR 1997, 431 ff.; *Wurst*, JuS 1991, 448 ff.

745 EuGH, Urteil v. 20.5.2003, Rs. C-465/00, C-138/01 und C-139/01 – Österreichischer Rundfunk u.a., DuD 2003, 573, Abs. 95 ff.; für eine Übertragung auf die gesamte DSRL *Brühann*, DuD 2004, 201, 208 f. (s. bereits *Jacob*, RDV 1999, 1, 3); zurückhaltend *Viethen* 2003, 47. In jedem Fall bildet die DSRL eine Vorgabe für die Auslegung der Normen, die sie im nationalen Recht umsetzen, s. *Lorenz*, DVBl. 2001, 428, 431.

746 Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates v. 12.7.2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation, ABl. EG L 201/37 v. 31.7.2002, s. *Gola/Klug* 2003, 26 ff.

747 Näher Roßnagel-*Brühann*, Kap. 2.4, Rn. 15 ff.; *Gola/Klug* 2003, 18 ff.; s.a. unten bei der Behandlung der jeweiligen Einzelfragen.

748 Meyer-*Borowsky*, Art. 51 Rn. 25 ff.

749 *Golembiewski/Probst* 2003, 30.

4.1.1.2 Deutsches Datenschutzrecht

Das deutsche Datenschutzrecht ist zum Teil durch diese völker- und europarechtlichen Vorgaben geprägt worden und hat umgekehrt deren Entwicklung beeinflusst. Es ist zwischen den verfassungsrechtlichen Anforderungen und einfachgesetzlichen Datenschutznormen zu unterscheiden, die allerdings häufig Ausprägungen des Verfassungsrechts widerspiegeln. Inhalt und Reichweite des grundgesetzlichen Rechts auf informationelle Selbstbestimmung (oder Datenschutz) werden nach wie vor maßgeblich durch das vom Bundesverfassungsgericht getroffene Volkszählungsurteil bestimmt, das am 15. Dezember 2003 seinen 20jährigen Geburtstag feierte.[750]

In dieser Entscheidung – deren Inhalt und Bedeutung nur vor dem Hintergrund der gesellschaftlichen Diskussion um die Volkszählung zu verstehen ist[751] – wurde erstmals in Deutschland höchstrichterlich anerkannt, dass der Datenschutz Verfassungsrang hat.[752] Zwar hatte das Bundesverfassungsgericht bereits im Jahre 1969 im Mikrozensus-Urteil festgestellt, die Menschenwürde sei verletzt, „wenn der Staat das Recht für sich in Anspruch nehmen könnte, den Menschen zwangsweise in seiner ganzen Persönlichkeit zu registrieren und zu katalogisieren, sei es auch in der Anonymität einer statistischen Erhebung, und ihn damit wie eine Sache zu behandeln, die einer Bestandsaufnahme in jeder Beziehung zugänglich ist".[753] Im Volkszählungsurteil begründeten die Richter jedoch ein erheblich weiter reichendes, allgemeines Grundrecht des Einzelnen. Das Gericht leitete aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG „die aus dem Gedanken der Selbstbestimmung folgende Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen"[754] ab, wobei es allerdings auf dogmatische Vorarbeiten der Wissenschaft aufbauen konnte.[755]

Das Grundrecht auf informationelle Selbstbestimmung fußt im allgemeinen Persönlichkeitsrecht.[756] Es bildet jedoch gegenüber den zuvor entwickelten Fallgruppen dieses Rechts

---

750 BVerfGE 65, 1; s. aus der späteren Rspr. BVerfGE 77, 1 (46 ff.); 84, 192 (194 ff.); 92, 191 (197 ff.); zum Volkszählungsurteil vgl. etwa *Simitis*, NJW 1984, 398 ff.; *Schlink*, Der Staat 1986, 233 ff.; *Mückenberger*, KJ 1984, 1 ff.; *Heußner*, BB 1990, 1281 ff.; *Konferenz der Datenschutzbeauftragten*, DÖV 1984, 504 ff.; *Vogelgesang* 1987, 51 ff.; *Faber*, RDV 2003, 278 ff.; kritischer *Duttge*, NJW 1998, 1615 ff.; zum Folgenden und zu den aktuellen Herausforderungen im Bereich des Internets vgl. *Hornung*, MMR 2004, 3 ff.

751 Vgl. hierzu und zum konkreten Entscheidungsinhalt ausführlich unten 7.3.2.1.

752 *Konferenz der Datenschutzbeauftragten*, DÖV 1984, 504; Simitis-*Simitis*, Einl. Rn. 30. Eine ausdrückliche Erwähnung eines „Grundrechts auf Datenschutz" erfolgte noch nicht im Volkszählungsurteil, aber später in BVerfG, NJW 1991, 2129, 2132.

753 BVerfGE 27, 1 (6); s. zu weiteren Entscheidungen des Gerichts, auf die das Volkszählungsurteil aufbaut, AK GG-*Podlech*, Art. 2 Abs. 1 Rn. 20 m.w.N.; *Vogelgesang* 1987, 39 ff.

754 BVerfGE 65, 1 (42).

755 Z.B. *Podlech*, DVR 1976, 23 ff., *ders.* 1976, 313; *ders.* 1982, 453; *Steinmüller/Lutterbeck/Mallmann/Harbort/Kolb/Schneider* 1971, 88 ff.; *Benda* 1974, 32; *Mallmann* 1976, 47 ff.; s.a. die Nachweise bei Roßnagel-*Trute*, Kap. 2.5, Rn. 7; *Denninger*, KJ 1985, 215, 218. Von „einer der größten Erfindungen der Rechtswissenschaft" spricht in diesem Zusammenhang *Vultejus*, ZRP 2002, 70. Das dürfte jedenfalls eher zutreffen als die Auffassung von *Fromme*, FAZ v. 17.12.1983, 12, wonach das BVerfG „ein neues Grundrecht erfunden" habe. Vielmehr gab es einen internen Beschluss des Gerichts, in den Urteilsgründen keine Zitate auszuweisen, s. *Podlech*, Leviathan 1984, 85, 91; s. zur (philosophischen) Begründung informationeller Selbstbestimmung auch *Rössler* 2001, 201 ff.

756 Zur Herleitung des allgemeinen Persönlichkeitsrechts und der Relevanz der Menschenwürde in diesem Zusammenhang vgl. v. Münch/Kunig-*Kunig*, Art. 1 Rn. 10; v. Mangoldt/Klein/Starck-*Starck*, Art. 2 Rn. 15; kritisch gegenüber einer Vermengung von Art. 1 Abs. 1 und Art. 2 Abs. 1 GG ebd., Art. 2 Rn. 54 f.; zur Einbettung des Rechts auf informationelle Selbstbestimmung in das allgemeine Per-

keine neue Kategorie, sondern liegt „quer“ zu ihnen.[757] Seine dogmatische Bedeutung in diesem Zusammenhang besteht vor allem in der Abkehr von der bis dahin vorherrschenden „Sphärentheorie“.[758] Das Bundesverfassungsgericht erkannte, dass es aufgrund den der Informationstechnologie eigenen Verarbeitungs- und Verknüpfungsmöglichkeiten „unter den Bedingungen der automatisierten Datenverarbeitung kein `belangloses Datum` mehr“ gibt.[759]

Neben dieser auf den Schutz des Einzelnen und seiner Identität[760] bezogenen Argumentationslinie misst das Bundesverfassungsgericht dem Grundrecht eine überindividuelle Komponente zu: „Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß. Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen. Wer damit rechnet, dass etwa die Teilnahme an einer Versammlung oder einer Bürgerinitiative behördlich registriert wird und dass ihm dadurch Risiken entstehen können, wird möglicherweise auf eine Ausübung seiner entsprechenden Grundrechte (Art. 8, 9 GG) verzichten. Dies würde nicht nur die individuellen Entfaltungschancen des Einzelnen beeinträchtigen, sondern auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungsfähigkeit und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist.“[761] Informationelle Selbstbestimmung ist damit nicht nur ein subjektives Recht des Einzelnen, und dieser kann auch nicht eigentumsähnlich darüber verfügen. Sie ist eine strukturelle Komponente jeder demokratischen Gesellschaft.[762] Diese Verbindung mit dem kommunikativen, das heißt auch diskursiven Aspekt dieser Gesellschaft[763] verleiht der informationellen Selbstbestimmung besonderes Gewicht. Hierdurch

---

sönlichkeitsrecht s.a. *Jarass*, NJW 1989, 857 ff.; *Kunig*, Jura 1993, 595 ff.; zusammenfassend hierzu *Scholz* 2003, 128 ff. m.w.N.

757 V. Münch/Kunig-*Kunig*, Art. 2 Rn. 38; Sachs-*Murswiek*, Art. 2 Rn. 73; unentschieden Dreier-*Dreier*, Art. 2 Rn. 79.

758 *Simitis*, NJW 1984, 398, 402; v. Münch/Kunig-*Kunig*, Art. 2 Rn. 41; M/D-*Di Fabio*, Art. 2 Abs. 1 Rn. 174; Sachs-*Murswiek*, Art. 2 Rn. 106; *Scholz* 2003, 132 f. m.w.N.; AK GG-*Podlech*, Art. 2 Abs. 1 Rn. 40; *Mückenberger*, KJ 1984, 1, 7 f.; Roßnagel-*Trute*, Kap. 2.5, Rn. 10 f.; *Donos* 1998, 70 f.; *Geis*, JZ 1991, 112, 113 (der wegen der Gefahr einer Aufgabe des absoluten Schutzes der Intimsphäre für die Aufrechterhaltung der Sphärentheorie plädiert, ebd., 115 ff.); a.A. *Gounalakis/Rhode* 2002, Rn. 194; *Schmidt-Glaeser*, HdbStR VI (2001), § 129 Rn. 77.

759 BVerfGE 65, 1 (45).

760 Vgl. zum Hintergrund des Schutzes der Identitätsbildung oben 1.

761 BVerfGE 65, 1 (43); dazu Roßnagel-*Trute*, Kap. 2.5, Rn. 9; *Denninger*, KJ 1985, 215, 220 f.

762 *Simitis*, DuD 2000, 714, 719. Das ist (auch) Ausdruck der Auffassung des BVerfG zur Rechtsnatur der Grundrechte, wonach diese nicht nur subjektiv-rechtliche Bedeutung haben, sondern auch eine objektive Wertordnung verkörpern (st. Rspr. seit BVerfGE 7, 198). Zu weitgehend ist es allerdings zu folgern, das Recht auf informationelle Selbstbestimmung sei „kein subjektives Recht“ (so aber *Donos* 1998, 120 ff.). Die individuelle und überindividuelle Komponente ergänzen sich vielmehr gegenseitig. Andernfalls bestünde die Gefahr, den einzelnen Betroffenen mit seinen Interessen aus dem Blick zu verlieren oder ihn zugunsten einer verobjektivierten Perspektive zu funktionalisieren.

763 Zum Konzept des Datenschutzes als kommunikatives Recht s. bereits *Simitis*, DVR 1973, 138, 147 ff., ferner *ders.* 1982, 495 ff.; *Hoffmann-Riem* 1998, 11 ff.; *Roßnagel*, KJ 1990, 267 ff.; *Roßnagel/Pfitzmann/Garstka* 2001, 38 f., 58; zusammenfassend Simitis-*Simitis*, § 1 Rn. 36 ff. m.w.N.; zur Einordnung in die prozedural-diskursive Grundrechtstheorie und zur Verbindung zu *Habermas'* Theorie des kommunikativen Handelns s. *Donos* 1998, 108 ff.; zum Begriff des Privaten aus philosophischer Sicht vgl. *Rössler* 2001, 16 ff.

wird sie insbesondere in Abwägungsprozessen (beispielsweise bei der Frage der Verhältnismäßigkeit) substantiell verstärkt.

Das Bundesverfassungsgericht hat die Ausformungen des Grundrechts auf informationelle Selbstbestimmung im Volkszählungsurteil und in späteren Entscheidungen weiter konkretisiert. Diese bilden sich in den heutigen allgemeinen verfassungsrechtlichen Grundsätzen des Datenschutzrechts ab; im Einzelnen handelt es sich insbesondere um das Erfordernis eines überwiegenden Allgemeininteresses zur Beschränkung des Grundrechts, den Gesetzesvorbehalt, den Vorrang bereichsspezifischer Regelungen, den Bestimmtheitsgrundsatz, die Grundsätze der Datensparsamkeit, Transparenz und Zweckbindung, das Verbot der Vorratsdatenspeicherung und eines allgemeinen Personenkennzeichens, das Prinzip der informationellen Gewaltenteilung, die Beschränkung von Profilbildungen und das Verhältnismäßigkeitsprinzip.[764] Diese stellen das Grundgerüst der datenschutzrechtlichen Überlegungen dieser Abhandlung dar.

Einfachgesetzliche Datenschutznormen gliedern sich in das allgemeine Datenschutzrecht (Bundesdatenschutzgesetz und Landesdatenschutzgesetze) und bereichsspezifische Regelungen. Inwieweit letztere einschlägig sind, richtet sich nach dem jeweiligen Chipkartensystem. So finden sich datenschutzrechtliche Anforderungen an den digitalen Personalausweis im Personalausweisgesetz; für den Umgang mit Gesundheitsdaten auf der Gesundheitskarte gilt das fünfte Buch des Sozialgesetzbuches.[765] Insbesondere im Gesundheitswesen bestehen gesetzliche Geheimhaltungspflichten, die ebenfalls einen Bezug zum Datenschutz aufweisen. Auch auf der untergesetzlichen Ebene gibt es für einige Chipkarten Regeln zum Datenschutz, etwa im Standesrecht der Ärzte.

Nach § 1 Abs. 3 BDSG gehen auf Bundesebene andere Rechtsvorschriften den Vorschriften des Bundesdatenschutzgesetzes vor, und die Verpflichtung zur Wahrung gesetzlicher Geheimhaltungspflichten oder von Berufs- oder besonderen Amtsgeheimnissen, die nicht auf gesetzlichen Vorschriften beruhen, bleibt unberührt.[766] Dies gilt allerdings nur, soweit eine abweichende Bestimmung für den exakt gleichen Sachverhalt vorliegt.[767] Dies kann durch eine explizite Regelung geschehen, oder durch das Fehlen einer solchen Regelung in einer vom Gesetzgeber erkennbar als abschließend verstandenen Gesamtregelung.

Im personellen Anwendungsbereich ist das Bundesdatenschutzgesetz gemäß § 1 Abs. 2 Nr. 1 BDSG uneingeschränkt auf öffentliche Stellen des Bundes anwendbar. Öffentliche Stellen der Länder werden nach § 1 Abs. 2 Nr. 2 BDSG dagegen nur erfasst, wenn sie Bundesrecht ausführen und der Datenschutz nicht durch Landesgesetz geregelt ist.[768] Ansonsten ist für sie das jeweilige Landesdatenschutzgesetz einschlägig. Nicht-öffentliche Stellen unterfallen dem Bundesdatenschutzgesetz ohne Ausnahme, wenn sie Daten unter Einsatz von Datenverarbeitungsanlagen verarbeiten, nutzen oder dafür erheben (§ 1 Abs. 2 Nr. 3, 1. Alt. BDSG). Der Zugriff auf die elektronisch gespeicherten Daten in Chipkartenausweisen und das Auslesen und Weiterverarbeiten dieser Daten ist nur unter Zuhilfenahme derartiger Anlagen möglich. Insoweit werden die entsprechend tätigen nicht-

764 S. etwa *Roßnagel/Pfitzmann/Garstka* 2001, 70 ff.; Simitis-*Simitis*, Einl. Rn. 30 ff.; *Tinnefeld/Ehmann* 1998, 85 ff.; Roßnagel-*Trute*, Kap. 2.5, Rn. 32 ff.; *Scholz* 2003, 135 ff., jeweils m.w.N. Diese Grundsätze bilden auch die Grundlage für die aktuelle Reformdiskussion; vgl. dazu *Roßnagel/Pfitzmann/Garstka* 2001.

765 S. bereits oben 2.2.1 und 2.2.2.

766 Zum Verhältnis von Berufsgeheimnissen und allgemeinem Datenschutz s. *Tinnefeld/Ehmann* 1998, 115 ff.; Simitis-*Walz*, § 1 Rn. 174 ff.

767 Simitis-*Walz*, § 1 Rn. 169.

768 Die Variante in § 1 Abs. 2 Nr. 2b) (Tätigkeit als Organe der Rechtspflege) ist im vorliegenden Zusammenhang irrelevant.

öffentlichen Stellen zur Einhaltung des Bundesdatenschutzgesetzes verpflichtet, ohne dass es auf die 2. Alternative in § 1 Abs. 2 Nr. 3 BDSG (Verarbeitung, Nutzung oder Erhebung von Daten in oder aus nicht automatisierten Dateien, jedoch unter Ausschluss persönlicher und familiärer Tätigkeiten) ankommt. Etwas anderes gilt jedoch für die Verwendung der Chipkarte als Sichtausweis. Hier ist diese Einschränkung zu beachten.

Nach diesen Kriterien ist für jede Chipkarte und jeden Verwendungsvorgang die jeweils einschlägige Rechtsgrundlage zu bestimmen. So ist zum Beispiel beim digitalen Personalausweis das Personalausweisgesetz vor allen anderen Normen anzuwenden. Soweit dieses keine Regelung enthält, unterfallen nach § 1 Abs. 2 Nr. 1 BDSG zunächst alle mit dem Personalausweis befassten Stellen des Bundes dem Bundesdatenschutzgesetz. Dies betrifft insbesondere die Vollzugsbeamten des Bundes, wie beispielsweise den Bundesgrenzschutz. Bei Antrag, Ausstellung und Kontrolle des Personalausweises werden auch eine Reihe weiterer Behörden tätig, insbesondere Personalausweis- und Landespolizeibehörden. Die Länder führen das Personalausweisgesetz des Bundes als eigene Angelegenheit aus (Art. 83 GG). Da sie jedoch durchweg eigene Landesdatenschutzgesetze erlassen haben, ist das Bundesgesetz nach § 1 Abs. 2 Nr. 2 BDSG nicht anwendbar. Ähnlich wie beim Vorrang von Spezialgesetzen gilt dies allerdings nur, „soweit" eine Regelung durch Landesgesetz erfolgte. Das bedeutet, dass eine Norm des Bundesdatenschutzgesetzes immer dann einschlägig bleibt, wenn das Landesgesetz keine Regelung im sachlichen Geltungsbereich dieser Norm getroffen hat.[769] Insbesondere bei einigen neueren Regelungen wie denjenigen zu mobilen personenbezogenen Speicher- und Verarbeitungsmedien (§ 6c BDSG) kann es zu Abgrenzungsproblemen kommen.[770]

Soweit auch nicht-öffentliche Stellen auf die elektronisch gespeicherten Daten des digitalen Personalausweises zugreifen dürfen,[771] liegt ein Einsatz von Datenverarbeitungsanlagen vor. Damit sind diese Stellen an das Bundesdatenschutzgesetz gebunden. Ansonsten ist die erwähnte Einschränkung in § 1 Abs. 2 Nr. 3, 2. Alt. BDSG zu beachten. Diese dürfte jedoch im Regelfall nicht greifen, sodass das Gesetz anwendbar ist.

Für die elektronische Gesundheitskarte ist zunächst auf die bereichsspezifischen Regeln des Sozialgesetzbuches (insbesondere § 284 Abs. 1 Nr. 2, § 291a und § 307a SGB V), die ärztliche Schweigepflicht und die standesrechtlichen Dokumentations- und Datenschutzpflichten zurückzugreifen.[772] Hinsichtlich des personellen Anwendungsbereiches ist zu unterscheiden.[773] Vertragsärzte nehmen normal am Rechtsverkehr teil. Sie fallen deshalb unter die Bestimmungen des Bundesdatenschutzgesetzes für nicht-öffentliche Stellen. Gleiches gilt für etwaige externe Dienstleister im System der Gesundheitskarte. Für Krankenhäuser ist dagegen nach dem jeweiligen Träger und Bundesland zu differenzieren. Teilweise bestehen Spezialregelungen in Landeskrankenhausgesetzen und Gesundheitsdatenschutzgesetzen. Die Unterschiede sind jedoch für die Gesundheitskarte ohne wesentlichen Belang. Deshalb unterbleibt eine ausführliche Darstellung an dieser Stelle.[774]

769 *Auernhammer*, § 1 Rn. 26; Simitis-*Dammann*, § 1 Rn. 124 f.
770 S.u. 4.3.3.2.2.
771 Dies ist nach der aktuellen Rechtslage durch § 4 Abs. 3 PersAuswG ausgeschlossen; s. hierzu unten 4.2.2.5.
772 S.o. 2.2.2.1.
773 S. die Übersicht bei *Hermeler* 2000, 65 ff.
774 S. im Einzelnen *Hermeler* 2000, 69 ff.; *Meier* 2003, 12 ff.

4.1.2 Grundsätzliche Anwendbarkeit des Datenschutzrechts: Personenbezug

Bundes- wie Landesdatenschutzgesetze sind in ihrem Anwendungsbereich auf „personenbezogene" Daten beschränkt;[775] der Betroffene ist also nur dann geschützt (oder genauer: überhaupt nur dann Betroffener), wenn er identifiziert oder identifizierbar ist.[776] Das entspricht dem Anwendungsbereich des Rechts auf informationelle Selbstbestimmung und damit des Datenschutzrechts insgesamt. Auch für Chipkarten stellt sich daher die Frage, ob die auf ihnen oder durch sie verwendeten Daten personenbezogen sind. Nach der Legaldefinition des § 3 Abs. 1 BDSG ist dies der Fall, wenn es sich um „Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person" handelt. Problematisch ist dabei regelmäßig die Frage der Bestimmtheit oder Bestimmbarkeit.[777]

Für Ausweise im Chipkartenformat ist zwischen den visuell aufgedruckten Daten, elektronisch auf dem Chip gespeicherten Angaben und mittels der Karte in der Peripherie abgelegten Daten zu unterscheiden. Nur im ersten Fall ist der Personenbezug eindeutig: Durch die Verbindung mit Namen, Photo und weiteren Identifikationsdaten des Ausweisinhabers sind alle auf dem Ausweis aufgedruckten Daten unmittelbar personenbezogen. Problematisch ist die Beziehbarkeit jedoch bei anonymisierten, pseudonymisierten und verschlüsselten Daten, sowie insbesondere bei biometrischen Identifikationsdaten.

4.1.2.1 Anonyme, pseudonyme und verschlüsselte Daten

Die einem Datum zugehörige Person ist bestimmt, wenn sich aus den Angaben selbst ergibt, dass sie sich auf diese Person und nur auf diese beziehen. Bestimmbar ist sie dann, wenn ihre Identität mit Hilfe anderer Informationen festgestellt werden kann.[778] Das Bundesdatenschutzgesetz enthält keine nähere Bestimmung über die Abgrenzung zu nicht personenbezogenen Daten. Diese ist im Einzelnen umstritten. Werden zur Herstellung des Personenbezugs technische Verfahren oder wissenschaftliche Erfahrung benötigt, so muss es ausreichen, dass beides objektiv am Markt verfügbar ist.[779] Ist jedoch zur Zuordnung zu einer Person Zusatzwissen erforderlich, so richtet sich der Personenbezug danach, ob die jeweilige Stelle über dieses Wissen verfügt oder es ihr zugänglich ist.[780] Dasselbe Datum kann deshalb je nach verantwortlicher Stelle gleichzeitig personenbezogen und nicht personenbezogen sein. Der Begriff des Personenbezugs ist also relativ.[781]

---

775 Für das Bundesrecht vgl. § 1 Abs. 1 BDSG. Das entspricht auch internationalen Grundsätzen, s. etwa Nr. 1 der Richtlinien der Vereinten Nationen, Art. 2 a) des Übereinkommens des Europarats (dazu *Henke* 1986, 68 ff.) und Art. 2 lit. a DSRL (s. *Schild*, EuZW 1996, 549, 550).

776 Vgl. zum Zusammenhang zwischen Identifizierung und Identität oben 1.

777 Eine Unterscheidung zwischen diesen beiden Kategorien ist allerdings überflüssig, da das Datenschutzrecht in beiden Fällen anwendbar ist, s. Simitis-*Dammann*, § 3 Rn. 22. Entscheidend ist die Abgrenzung zwischen Daten einer bestimmbaren und solchen einer nicht mehr bestimmbaren Person.

778 Simitis-*Dammann*, § 3 Rn. 21; *Tinnefeld/Ehmann* 1998, 184; s.a. Art. 2a DSRL, wonach eine Person bestimmbar ist, „die direkt oder indirekt identifiziert werden kann, insbesondere durch Zuordnung zu einer Kennummer oder zu einem oder mehreren spezifischen Elementen, die Ausdruck ihrer physischen, physiologischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität sind"; dazu Roßnagel-*Brühann*, Kap. 2.4, Rn. 17; *Ehmann/Helfrich* 1999, Art. 2 Rn. 14 ff.; *Dammann/Simitis* 1997, Art. 2 Rn. 1 ff.

779 Simitis-*Dammann*, § 3 Rn. 31; *Hermeler* 2000, 154.

780 Simitis-*Dammann*, § 3 Rn. 32; *Gola/Schomerus*, § 3 Rn. 9.

781 Simitis-*Dammann*, § 3 Rn. 32; *Gola/Schomerus*, § 3 Rn. 9; *Roßnagel/Scholz*, MMR 2000, 721, 722 f.; Roßnagel-*Tinnefeld*, Kap. 4.1, Rn. 22; a.A. für den Fall der Pseudonymisierung Simitis-*Bizer*, § 3 Rn.

Anonyme, pseudonyme und verschlüsselte Daten sind nicht durchweg, aber in einer Vielzahl von Fällen dadurch gekennzeichnet, dass das Zusatzwissen, das zur Anonymisierung, Pseudonymisierung oder Verschlüsselung verwendet wurde, auch zur Re-Individualisierung eingesetzt werden kann. Dieses Wissen ist regelmäßig nur einem einzigen oder wenigen Beteiligten bekannt. Daher ist der Personenbezug der entsprechend behandelten Daten fraglich. Bei Chipkartenausweisen können pseudonyme Verfahren etwa dann eingesetzt werden, wenn diese qualifizierte Signaturen erstellen können und das zugehörige Zertifikat auf ein Pseudonym ausgestellt wird.[782] Außerdem können mit Hilfe der Karte pseudonyme Daten in der Peripherie verarbeitet oder genutzt werden. Die Zentrale Speicherstelle im JobCard-Verfahren muss beispielsweise den konkreten Betroffenen nicht kennen, sondern lediglich alle für ihn eintreffenden Bescheinigungen sammeln, wobei die Daten sogar erst dann zusammengeführt werden müssen, wenn der Leistungsfall eintritt. Auch bei der elektronischen Gesundheitskarte ist der Einsatz von Pseudonymen ein wesentliches Mittel zur Datensparsamkeit.[783] Schließlich sind Fälle denkbar, in denen Daten durch den Karteninhaber oder einen anderen (etwa einen Leistungserbringer im Gesundheitswesen) sicher verschlüsselt und dann zur Speicherung an einen Dritten übermittelt werden.

Daten sind nach § 3 Abs. 6 BDSG anonym, wenn sie „nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können". Da die erste Alternative in der Praxis faktisch nicht zu bewerkstelligen ist,[784] muss die Wahrscheinlichkeit, die Daten einer Person zuordnen zu können, so gering sein, dass sie nach der Lebenserfahrung oder dem Stand der Wissenschaft praktisch ausscheidet.[785] Pseudonymität liegt demgegenüber vor, wenn der Name oder andere Identifikationsmerkmale an den Daten durch ein Kennzeichen ersetzt werden, um die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren (§ 3 Abs. 6a BDSG).[786]

Es wird vertreten, anonyme Daten fielen solange unter das Datenschutzrecht, wie keine „absolute" Anonymisierung im Sinne von § 3 Abs. 6, 1. Alt. BDSG vorliege.[787] Sei hingegen eine Zuordnung, wenn auch mit unverhältnismäßig großem Aufwand, möglich, so bleibe die Qualität der Einzelangabe als personenbezogenes Datum erhalten. Bei der Einordnung von Pseudonymen wird eine Differenzierung zwischen der Stelle, die über die Zuordnungsregel verfügt, und anderen Stellen abgelehnt.[788] Nach der Gegenauffassung

---

223, wonach das objektive Vorhandensein einer Aufdeckungsregel bei einer Stelle die Daten auch für jede andere Stelle personenbeziehbar werden lassen soll; s. dazu im Folgenden.

782 Vgl. §§ 5 Abs. 2 und 3, 7 Abs. 1 Nr. 1 SigG; zum Einsatz von Pseudonymen im Signaturverfahren Roßnagel-*Roßnagel*, Kap. 7.7, Rn. 61 m.w.N.

783 Zum Einsatz anonymer und pseudonymer Verfahren im zukünftigen Gesundheitswesen s. *ATG/GVG* 2004a, insbes. 24 ff., 48 ff.; s.a. unten 6.3.2.

784 *Gola/Schomerus*, § 3 Rn. 44; Roßnagel-*Tinnefeld*, Kap. 4.1, Rn. 23.

785 Roßnagel-*Roßnagel*, Kap. 3.4, Rn. 57.

786 Dabei lässt sich nach unterschiedlichen Verfahren, Arten von Pseudonymen und pseudonymisierenden Instanzen unterscheiden, s. näher *AKT*, DuD 1997, 709, 711 f.; Simitis-*Bizer*, § 3 Rn. 225 ff.; Roßnagel-*Hansen*, Kap. 3.3, Rn. 52 ff.; *Roßnagel/Pfitzmann/Garstka* 2001, 104 ff.; *Roßnagel/Scholz*, MMR 2000, 721, 724 f.; *Scholz* 2003, 190 ff. m.w.N.

787 *Auernhammer*, § 3 Rn. 47; Simitis-*Dammann*, § 3 Rn. 202 f. (wonach allerdings einzelne Vorschriften des BDSG im vergleichbaren Fall des Verschlüsselns „der spezifischen Situation angepasst werden" sollen, s. ebd., Rn. 34. Damit wird freilich inzident die Unanwendbarkeit des BDSG anerkannt); *Albrecht* 2003a, 154; s.a. die Nachweise bei *Scholz* 2003, 193 ff.

788 Simitis-*Bizer*, § 3 Rn. 223; RMD-*ders.*, § 3 TDDSG a.F. Rn. 176 (Stand Januar 2000).

entfällt im Fall der Anonymisierung jeder Personenbezug.[789] Für Pseudonyme sei eine Differenzierung danach geboten, ob die verarbeitende Stelle über die Zuordnungsregel verfüge. Sei das der Fall, so liege ein personenbezogenes Datum vor, andernfalls bestehe kein Unterschied zur Verwendung anonymer Daten.[790]

Begrifflich schließen sich personenbeziehbare und anonyme Daten zwar nicht ausdrücklich nach dem Gesetzeswortlaut, wohl aber materiell gegenseitig aus. Die – auch von Vertretern der ersten Auffassung – zur Frage der noch-personenbeziehbaren Daten entwickelten Definitionen (etwa mittels Zusatzwissen, dessen „Bekanntwerden nach sozialüblichen Maßstäben nicht ausgeschlossen werden kann“[791]) decken sich inhaltlich mit der Grenze, die § 3 Abs. 6, 2. Alt. BDSG für die Verhältnismäßigkeit des Aufwands einer Re-Identifizierung aufstellt. Sobald dieser unverhältnismäßig ist und die Daten damit anonym im Sinne der Legaldefinition sind, ist ein Bekanntwerden des Betroffenen nach sozialüblichen Maßstäben ausgeschlossen, und eine Anwendbarkeit des Bundesdatenschutzgesetzes scheidet aus.[792] Ist die Unverhältnismäßigkeitsgrenze nicht erreicht, so erfüllt auch eine Entfernung des Personenbezugs nicht die Definition des § 3 Abs. 6 BDSG,[793] und das Gesetz bleibt anwendbar. Bei Chipkarten ist zu beachten, dass diese häufig zum Umgang mit sensiblen Daten eingesetzt werden.[794] Hier kann die zuständige Stelle mitunter ein erhebliches Interesse an einer Re-Identifizierung haben. In diesem Fall steigt die Grenze der Verhältnismäßigkeit des Aufwands, weil dann auch mit dem Einsatz von zeit-, kosten- und arbeitsintensiven Mitteln zu rechnen ist. Dies kann die Anonymität der Daten einschränken oder aufheben.

Akzeptiert man schließlich die Relativität des Personenbezugs, so müssen pseudonyme Daten immer dann vom Anwendungsbereich des Bundesdatenschutzgesetzes ausgenommen werden, wenn der jeweiligen Stelle das Zusatzwissen fehlt, um die hinter dem Pseudonym stehende Person zu bestimmen. Ein solches Zusatzwissen liegt nicht nur dann vor, wenn die zur Pseudonymisierung verwendete Zuordnungsregel bekannt ist, sondern auch dann, wenn aus den gesammelten Daten (beispielsweise durch Verkettung der Daten, die bei verschiedenen Erhebungsvorgängen für dasselbe Pseudonym entstehen)[795] oder aus anderen Informationen auf den Betroffenen geschlossen werden kann. Bei Chipkarten besteht ein spezifisches Problem darin, dass Daten, die mit ihrer Hilfe unter Pseudonymen in Peripheriesystemen gespeichert werden, für den Fall des Verlusts der Karte auch alter-

789 *Gola/Schomerus*, § 3 Rn. 43 f.; *Roßnagel/Scholz*, MMR 2000, 721, 725 ff.; *Roßnagel/Pfitzmann/Garstka* 2001, 103; Roßnagel-*Roßnagel*, Kap. 3.4, Rn. 57; *Scholz* 2003, 193 ff.; *Dierks/Nitz/Grau* 2003, 44, 77; *Berg*, MedR 2004, 411, 412; *Yildirim* 2004, 154 ff.; der Sache nach auch Roßnagel-*Tinnefeld*, Kap. 4.1, Rn. 23 f.

790 *Gola/Schomerus*, § 3a Rn. 10; *Gundermann*, K&R 2000, 225, 232; *Roßnagel/Scholz*, MMR 2000, 721, 725; *Roßnagel/Pfitzmann/Garstka* 2001, 103; Roßnagel-*Roßnagel*, Kap. 3.4, Rn. 60.; *Scholz* 2003, 193 ff.; *Schaffland/Wiltfang*, § 3 Rn. 13; s.a. Begründung des *ULD* zu § 22 Abs. 2 DSG SH, LT-Drs. 14/1738, 67 f.

791 Simitis-*Dammann*, § 3 Rn. 36.

792 Auch *Gola/Schomerus*, § 3 Rn. 10 und *Tinnefeld/Ehmann* 1998, 187 f. betonen den Zusammenhang zwischen der Verhältnismäßigkeit der Re-Individualisierung und dem Vorliegen eines Personenbezugs. Ein ähnliches Konzept verfolgt Erwägungsgrund 26 der DSRL, wonach alle Mittel berücksichtigt werden sollten, „die vernünftigerweise entweder von dem Verantwortlichen für die Verarbeitung oder von einem Dritten eingesetzt werden könnten, um die betreffende Person zu bestimmen“.

793 Ein solches Vorgehen, das den Personenbezug entfernt, jedoch wieder rückgängig gemacht werden kann (also die Personenbeziehbarkeit nicht beseitigt), sollte – trotz vergleichbarer Verfahrensweise – dementsprechend auch nicht als „Anonymisieren“ bezeichnet werden.

794 Etwa im Gesundheitswesen und im Gefahrenabwehrbereich; zum Problem der „besonderen Arten personenbezogener Daten“ i.S.v. § 3 Abs. 9 BDSG s.u. 4.3.4.

795 Dazu *Roßnagel/Scholz*, MMR 2000, 721, 728 f.

nativ zugänglich sein müssen. Das betrifft etwa die elektronische Krankenakte. Es wäre nicht akzeptabel, wenn diese Daten dauerhaft verloren gingen. Hier gibt es zwei grundsätzliche Möglichkeiten: Entweder es erfolgt eine Speicherung von Duplikaten, zum Beispiel beim behandelnden Arzt.[796] In diesem Fall bleiben die auf Servern gespeicherten Daten für die speichernde Stelle pseudonym und das Bundesdatenschutzgesetz nicht anwendbar. Oder aber es wird eine Aufdeckungsmöglichkeit außerhalb der Chipkarte eingerichtet.[797] Erfolgt dies bei der speichernden Stelle selbst, so werden die Daten personenbezogen. Dies zieht die Anwendbarkeit des Datenschutzrechts nach sich. Das gilt auch bei einer organisatorischen Trennung zwischen Daten und Zuordnungssystem innerhalb der Stelle. Wird die Zuordnungsregel jedoch bei einem vertrauenswürdigen Dritten gespeichert, so bleibt es für die Speicherstelle beim fehlenden Personenbezug.

Wenn Daten, die zu einer Person gehören, mittels der Chipkarte in der Peripherie unter demselben Pseudonym gespeichert werden, so steigt das Risiko einer Aufdeckung, weil möglicherweise aus der Verkettung unterschiedlicher Verarbeitungs- und Nutzungsvorgänge (zum Beispiel regelmäßiger Behandlungs- und Abrechnungsvorgänge im Gesundheitswesen) mit hinreichender Wahrscheinlichkeit auf den Betroffenen geschlossen werden kann. Gleiches gilt wie bei anonymen Daten dann, wenn aufgrund des Charakters der Daten ein besonderes Interesse an der Aufdeckung unterstellt werden muss. Beides kann dazu führen, dass ein Personenbezug besteht und das Datenschutzrecht anwendbar bleibt.

Da bei sicher verschlüsselten Daten nur eine oder eine kleine Zahl von Stellen in der Lage ist, diese zu entschlüsseln, sind sie im Grundsatz wie pseudonyme Daten zu behandeln. Auch hier wird vertreten, aufgrund der theoretischen Möglichkeit einer Entschlüsselung mittels großen Zeitaufwands und enormer Rechenkapazität müsse trotz Verschlüsselung von einem personenbezogenen Datum ausgegangen werden.[798] Dem kann jedoch aus den oben genannten Gründen nicht gefolgt werden.[799] Allerdings handelt es sich hier nicht um ein Problem des Personenbezugs, sondern um die Frage, ob überhaupt eine „Einzelangabe über persönliche oder sachliche Verhältnisse“ (§ 3 Abs. 1 BDSG) vorliegt. Wenn im Rahmen einer externen Archivierung ein Datum übermittelt und wieder abgerufen wird, das mit einem Verschlüsselungsverfahren gesichert ist, welches nur mit Rechnerkapazitäten kompromittiert werden könnte, die nach dem aktuellen Stand der Technik auch in Rechnerverbünden nicht erreicht werden können, so kann nicht davon gesprochen werden, dass dieses Datum für die speichernde Stelle eine derartige Einzelangabe enthält, weil der Datensatz für diese keinen inhaltlichen Sinn ergibt. Gleiches gilt, wenn ein Datum von einer verantwortlichen Stelle in verschlüsselter Form auf der Karte selbst zum Transport oder späteren Abruf abgespeichert wird. Im Ergebnis ist damit nicht nur der Begriff der Bestimmbarkeit, sondern auch der der Einzelangabe ein relativer.

Die Unanwendbarkeit des Datenschutzrechts auf anonyme, pseudonyme und sicher verschlüsselte Daten unter den genannten Bedingungen führt zu einer Reihe von Folgeproblemen, wenn die Daten zufällig, aufgrund technischen Fortschritts oder einer veränderten Beurteilung der Verhältnismäßigkeitskriterien re-personalisierbar werden oder dies nicht

---

796 Dieser wird ohnehin weiterhin eine Speicherung vornehmen, s.u. 4.2.3.4.1.

797 Das ist regelmäßig erforderlich, wenn eine Vielzahl von Stellen beteiligt ist, weil dann die Rekonstruktion des gesamten Dateninhalts nur schwer möglich ist.

798 *Hermeler* 2000, 168 i.V.m. 152 ff.

799 Insoweit auch Simitis-*Dammann*, § 3 Rn. 34, der allerdings aus der Erkenntnis, dass die verschlüsselten Daten „für Personen, denen der Code unzugänglich ist, keine personenbezogenen, sondern anonyme Daten“ sind, nicht den verallgemeinernden Schluss einer grundsätzlichen Unanwendbarkeit des Datenschutzrechts auf anonyme Daten zieht.

ausgeschlossen werden kann.[800] Deshalb sind unter dem Gesichtspunkt der Gefahrenvorsorge für das Grundrecht auf informationelle Selbstbestimmung Maßnahmen zur Transparenz, zur Wahrung der Anonymitäts- und Pseudonymitätseigenschaft und zur technischen und organisatorischen Sicherheit zu treffen.[801]

4.1.2.2 Biometrische Daten

Zum Personenbezug biometrischer Daten werden stark unterschiedliche Ansichten vertreten, die jedoch überwiegend der Relativität des Begriffs und der Frage, wann die Herstellung eines solchen Bezugs nach sozialüblichen Erwartungen und Verhältnismäßigkeitskriterien zu erwarten ist, nicht gerecht werden.[802]

4.1.2.2.1 Bisherige Auffassungen zum Personenbezug

Vertreten wird zunächst die Auffassung, biometrische Daten seien stets personenbezogen, weil zumindest bei leistungsstarken Merkmalen und Verfahren ein biometrischer Datensatz nur zu einer einzigen Person gehöre.[803] Überwiegend wird demgegenüber zwischen biometrischen Volldatensätzen und Templates unterschieden,[804] jedoch mit unterschiedlichen Konsequenzen. So soll nach einer Auffassung bei Templates ein Personenbezug stets zu verneinen sein.[805] Nach anderer Ansicht besteht ein solcher nur dann, wenn zusätzliche Identifizierungsinformationen mit den Template-Daten verbunden werden.[806] Bei Volldaten sei hingegen nach der Art des Merkmals zu differenzieren. Handele es sich um Merkmale wie das Gesicht, „die im Allgemeinen offen liegen und für das menschliche Gehirn leicht zu verarbeiten sind", so könne kaum je ausgeschlossen werden, dass aus den Daten unmittelbar auf eine bestimmte Person zurückgeschlossen werden könne.[807] Bei Volldaten, die (wie der Fingerabdruck) an „weniger offen liegende Merkmale" anknüpften, sei dagegen zur Herstellung eines Personenbezugs wie bei Templates eine zusätzliche Adressierungs- oder Identifizierungsinformation erforderlich.[808] Die Unterscheidung hinsichtlich der Volldaten wird hier also ausdrücklich danach getroffen, ob es sich um Daten handelt, „die in gleicher Weise auch vom menschlichen Geist für die Wiedererkennung von Personen verwendet werden".[809] Kein Personenbezug liege schließlich bei templatefreien Verfahren vor.

Nach anderer Ansicht ist für biometrische Volldaten auf die erläuterte Differenzierung zu verzichten. Vielmehr könne die Herstellbarkeit eines Personenbezugs unter Berücksichtigung grundsätzlich verfügbaren Zusatzwissens, besonderer Fähigkeiten mathematisch-

800 *Roßnagel/Scholz*, MMR 2000, 721, 728 f.
801 Dieser Frage kann hier nicht im Einzelnen nachgegangen werden; s. näher *Roßnagel/Pfitzmann/Garstka* 2001, 108 ff.; *Roßnagel/Scholz*, MMR 2000, 721, 730 f.; *Scholz* 2003, 198 ff.
802 S. zum Folgenden bereits *Hornung*, DuD 2004, 429 ff.
803 *Weichert*, CR 1997, 369, 372; *TeleTrusT* 2002, 30, 34; in diese Richtung auch *Nanavati/Thieme/Nanavati* 2002, 243; *Art. 29 DPWP* 2003, 5; s.a. VG Wiesbaden, Urteil v. 11.11.1980 (zitiert nach *Albrecht* 2003a, 156); ebenso noch *Probst* 2002, 117 (s. aber Roßnagel-*Gundermann/Probst*, Kap. 9.6, Rn. 43 ff.).
804 S. zur Terminologie oben 2.3.3.2.
805 *Kruse/Peuckert*, DuD 1995, 142, 145; *Fuest* 1999, 192.
806 *Bäumler/Gundermann/Probst* 2001, 16; Roßnagel-*Gundermann/Probst*, Kap. 9.6, Rn. 48; s.a. *TAB* 2002, 44.
807 Roßnagel-*Gundermann/Probst*, Kap. 9.6, Rn. 43 ff.
808 *Bäumler/Gundermann/Probst* 2001, 15; Roßnagel-*Gundermann/Probst*, Kap. 9.6, Rn. 46 f.; *TAB* 2002, 44.
809 Roßnagel-*Gundermann/Probst*, Kap. 9.6, Rn. 47.

statistischer Experten und externer Datenverarbeitungskapazitäten grundsätzlich nie ausgeschlossen werden.[810] Biometrische Volldaten müssten demnach stets als einer bestimmten oder bestimmbaren Person zugeordnet verstanden werden. Bei Templates sei demgegenüber nach dem Speicherort zu differenzieren. Im Fall einer zentralen Speicherung seien die Daten personenbezogen, weil die einzelnen Betroffenen über die jeweilige Zuordnungsliste ermittelt werden könnten.[811] Fände dagegen lediglich eine dezentrale Ablage statt, beispielsweise auf Chipkarten, so seien die dort abgelegten Daten nur personenbezogen, wenn beim Prüfvorgang gleichzeitig eine Zuordnung zu einer Berechtigtenliste mittels einer zusätzlichen Kennzahl oder des Namens des Betroffenen erfolge.[812] Gleiches gelte für Systeme mit biometrischem Sensor auf der Karte, sofern die Daten auch im Verlustfall nicht ausgelesen werden könnten. Bei templatefreien Verfahren seien schließlich „keine personenbezogenen Daten mehr verfügbar".[813]

4.1.2.2.2 Analyse

Im Ergebnis kann keine der erläuterten Auffassungen überzeugen.[814] Zunächst kann ein Personenbezug von Templates nicht grundsätzlich verneint werden, weil auch diese (extrahierte) Informationen über eine natürliche Person enthalten. Außerdem können sie je nach Kontext, etwa über Zuordnungslisten, bestimmbaren Personen zugewiesen werden. Gegen die Annahme eines Personenbezugs ohne Differenzierung nach den jeweiligen Kontextbedingungen spricht demgegenüber, dass dabei spezifische Verfahren ignoriert werden. Zur Überprüfung einer Zugangsberechtigung kann es etwa ausreichen, die Templates aller Mitarbeiter eines Unternehmens ohne jede Kennung in einer Datenbank zu speichern und bei der Einlasskontrolle lediglich zu prüfen, ob die Daten des Betroffenen, der das Merkmal präsentiert, in der Datenbank enthalten sind. Im Moment des Abgleichs wird das jeweilige Template zwar personenbezogen, da die zugehörige Person (die am Sensor steht) bestimmbar ist. Zwischen den Matchingvorgängen besteht jedoch für die speichernde Stelle bei hinreichender Größe der Datenbank keine Möglichkeit der Herstellung eines Personenbezugs.[815]

4.1.2.2.2.1 Differenzierung nach Verfahrensschritten

Grundsätzlich konzentrieren sich die erläuterten Ansätze zu sehr auf die unterschiedlichen Verfahren, Merkmale, Speicherungsformen und -orte, anstatt von der Relativität des Personenbezugs auszugehen und im Einzelfall die Bestimmbarkeit des Betroffenen zu analysieren.[816] Hierzu ist es sinnvoll, nicht den Personenbezug biometrischer Daten „an sich" zu betrachten, sondern nach Verarbeitungsschritten und Speicherorten zu differenzie-

---

810 *Albrecht* 2003a, 157 f.; *dies*. 2002b, 100.
811 *Albrecht* 2003a, 159.
812 *Albrecht* 2003a, 160.
813 *Albrecht* 2003a, 161.
814 Vgl. bereits *Hornung*, DuD 2004, 429 ff.
815 S. *Gundermann/Köhntopp*, DuD 1999, 143, 147; diese Variante wird bei der Analyse zentraler Speicherungen übersehen von *Albrecht* 2003a, 159 (s. aber ebd., 57); zur technischen Realisierung z.B. *Donnerhacke*, DuD 1999, 151 ff.
816 Diese Analyse ist in jedem Fall notwendig, weil an den Personenbezug im konkreten Fall Rechte und Pflichten der Beteiligten geknüpft sind. Die Empfehlung von *Albrecht* (2003b, 17), biometrische Daten „obwohl dies nicht auf alle Anwendungen in allen Fällen zutreffen mag" stets als personenbezogen anzusehen, ist zur rechtlichen Absicherung der Betreiber möglicherweise aus pragmatischer Sicht sinnvoll. Bei der Rechtsanwendung muss die Frage jedoch entschieden werden.

ren. Im Ergebnis erweisen sich dabei einige der vorgeschlagenen Unterscheidungsgruppen als brauchbare Kriterien für die Bestimmbarkeit im Einzelfall, ohne jedoch abstrakte Kategorien zu bilden.

Bei vielen Verarbeitungsschritten biometrischer Identifikationsverfahren ist der Betroffene schon deshalb bestimmbar, weil er aus unterschiedlichen Gründen identifizierbar sein jeweiliges Merkmal präsentiert. Das gilt für das Enrolment ebenso wie für jeden weiteren Matchingvorgang, der unter der Kontrolle der verantwortlichen Stelle stattfindet.[817] Eine Ausnahme bilden lediglich Verfahren mit einem Sensor auf einer Chipkarte, weil hierbei die biometrischen Daten unter der ausschließlichen Verfügungsgewalt des Inhabers bleiben. Bei allen anderen Verfahren sind die zum Matching erhobenen Daten personenbeziehbar, dies allerdings nicht deswegen, weil es sich um Volldatensätze handelt, sondern weil der Betroffene anwesend und identifizierbar ist. Bei Chipkartenausweisen, die gleichzeitig als Sichtausweise fungieren, ist dies aufgrund des aufgedruckten Namens des Inhabers sogar besonders einfach. Die Existenz personenbezogener biometrischer Daten beim Matching ist – was in der Diskussion häufig untergeht – völlig unabhängig vom verwendeten Verfahren und der Art der Speicherung der Referenzdaten als Volldaten oder Templates, in zentraler, dezentraler oder templatefreier Form.

Beim Personenbezug der gespeicherten Referenzdaten ist demgegenüber zu differenzieren. In dem Moment, in dem ein Referenzdatensatz positiv dem neu erhobenen Vergleichsdatensatz zugeordnet wird, wird er immer dann personenbezogen, wenn jener personenbezogen ist. Wie soeben erläutert, ist dies häufig der Fall. Da allerdings mit dem Vergleichsdatensatz ohnehin Daten vorhanden sind, die zu einem sehr hohen Grad mit den Referenzdaten übereinstimmen, ist hiermit keine weitergehende Gefährdung für die informationelle Selbstbestimmung des Betroffenen verbunden.

Außerhalb von Matchingprozessen sind Daten innerhalb von Identifikationssystemen jedenfalls dann personenbezogen, wenn diese – wie häufig – über ein Zuordnungsverfahren, beispielsweise eine eindeutige Referenzliste, verfügen. In diesem Fall kommt es nicht auf die Frage an, ob die Referenzdaten auch ohne Zusatzinformationen einer Person zugeordnet werden könnten.

Nur bei Referenzdaten in Systemen ohne Zuordnungsverfahren und bei Daten, die außerhalb des bestimmungsgemäßen Ablaufs eines biometrischen Identifikationssystems verfügbar sind,[818] kommt es tatsächlich auf den Personenbezug biometrischer Daten „an sich“ an. Eine Zuordnung wird dann bei Volldaten regelmäßig leichter möglich sein, weswegen eine Differenzierung hier in der Tat sinnvoll ist. Dennoch kann den Auffassungen nicht gefolgt werden, wonach biometrische Volldaten stets[819] oder immer bei offen liegenden Merkmalen[820] Angaben über eine bestimmte oder bestimmbare Person enthalten. Vielmehr kommt es auch hier auf die Kontextbedingungen, also das verfügbare Zusatzwissen und die Verarbeitungsmöglichkeiten der verantwortlichen Stelle, an.

So gibt es durchaus Fälle, in denen Volldaten des „offen liegenden“ Gesichtes durch eine verantwortliche Stelle keiner Person zugeordnet werden können – etwa, wenn diese Stelle sich im Ausland befindet und keinerlei Informationen über die Identität oder den Herkunftsort des Betroffenen hat. Der Fingerabdruck einer bereits erkennungsdienstlich

817 Dies ist allerdings erforderlich. Werden etwa in automatischen Abfertigungssystemen Daten ohne Aufsicht präsentiert, so müssen weitere Umstände (Charakter der Daten, Referenzlisten, sonstiges Zusatzwissen, s. im Folgenden) hinzutreten, um einen Personenbezug herzustellen.

818 Hierzu kann es entweder durch eine Merkmalserhebung außerhalb eines solchen Systems oder durch die Weitergabe oder Entwendung von Referenzdaten kommen.

819 *Albrecht* 2003a, 157 f.

820 Roßnagel-*Gundermann/Probst*, Kap. 9.6, Rn. 43 ff.

behandelten Person ist in den Händen einer Polizeidienststelle ein personenbezogenes Datum. Weitere Adressierungs- oder Identifizierungsinformation sind nicht erforderlich, weil eine einfache Abfrage im AFIS[821] der Polizei zur Zuordnung durch die Dienststelle genügt. Dagegen ist es ohne dieses Zusatzwissen (das die Polizei im Regelfall nicht mit anderen Stellen teilt) normalerweise nicht möglich, den Fingerabdruck einer Person zuzuordnen. Das Wissen ist zwar objektiv bei Dritten vorhanden, jedoch der verantwortlichen Stelle nach sozialadäquaten Maßstäben nicht verfügbar. Dies kann sich für andere Stellen und bei entsprechendem technischem Fortschritt anders darstellen. Nichtsdestotrotz bleibt festzuhalten, dass auch biometrische Volldaten beim Fehlen jeglichen adäquaten Zusatzwissens nicht immer personenbezogen sind.[822]

Unter keinen Umständen kann es darauf ankommen, ob es sich um ein „für das menschliche Gehirn leicht zu verarbeitendes" oder „vom menschlichen Geist für die Wiedererkennung von Personen verwendetes" Merkmal handelt.[823] Bei der Beurteilung der Bestimmbarkeit des Betroffenen ist auf die konkreten Umstände, insbesondere die verfügbaren technischen Verarbeitungsverfahren und das der zuständigen Stelle verfügbare Zusatzwissen abzustellen.[824] Hinsichtlich technischer Mittel kommt es noch nicht einmal darauf an, ob die Stelle selbst in ihrem Besitz ist, sondern nur darauf, ob diese am Markt verfügbar sind. Obige Auffassung hätte zur Folge, dass die Anwendbarkeit des Datenschutzrechts von den Möglichkeiten einer manuellen Datenverarbeitung auf der Basis menschlich-visuell erfasster Daten abhinge. Das ist unter den Bedingungen moderner Informationsverarbeitung nicht vertretbar.

4.1.2.2.2.2 Besonderheiten bei Templates

Templates sind gesondert zu beurteilen, wenn hierunter ausschließlich Datenextrakte verstanden werden, die substantiell weniger Daten als Volldaten enthalten.[825] Außerdem muss es ausgeschlossen sein, aus den Templates die zugehörigen Volldaten zurückzurechnen. Die Unumkehrbarkeit des Extraktionsverfahrens wird in der bisherigen Literatur durchweg vorausgesetzt.[826] Zumindest bei einigen Merkmalen und einigen der verwende-

---

821 Das AFIS (Automatisches Fingerabdruck-Identifizierungssystem) ist eine beim BKA geführte Datenbank mit daktyloskopischen Angaben aus Straf- und Asylverfahren; näher *Weichert*, DuD 1999, 167.

822 Deshalb ist die Auffassung von *Albrecht* (2003, 158) abzulehnen. So richtig es ist, dass die Notwendigkeit der Verwendung technischer Hilfsmittel „gerade kein Ausschlusskriterium für die Annahme des Personenbezugs sein" kann, so wenig kann *hieraus* gefolgert werden, dass biometrische Volldaten „demnach stets als Einzelangaben über persönliche Verhältnisse des Merkmalsträgers verstanden werden" müssen. Es gibt nämlich Fälle, in denen technische Hilfsmittel objektiv nicht am Markt verfügbar sind oder ihr Einsatz allein zur Bestimmung des Betroffenen nicht ausreicht, sondern auf Zusatzwissen zurückgegriffen werden muss. Dieses kann jedoch – wie gezeigt – ungleich verteilt sein und damit für bestimmte Stellen einen Personenbezug herstellen, für andere jedoch nicht. Die Ansicht von *Albrecht* ist allerdings konsequent, da dort im Unterschied zur hier vertretenen Auffassung auch anonyme und pseudonyme Daten trotz des unverhältnismäßigen Aufwands zur Re-Identifizierung als personenbezogen angesehen werden; s. dazu oben 4.1.2.1.

823 So aber Roßnagel-*Gundermann/Probst*, Kap. 9.6, Rn. 43, 45, 47; die Differenzierung ablehnend auch *Albrecht* 2003a, 157 f.; mit leicht anderem Akzent im Übrigen *Bäumler/Gundermann/Probst* 2001, 15, wonach es ausreichen soll, wenn „die fraglichen Daten...mit Hilfe von technischen Geräten in eine für den menschlichen Geist lesbare Form gebracht werden können".

824 S. dazu schon oben 4.1.2.1.

825 Bisweilen werden alle Referenzdaten (auch Volldaten) und nur leicht komprimierte Rohdaten als „Templates" bezeichnet; s. zur Terminologie oben 2.3.3.2.

826 *AKT*, DuD 1997, 709, 713; *Gundermann/Köhntopp*, DuD 1999, 143, 150; *Bäumler/Gundermann/Probst* 2001, 16; *Nanavati/Thieme/Nanavati* 2002, 243, 245; Roßnagel-*Gundermann/Probst*, Kap. 9.6, Rn. 48; *Albrecht* 2003a, 158.

ten Algorithmen erscheint jedoch eine Rückwärtskonstruktion möglich.[827] Können die Volldatensätze vollständig ermittelt werden, sind Templates und Volldaten datenschutzrechtlich gleich zu behandeln. Aber auch bei einem lediglich teilweisen Rückschluss auf den Volldatensatz ergibt sich eine (Teil-)Information, die je nach Kontext und weiterem Zusatzwissen der verantwortlichen Stelle ein personenbezogenes Datum entstehen lassen kann. Der benötigte Rechenaufwand spielt solange keine Rolle, wie er realistischerweise am Markt verfügbar ist.

Nur wenn beim verwendeten Merkmal und Verfahren eine Rückwärtskonstruktion ausgeschlossen ist, kann aus dem Template selbst nicht auf den Betroffenen geschlossen werden. In diesem Fall sind die Daten nur bei Vorliegen eines Zuordnungssystems personenbezogen.

4.1.2.2.2.3 Speicherung und Verarbeitung auf Chipkartenausweisen

Im vorliegenden Zusammenhang ist insbesondere der Personenbezug biometrischer Referenzdaten von Interesse, die auf Chipkarten gespeichert werden. Hierbei ist nach den unterschiedlichen Verfahren beim Matching zu unterscheiden.[828]

Werden die Referenzdaten (in Form von Volldaten oder Templates) zum Matching aus der Karte ausgelesen, und fungiert diese damit lediglich als Speicher- und Transportmedium, so sind die Daten für jede Stelle, die sie aus dem Chip ausliest, personenbezogen. Hierzu ist keine zusätzliche Zuordnung zu einer Berechtigtenliste mittels Kennzahl oder Namens erforderlich, weil der Betroffene persönlich anwesend (und damit identifizierbar) ist und seine weiteren Daten auf dem Ausweis sichtbar aufgedruckt sind.[829] Zwischen den einzelnen Auslesevorgängen hat die verantwortliche Stelle zwar keine Verfügungsgewalt über die Daten. Daraus kann jedoch nicht gefolgert werden, dass in diesen Zeiträumen keine personenbezogenen Daten vorliegen. Die verantwortliche Stelle hat die Speicherung auf der Chipkarte vorgenommen und die entstehenden Zwischenräume sind lediglich notwendige Folge dieser spezifischen Art der Speicherung, die bei jedem Kontakt der verantwortlichen Stelle den Zugriff auf die Daten ermöglicht. Die biometrischen Daten bleiben also personenbezogen. Dies ist insbesondere für die Sicherungsmaßnahmen von Bedeutung, die die verantwortliche Stelle gerade für die Zeiträume zu treffen hat, in denen der Berechtigte den Ausweis bei sich führt.[830]

Findet Matching-On-Card statt, so sendet der Sensor die Vergleichsdaten an die Karte, die den Abgleich vornimmt. Damit verlassen die Referenzdaten den Ausweis nicht. Dies lässt jedoch den Personenbezug der Daten nicht entfallen. Die Referenzdaten sind vielmehr objektiv auf der Karte vorhanden und untrennbar mit dieser – und damit mit den Identifizierungsdaten auf der Oberfläche – verbunden. Wird die Karte zur Verifikation präsentiert,[831] und verläuft diese positiv, so ist auch eine Bestimmung des Dateninhalts möglich, weil dieser zu einem sehr hohen Grad mit den an die Karte gesendeten Referenzdaten übereinstimmt.

---

827 S. hierzu ausführlich unten 4.2.2.4.2.

828 S. insoweit oben 2.3.3.2.

829 Dabei wird vorausgesetzt, dass sowohl die Kartenoberfläche als auch die gespeicherten biometrischen Identifikationsdaten gegen Manipulationen geschützt sind. Der genannte Kontext wird übersehen von *Albrecht* 2003a, 160, die lediglich auf die biometrischen Daten abstellt und vernachlässigt, dass eine Zuordnung über die aufgedruckten Daten möglich ist. Die von *Albrecht* a.a.O. als Beleg angeführten *Gundermann/Köhntopp*, DuD 1999, 143, 147 beziehen sich dort im Übrigen gerade nicht auf eine Speicherung auf Chipkarten, sondern in zentralen Systemen.

830 S. dazu unten 4.3.8, 6.2.1 und 6.3.1.

831 Beim Matching-On-Card ist nur eine Verifikation, keine Identifikation möglich.

Verfügt der Ausweis dagegen über einen Sensor, und findet die Merkmalsextraktion und das Matching auf der Karte statt,[832] so läuft das gesamte Verfahren unter der Verfügungsgewalt des Ausweisinhabers ab. Ist nach der Personalisierung des Chips ein externer Zugriff nicht mehr möglich, so hat die verantwortliche Stelle keinen Einfluss auf die Daten.[833] Anders als beim schlichten Matching-On-Card ist im Regelfall auch kein Schluss auf die gespeicherten Daten möglich. Zwar bleiben die Angaben dem Inhaber an sich zugeordnet, weil sie fest in der Karte gespeichert sind. Da jedoch niemand in der Lage ist, von ihrem Inhalt Kenntnis zu nehmen, fehlt es hier im Ergebnis an einem personenbezogenen Datum. Ähnlich wie bei anonymen und pseudonymen Daten besteht dann aber unter dem Aspekt der Risikovorsorge eine Pflicht zur Sicherung der Referenzdaten auf dem Chip gegen unbefugten Zugriff. Orientierungshilfe bietet insoweit der Pflichtenkatalog aus der Anlage zu § 9 BDSG.[834]

4.1.2.2.2.4 Vermeidung des Personenbezugs durch templatefreie Verfahren?

Mit Hilfe templatefreier Verfahren ist es möglich, mittels eines „biometrischen Schlüssels“ unterschiedliche Klartext-Chiffrat-Paare zu erzeugen, die in verschiedenen Anwendungen eingesetzt und dort auch ausgetauscht werden können.[835] Beim Einsatz sicherer Algorithmen ist es der Stelle, die das jeweilige Chiffrat speichert, nicht möglich, aus diesem auf den Klartext oder das biometrische Merkmal zurückzuschließen.

Aus zweierlei Gründen kann daraus jedoch nicht gefolgert werden, es seien „hier keine personenbezogenen Daten mehr verfügbar“,[836] entsprechende Verfahren realisierten „biometrische Anwendungen ohne Personenbezug“,[837] beziehungsweise es handele sich um „anonyme Biometrie“.[838] Zunächst ist bei jedem Authentifikationsvorgang nach wie vor die Erhebung der biometrischen Volldaten erforderlich, weil aus diesen der biometrische Schlüssel berechnet werden muss, mit dem wiederum der Klartext zum Vergleich mit dem Chiffrat verschlüsselt wird. Insofern entstehen wie bei jedem Matching unter Kontrolle der zuständigen Stelle – abgesehen von Verfahren mit Sensor auf der Chipkarte – personenbezogene Daten.

Darüber hinaus kann es sich bei dem zum Vergleich gespeicherten Chiffrat um ein personenbezogenes Datum handeln. Es enthält zumindest die Angabe, dass der Betroffene im System enroled wurde und beispielsweise zum Zugang zu einem gesicherten Bereich berechtigt ist. Beides stellt eine Einzelangabe über persönliche oder sachliche Verhältnisse dar. Zwar kann aus dem verformelten Inhalt des Chiffrats nicht direkt auf den Betroffenen geschlossen werden. Sobald jedoch eine Zuordnungsliste zwischen Chiffraten und den jeweiligen Betroffenen vorhanden ist, ist das Chiffrat personenbezogen. Im Ergebnis vermeiden templatefreie Verfahren damit die Speicherung personenbezogener biometrischer Referenzdaten, im Regelfall jedoch nicht die Verwendung jeglicher personenbezogener Daten.

---

832 Hier bestehen bislang noch erhebliche technische Probleme hinsichtlich der Rechenkapazität, die zur Extraktion eines Templates oder – falls darauf verzichtet wird – zum Matching von Volldaten erforderlich ist. Außerdem sind Sensoren nur für den Fingerabdruck möglich; s. *Janke* 2002, 207 und unten 4.2.2.4.4.

833 Sofern die Karten ausgebende Stelle (bspw. zu Kontrollzwecken) zusätzlich in der Lage ist, die Daten auszulesen, besteht wieder Personenbezug.

834 S. dazu näher unten 4.3.8.

835 Zur Funktionsweise vgl. oben 2.3.3.2.

836 *Albrecht* 2003a, 161.

837 Roßnagel-*Gundermann/Probst*, Kap. 9.6, Rn. 49.

838 *Donnerhacke*, DuD 1999, 151 ff.

4.1.2.2.3 Zusammenfassung

Im Ergebnis ist festzuhalten, dass bei einer Merkmalspräsentation in aller Regel personenbezogene biometrische Daten entstehen.[839] Das ist beim Enrolment nahezu stets,[840] beim Matching immer dann der Fall, wenn die Identität des Betroffenen durch die verantwortliche Stelle zumindest potentiell feststellbar ist. Da der Betroffene anwesend ist und seine Identifikationsdaten bei den hier untersuchten Chipkartenverfahren auf der Kartenoberfläche aufgedruckt sind, trifft dies durchweg zu. Dann werden bei einem positiven Matchingergebnis darüber hinaus auch die gespeicherten Referenzdaten personenbezogen. Ohne Matching sind Referenzdaten in zentralen Datensammlungen immer dann personenbezogen, wenn die Datenbank – wie regelmäßig – über ein Zuordnungssystem verfügt. Bei einer Speicherung auf personalisierten Chipkarten ist die Person des Inhabers unabhängig davon, ob das Matching auf der Karte oder in der Peripherie stattfindet, stets bestimmbar. Einzige Ausnahme sind mit Sensoren versehene Karten, bei denen jedes Auslesen der Referenzdaten ausgeschlossen ist.

Die Frage eines Personenbezugs der biometrischen Daten „an sich" stellt sich damit nur in Ausnahmefällen, nämlich dann, wenn Merkmale außerhalb eines bestimmungsgemäßen Matchingprozesses erhoben werden, Daten aus Referenzdatenbanken entwendet oder weitergegeben werden, sowie beim Verlust der Zuordnungsregel in der Datenbank. In diesen Fällen ist eine Analyse der am Markt verfügbaren technischen Systeme und des jeweiligen individuell verfügbaren Zusatzwissens der verantwortlichen Stelle erforderlich. Hierbei kann es Unterschiede zwischen einzelnen Merkmalsarten geben, weil einige der Merkmale leichter einer Person zugeordnet werden können. Eine Verallgemeinerung dahin, dass alle oder einige biometrische Daten stets personenbezogen wären, verbietet sich jedoch aufgrund der Relativität des Begriffs des Personenbezugs. Bei Templates kommt es entscheidend auf die Möglichkeit der Rückwärtskonstruktion an. Wenn diese technisch ausgeschlossen ist und keine weiteren Identifizierungsinformationen bestehen, sind Templates nicht personenbezogen. Ist eine Berechnung der Volldaten dagegen möglich, so kommt es wie bei diesen auf die jeweils verfügbaren Zusatzinformationen an. Templatefreie Verfahren vermeiden den Aufbau einer zentralen Datenbank mit personenbezogenen biometrischen Daten. Sie lassen das Problem der Erhebung derartiger Daten zum Matching jedoch unberührt und können außerdem mit der Chiffrat-Datenbank über eine Sammlung personenbezogener Daten verfügen.

4.2 Verfassungsrechtliche Zulässigkeit

Wenn und soweit im Zusammenhang mit Chipkartenausweisen personenbezogene Daten gegen den Willen des Betroffenen erhoben, verarbeitet oder genutzt werden, wird in das Grundrecht auf informationelle Selbstbestimmung eingegriffen.[841] Der Eingriff bedarf der Rechtfertigung und muss deshalb mehreren verfassungsrechtlichen Anforderungen genügen. Für den digitalen Personalausweis und die elektronische Gesundheitskarte beste-

839 S. hierzu, und zur Frage des Personenbezugs insgesamt, bereits *Hornung*, DuD 2004, 429 ff.

840 Eine Ausnahme besteht z.B., wenn das Verfahren nicht der Wiedererkennung, sondern der Verhinderung von Doppelanträgen dient. Soll etwa eine Hilfsleistung in einem Katastrophengebiet nur einmal gewährt werden, so reicht es aus, alle Empfänger anonym in eine Datenbank aufzunehmen und bei der Ausgabe zu kontrollieren, ob der Antragsteller bereits in dieser enthalten ist.

841 Jede Datenverwendung gegen den Willen des Betroffenen ist ein solcher Eingriff, s. BVerfGE 100, 313 (366); Roßnagel-*Trute*, Kap. 2.5, Rn. 10 ff.; AK GG-*Podlech*, Art. 2 Abs. 1 Rn. 79.

hen bereits rechtliche Regelungen, die anhand dieses Maßstabs daraufhin zu überprüfen sind, ob sie rechtmäßig und hinreichend sind.

4.2.1 Verfassungsrechtliche Anforderungen

4.2.1.1 Gesetzesvorbehalt und Bestimmtheitsgrundsatz

Staatliches Handeln darf nur dann in Grundrechte eingreifen, wenn dem Grundsatz des Gesetzesvorbehalts entsprochen wird.[842] Dieser findet sich als Anforderung auch in internationalen Rechtsgrundlagen zum Datenschutz, so in Art. 17 IPbpR,[843] Art. 8 Abs. 2 EMRK[844] und Art. 8 Abs. 2 Satz 1 der Charta der Grundrechte der Europäischen Union.[845]

Um dem Gesetzesvorbehalts zu genügen, sind im Rahmen des deutschen Verfassungsrechts grundsätzlich auch Gesetze im nur materiellen Sinn ausreichend.[846] Im Schutzbereich des allgemeinen Persönlichkeitsrechts ist wegen der besonderen Bedeutung dieses Grundrechts in Abweichung hiervon jedoch durchweg ein formelles Gesetz erforderlich.[847] An die Ermächtigungsgrundlage sind außerdem hohe Anforderungen zu stellen.[848]

Das formelle Gesetz muss nicht sämtliche Umstände und Modalitäten der Datenverwendung selbst regeln. Es ist vielmehr zulässig, einzelne (mehr administrative) Aspekte der Verwaltung zu überlassen. Dies kann durch eine Ermächtigung zur Rechtssetzung mittels Rechtsverordnung oder zum faktischen Handeln geschehen. Eine derartige Delegation auf die Verwaltung darf jedoch nicht unbeschränkt erfolgen. Nach der vom Bundesverfassungsgericht entwickelten Wesentlichkeitslehre muss der Gesetzgeber vielmehr „in grundlegenden normativen Bereichen, zumal im Bereich der Grundrechtsausübung, soweit diese staatlicher Regelung zugänglich ist, alle wesentlichen Entscheidungen selbst...treffen“.[849] Diese Funktion steht nur dem parlamentarischen Gesetzgeber selbst zu; der Gesetzesvorbehalt „erstarkt“ damit zum Parlamentsvorbehalt.[850] Damit soll einem zu großen Eigenleben der Verwaltung vorgebeugt und Rechtsklarheit für den Bürger geschaffen werden.[851] Unter den Bedingungen der modernen Informationstechnologie kommt dem Wesentlichkeitsgrundsatz eine demokratischen Einfluss sichernde Funktion zu: Aufgrund

---

842 Das ist bei belastenden Eingriffen in individuelle Rechtspositionen unumstritten. Über die normative Herleitung des Grundsatzes und seine Geltung im Bereichs der Leistungsverwaltung besteht dagegen Streit, vgl. v. Münch/Kunig-*Schnapp*, Art. 20 Rn. 53 ff.; ausführlich *Ossenbühl*, HdbStR III (1996), § 62 Rn. 7 ff.

843 Aus diesem lässt sich eine Pflicht ableiten, Datenerhebungen gesetzlich zu regeln, s. *Seidel* 1996, S. 40 ff.; Meyer-*Bernsdorff*, Art. 8 Rn. 4.

844 Nach der Rspr. des EGMR ist eine deutliche und genaue gesetzliche Grundlage erforderlich, s. Amann ./. Schweiz, Urteil v. 16.2.2000 (abrufbar unter http://www.echr.coe.int/Eng/Judgments.htm), Abs. 50, 55 ff.; vgl. zu den Anforderungen der EMRK an die Bestimmtheit der Rechtsgrundlage *Matz* 2003, 125 f.; *Grabenwarter* 2003, 221.

845 Dazu Meyer-*Bernsdorff*, Art. 8 Rn. 21.

846 Einzelheiten sind umstritten, vgl. Sachs-*Sachs*, vor Art. 1 Rn. 107 m.w.N.

847 *Schmitt Glaeser*, HdbStR VI (2001), § 129 Rn. 103; v. Mangoldt/Klein/Starck-*Starck*, Art. 2 Rn. 21; *Schlink*, Der Staat 1986, 233, 236; v. Münch/Kunig-*Kunig*, Art. 2 Rn. 42; Dreier-*Dreier*, Art. 2 Rn. 86 m.w.N.; speziell zum Parlamentsvorbehalt beim Einsatz von Biometrie *Weichert*, CR 1997, 369, 374.

848 M/D-*Di Fabio*, Art. 2 Abs. 1 Rn. 181.

849 BVerfGE 49, 89 (126); 61, 260 (275); 88, 103 (116); s. v. Münch/Kunig-*Schnapp*, Art. 20 Rn. 56 f. m.w.N.; Sachs-*Sachs*, Art. 20 Rn. 116 f. m.w.N.

850 *Pieroth/Schlink* 2003, Rn. 264; ausführlich *Krebs*, Jura 1979, 304 ff.; *Pietzker*, JuS 1979, 710, 711 ff.; s.a. *Ossenbühl*, HdbStR III (1996), § 62 Rn. 32 ff.

851 *Pieroth/Schlink* 2003, Rn. 261.

der langfristigen Folgewirkungen von Entscheidungen über technische Alternativen müssen diese durch die Legislative gefällt werden.[852]

Was in dem genannten Sinne „wesentlich" ist, richtet sich einerseits danach, ob die staatliche Maßnahme „Grundrechtsrelevanz" aufweist,[853] andererseits nach der Intensität des Eingriffs.[854] Im Rahmen des allgemeinen Persönlichkeitsrechts muss dessen Bedeutung Rechnung getragen werden.[855] Dies bedeutet insbesondere, dass die Voraussetzungen für die Datenerhebung, die jeweiligen Verwendungszwecke,[856] die Modalitäten der Speicherung und die Zugriffsberechtigungen ausdrücklich und genau in einer formellen gesetzlichen Grundlage zu regeln sind. Das deckt sich auch mit den Anforderungen der Europäischen Menschenrechtskonvention. Der Europäische Gerichtshof für Menschenrechte hat entschieden, dass die gesetzlichen Bestimmungen umso klarer und detaillierter sein müssen, je schwerer der Eingriff in die Privatsphäre ist.[857]

Eng mit der Wesentlichkeitslehre verwandt ist der Bestimmtheitsgrundsatz.[858] Das Bundesverfassungsgericht hat im Volkszählungsurteil eindeutige Anforderungen an das „rechtsstaatliche Gebot der Normenklarheit" aufgestellt.[859] Danach müssen die Voraussetzungen und der Umfang der Beschränkungen klar und für den Bürger erkennbar sein, sodass dieser sein Verhalten danach ausrichten kann.

Für biometrische Systeme ist insbesondere fraglich, ob allgemeine, generalklauselartige Ermächtigungsgrundlagen (etwa „zur Durchführung" eines Gesetzes) für die Erhebung, Verarbeitung und Nutzung gerade biometrischer Daten ausreichend sind. Teilweise wird dies abgelehnt, weil die Verwendung körperlicher Merkmale als Informationsquelle in staatlichen biometrischen Systemen nicht nur in das informationelle Selbstbestimmungsrecht, sondern darüber hinaus in einen weiteren, bislang noch nicht klar definierten Bereich des allgemeinen Persönlichkeitsrechts eingreife.[860] Daraus folge, dass die allgemeinen Ermächtigungsgrundlagen zur Erhebung von Daten nicht zu einer Erhebung gerade biometrischer Daten ausreichten. Der über das informationelle Selbstbestimmungsrecht hinausgehende Eingriff erfordere vielmehr eine selbständige, ausdrückliche Entscheidung des Gesetzgebers.

Stichhaltigkeit wie Notwendigkeit dieser Konstruktion sind allerdings fraglich. Richtig ist zwar, dass es bei der Erhebung biometrischer Daten zu einer Verwendung des menschlichen Körpers kommt und hierin ein substantieller Unterschied zu anderen Formen der Datenerhebung (wie beispielsweise einer Befragung) liegt. Das ändert aber nichts daran, dass Zweck der Verwendung des Körpers die Gewinnung von Daten ist. Es handelt sich also um eine spezielle Form der Datenerhebung. Deshalb ist auch der angeführte Vergleich

852 *Roßnagel/Wedde/Hammer/Pordesch* 1990, 9.

853 BVerfGE 47, 46 (79 f.); 57, 295 (321); *Hesse* 1995, Rn. 509 m.w.N.; kritisch *Ossenbühl*, HdbStR III (1996), § 62 Rn. 44 ff.

854 *Pieroth/Schlink* 2003, Rn. 266.

855 BVerfGE 65, 1 (46); v. Münch/Kunig-*Kunig*, Art. 2 Rn. 42.

856 Diese sind im Gesetz selbst zu fixieren, s. BVerfGE 65, 1 (46); LVerfG MV, DVBl. 2000, 262, 266 f.; M/D-*Di Fabio*, Art. 2 Abs. 1 Rn. 182 m.w.N.

857 Kruslin ./. Frankreich, Urteil v. 24.4.1990 (abrufbar unter http://www.echr.coe.int/Eng/Judgments.htm), Abs. 33.

858 *Ossenbühl*, HdbStR III (1996), § 62 Rn. 23; dieser fußt gleichzeitig in den Grundrechten, dem Demokratieprinzip und dem Rechtsstaatsgebot des Art. 20 Abs. 3 GG, s. *Papier/Möller*, AöR 1997, 177, 178 ff.; v. Münch/Kunig-*Schnapp*, Art. 20 Rn. 25, 29.

859 BVerfGE 65, 1 (2. Leitsatz) und 44; zur Bestimmtheit von Gesetzen im datenschutzrechtlichen Kontext vgl. auch BayVerfGH, CR 1998, 396, 397; *Scholz* 2003, 138 ff.

860 Roßnagel-*Gundermann/Probst*, Kap. 9.6, Rn. 64 ff.; *Bäumler/Gundermann/Probst* 2001, 28 f.; s.a. *TAB* 2002, 46.

mit einer staatlichen Einwirkung auf Haar- und Barttracht bei Bundeswehrsoldaten[861] nicht zutreffend, weil es dort nicht um eine Datenerhebung, sondern um Fragen der Hygiene oder der Funktionsfähigkeit der Streitkräfte geht.[862] Daneben sprechen Gründe der dogmatischen Klarheit dafür, auch die Verfahrensaspekte der Datenerhebung in das Grundrecht auf informationelle Selbstbestimmung einzubeziehen. Die Konstruktion eines wenig greifbaren „zusätzlichen" Bereichs des allgemeinen Persönlichkeitsrechts erscheint vor allem deshalb schwierig, weil es sich dabei um dasselbe Grundrecht handelt, dennoch aber andere Anforderungen gelten und zusätzliche Ermächtigungsgrundlagen erforderlich sein sollen.

Dogmatisch überzeugender ist es demgegenüber, in der spezifischen Natur der biometrischen Daten und der spezifischen Art der Datenerhebung einen besonders intensiven Eingriff in das Recht auf informationelle Selbstbestimmung zu sehen, der so wesentlich ist, dass der parlamentarische Gesetzgeber eine eigene Entscheidung hierüber treffen muss. Im Ergebnis ist der oben genannten Auffassung darin zuzustimmen, dass die allgemeinen Ermächtigungsgrundlagen, die sich teilweise darin erschöpfen, eine Datenerhebung, -verarbeitung und -nutzung für die Zwecke des jeweiligen Gesetzes generell für zulässig zu erklären, für eine Erhebung, Verarbeitung und Nutzung biometrischer Daten nicht ausreichend sind. Die hier vorgeschlagene Lösung hat aber den Vorteil, dass sie auf die Konstruktion eines wenig fassbaren zusätzlichen Grundrechts verzichtet und auf das ausgearbeitete Konzept der Wesentlichkeitslehre zurückgreifen kann.

4.2.1.2 Anforderungen des Grundrechts auf informationelle Selbstbestimmung

Informationelle Selbstbestimmung ist „die aus dem Gedanken der Selbstbestimmung folgende Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen".[863] Aus dieser Befugnis haben Rechtsprechung und Literatur eine Reihe von Anforderungen an die Verwendung von Daten abgeleitet. Einige von ihnen wurzeln zusätzlich in anderen verfassungsrechtlichen Anforderungen (insbesondere dem Verhältnismäßigkeitsprinzip), haben sich jedoch mittlerweile terminologisch und inhaltlich verselbständigt.

4.2.1.2.1 Verhältnismäßigkeit

Das Verhältnismäßigkeitsprinzip ist ein fundamentaler Grundsatz für die Beurteilung der Rechtmäßigkeit allen staatlichen Handelns, der als „principle of proportionality" auch in der Europäischen Menschenrechtskonvention verankert ist.[864] Art. 8 Abs. 2 EMRK lässt nur solche Einschränkungen des Rechts auf Privatleben (das auch vor staatlicher Datenverarbeitung schützt) zu, die „erforderlich" sind. Der Verhältnismäßigkeitsgrundsatz findet sich auch in Art. 6 Abs. 1 lit. c DSRL[865] und in Art. 52 Abs. 1 der Charta der Grundrechte der Europäischen Union.[866] Er ist überdies ein allgemeiner Grundsatz des Europarechts.[867]

---

861 Roßnagel-*Gundermann/Probst*, Kap. 9.6, Rn. 64; *Bäumler/Gundermann/Probst* 2001, 28.

862 So jedenfalls die Begründungen der Rspr., vgl. BVerwGE 46, 1 (2 f.); 76, 60 (62); ebenso Sachs-*Murswiek*, Art. 2 Rn. 132.

863 BVerfGE 65, 1 (42); s. zur Herleitung oben 4.1.1.2.

864 Vgl. *Cremona* 1995, 323 ff.; *Eissen* 1993, 125 ff.; *Reed/Murdoch* 2001, 146 ff.; *v. Dijk/v. Hoof* 1998, 537 ff.; *Grabenwarter* 2003, 131 ff.

865 Simitis-*Bizer*, § 3a Rn. 32; Roßnagel-*Brühann*, Kap. 2.4, Rn. 30; *Schild*, EuZW 1996, 549, 551.

866 Näher Meyer-*Borowsky*, Art. 52 Rn. 18 ff.

867 S. *Craig/De Búrca* 2002, 371 ff.; *Usher* 1998, 37 ff.

Im deutschen Verfassungsrecht wird der Grundsatz der Verhältnismäßigkeit überwiegend auf das Rechtsstaatsprinzip,[868] teilweise zusätzlich auf die Grundrechte[869] gestützt. Obwohl er keine ausdrückliche Erwähnung im Grundgesetz findet, ist er in der Judikatur des Bundesverfassungsgerichts und der wissenschaftlichen Literatur allgemein anerkannt.[870] Im Einzelnen verlangt Verhältnismäßigkeit die Verfolgung eines rechtmäßigen Zwecks, den Einsatz eines rechtmäßigen Mittels, sowie die Eignung, Erforderlichkeit und objektive Zumutbarkeit des Mittels zur Zweckerreichung.[871] Konkret bedeutet Eignung, dass das eingesetzte Mittel den Zweck (nach bewährten Hypothesen) befördern muss;[872] erforderlich ist ein Mittel, wenn der Zweck nicht durch ein gleich wirksames, aber weniger belastendes Vorgehen erreichbar ist.[873] Das Kriterium der objektiven Zumutbarkeit ist nur dann erfüllt, wenn die negativen Auswirkungen des Mittels auf den Betroffenen nicht außer Verhältnis zum angestrebten Nutzen stehen.[874]

Alle dieser Prüfungspunkte können für die Rechtmäßigkeit einer Datenerhebung, -verarbeitung und -nutzung relevant werden.[875] Die Datenverwendung muss dazu geeignet sein, ein legitimes staatliches Ziel zu erreichen. Bei der Erforderlichkeitsprüfung ist stets zu fragen, ob auf ein konkretes Datum, einen konkreten Datenzugriff oder eine eingriffsintensive Datenvorhaltung nicht verzichtet werden kann, ohne dass die Zweckerreichung gefährdet wird. Im Rahmen der Beurteilung der objektiven Zumutbarkeit muss entschieden werden, ob die entstehenden Gefahren für das Grundrecht auf informationelle Selbstbestimmung außer Verhältnis zum angestrebten Zweck der Datenverwendung stehen.

Gegenüber dem allgemeinen Schutzbereich des Art. 2 Abs. 1 GG ist dieses Grundrecht – oder allgemeiner, das allgemeine Persönlichkeitsrecht – mit dem Bezug auf die Menschenwürde des Art. 1 Abs. 1 GG deutlich stärker geschützt.[876] Deshalb sind an die Verhältnismäßigkeit strengere materielle Anforderungen zu stellen als bei einem „normalen" Eingriff in Art. 2 Abs. 1 GG, die umso höher sind, je stärker die Komponente der Menschenwürde im konkreten Fall ist.[877] Zur Bejahung der Verhältnismäßigkeit ist damit erforderlich, dass die verantwortliche Stelle ohne die Datenverwendung nicht, nicht rechtzeitig, nicht vollständig oder nur mit unverhältnismäßigem Aufwand in der Lage wäre, ihre Aufgabe ordnungsgemäß zu erfüllen.[878]

---

868 BVerfGE 23, 127 (133); *Stern* 1994, 771 ff.; Sachs-*Sachs*, Art. 20 Rn. 146 m.w.N.

869 BVerfGE 90, 145 (173); v. Münch/Kunig-*Schnapp*, Art. 20 Rn. 32; *Pieroth/Schlink* 2003, Rn. 273.

870 *Stern* 1994, 762 m.w.N.; st. Rspr. seit BVerfGE 7, 377 (405, 407 f.).

871 V. Münch/Kunig-*v. Münch*, vor Art. 1-19 Rn. 55; Sachs-*Sachs*, Art. 20 Rn. 149 ff.; *Stern* 1994, 775 ff. (jeweils m.w.N.). Die Terminologie ist tlw. uneinheitlich, statt von objektiver Zumutbarkeit wird auch von Verhältnismäßigkeit im engeren Sinne, Proportionalität oder Angemessenheit gesprochen.

872 BVerfGE 30, 292 (316); 67, 157 (173); *Pieroth/Schlink* 2003, Rn. 283 f. Dem ist ein prognostisches Element der Unsicherheit immanent, vgl. Sachs-*Sachs*, Art. 20 Rn. 150 f. m.w.N.

873 *Pieroth/Schlink* 2003, Rn. 285 ff.; *Stern* 1994, 780 m.w.N.

874 BVerfGE 50, 217 (227); 80, 103 (107); *Stern* 1994, 782 m.w.N.; kritisch gegenüber dem selbständigen Charakter der objektiven Zumutbarkeit *Pieroth/Schlink* 2003, Rn. 289 ff.; zur Gefahr einer Beliebigkeit der Abwägung auch Sachs-*Sachs*, Art. 20 Rn. 155 m.w.N.

875 Vgl. *Gola/Schomerus*, § 13 Rn. 3 ff.; insbes. der Grundsatz der Erforderlichkeit zieht sich durch das gesamte BDSG, vgl. Simitis-*Sokol*, § 13 Rn. 25; zur Anwendbarkeit des Verhältnismäßigkeitsprinzips bereits *Benda* 1974, 23, 37 ff.

876 V. Mangoldt/Klein/Starck-*Starck*, Art. 2 Rn. 15; ausführlich *Lücke*, DÖV 2002, 93 ff.; *Tiedemann*, DÖV 2003, 74 ff.

877 Vgl. v. Münch/Kunig-*Kunig*, Art. 2 Rn. 43.

878 *Roßnagel/Pfitzmann/Garstka* 2001, 98; Simitis-*o.V.*, § 14 Rn. 15; s.a. BVerfGE 65, 1 (46); das ist im Sinne einer conditio sine qua non zu verstehen, s. *Auernhammer*, § 13 Rn. 6; Simitis-*Sokol*, § 13 Rn. 26; insbesondere geht es nicht darum, was technisch möglich, sondern darum, was tatsächlich geeignet und erforderlich ist, s. *Kutscha* 2001, 4.

4.2.1.2.2 Zweckbindung und Zweckbegrenzung

Der Grundsatz der datenschutzrechtlichen Zweckbindung fußt im Verhältnismäßigkeitsprinzip. Er ist deshalb ein Verfassungsgebot; Zweckentfremdungen sind verfassungsrechtlich unzulässig.[879] Da eine Datenverwendung immer nur in Bezug auf einen konkreten Zweck hin geeignet sein kann, muss dieser zuvor eindeutig und ausdrücklich bestimmt werden.[880] In der Folge dürfen die Daten nur zu diesem Zweck verarbeitet und genutzt werden. Nachträgliche Zweckänderungen, die zu einer Datenverwendung außerhalb des ursprünglichen Zwecks führen, stellen einen selbständigen Grundrechtseingriff dar,[881] weil auch ein an sich „harmloses" Einzeldatum durch eine Änderung des Verarbeitungszwecks neue Bedeutung erlangen kann.[882] Dieser neue Eingriff unterliegt den üblichen Anforderungen. Es ist also eine gesetzliche Ermächtigungsgrundlage oder eine Einwilligung erforderlich. Damit wird verhindert, dass Daten zu einem eng begrenzten Zweck erhoben und danach zu anderen, unbestimmten Zwecken verwendet werden.[883]

Neben dieser Verankerung im Verhältnismäßigkeitsprinzip verwirklicht die Zweckbindung der Datenverwendung auch das Gebot der Normenklarheit.[884] Nur so wird für den Betroffenen deutlich, wozu die Verwendung seiner Daten dient. Im Ergebnis bestimmt der Zweckbindungsgrundsatz Ziel und Umfang zulässiger Datenverarbeitung und begrenzt sie zugleich auf diese.[885] Daraus ergibt sich insbesondere, dass eine Datenverarbeitung auf Vorrat unzulässig ist.[886] Sobald der Zweck der Verwendung erreicht ist, sind die Daten außerdem zu löschen, da sie ab diesem Zeitpunkt im Rahmen ihrer Zweckbestimmung nicht mehr erforderlich sind.[887] Sofern sich im Laufe des Verwendungsprozesses ergibt, dass ein Personenbezug der Daten nicht mehr notwendig ist, sind dieses zu anonymisieren oder zu pseudonymisieren.[888] Schließlich findet sich in Nr. 8 der Anlage zu § 9 BDSG seit dem Jahre 2001 die Anforderung, das rechtliche Gebot der Zweckbindung auch technisch abzusichern.[889]

Der Grundsatz der Zweckbindung findet sich auch in internationalen Normen,[890] die nach der Rechtsprechung des Bundesverfassungsgerichts im Rahmen der völker- und europarechtsfreundlichen Auslegung des deutschen Rechts zu berücksichtigen sind.[891] So ist nach den Richtlinien der Generalversammlung der Vereinten Nationen der Zweck der

879 S. M/D-*Di Fabio*, Art. 2 Abs. 1 Rn. 186; AK GG-*Podlech*, Art. 2 Abs. 1 Rn. 82; *Bizer* 1992, 148; *Schmitz* 2000, 14 m.w.N.; Roßnagel-*v. Zezschwitz*, Kap. 3.1, Rn. 3; einfachgesetzliche Umsetzungen finden sich bspw. in §§ 14, 28 Abs. 1 Satz 2 BDSG, s. *Gola/Schomerus*, § 14 Rn. 9 ff.; Simitis-*Simitis*, § 28 Rn. 59 ff., 79 ff., 205 ff., 310 ff.; s.a. Roßnagel-*v. Zezschwitz*, Kap. 3.1, Rn. 20 ff.; kritisch gegenüber der Effektivität des Zweckbindungsgrundsatzes Roßnagel-*Trute*, Kap. 2.5, Rn. 37 ff.

880 BVerfGE 65, 1, (46); *Gola/Schomerus*, § 14 Rn. 9.

881 *Roßnagel/Pfitzmann/Garstka* 2001, 115; *Scholz* 2003, 139 m.w.N.

882 *Roßnagel/Wedde/Hammer/Pordesch* 1990, 120.

883 *Denninger*, KJ 1985, 215, 220. In der anglo-amerikanischen Diskussion wird das Problem mit „function creep" bezeichnet. Im Zusammenhang mit der Verarbeitung biometrischer Daten s. hierzu *Woodward* 1999, 396; *Nanavati/Thieme/Nanavati* 2002, 239 ff.; *Woodward/Orlans/Higgins* 2003, 207 f.

884 *Denninger*, KJ 1985, 215, 223; Simitis-*o.V.*, § 14 Rn. 37; *Ehmann/Helfrich* 1999, Art. 6 Rn. 8.

885 *Roßnagel/Pfitzmann/Garstka* 2001, 111.

886 BVerfGE 65, 1 (46); *Roßnagel/Pfitzmann/Garstka* 2001, 98; *Schaffland/Wiltfang*, § 14 Rn. 13, 17; Simitis-*Sokol*, § 13 Rn. 26 m.w.N.; das gilt auch nach der DSRL, s. *Ehmann/Helfrich* 1999, Art. 6 Rn. 23.

887 BVerfGE 100, 313 (362).

888 BVerfGE 65, 1 (51); *Roßnagel/Pfitzmann/Garstka* 2001, 100.

889 S. dazu unten 4.3.8.2.2.

890 Es handelt sich um einen weltweit anerkannten Grundsatz, s. *Banisar/Davies*, J. Marshall J. Computer & Info. L. 1999, 1, 11.

891 S. dazu oben Einl. zu 4.1.1.

Datenverarbeitung vor ihrem Beginn festzulegen und öffentlich bekannt zu machen. Eine nachträgliche Zweckänderung ist unzulässig. Nach Art. 6 Abs. 1 lit. b-e DSRL[892] dürfen Daten nur für festgelegte eindeutige und rechtmäßige Zwecke erhoben und nur im Rahmen dieser Zweckbestimmung weiterverarbeitet werden. Durch die Einbeziehung der Erhebung muss der Zweck vor der Datenerhebung festgelegt sein.[893] Die Daten müssen im Hinblick auf die Zwecke zutreffend und vollständig sein und nach ihrer Realisierung anonymisiert werden. Auch gemäß Nr. 9 der OECD-Richtlinien zum Datenschutz ist eine Zweckbestimmung vor der Datenerhebung erforderlich. Im Rahmen von Art. 5 b) des Übereinkommens des Europarats reicht demgegenüber zwar eine Zweckbestimmung mit dem Beginn des Speicherns aus.[894] Auch hier ist das Prinzip jedoch verankert.

In Umsetzung dieser Grundsätze ist für Chipkartenausweise eine ausdrückliche und präzise Bestimmung des Verwendungszwecks erforderlich. Das ist insbesondere deshalb wichtig, weil multifunktionalen Karten das Risiko der Überschreitung der Zweckbindung inhärent ist.[895] Überdies ist es unabdingbar, dass die gesetzliche Zweckbindung tatsächlich alle verwendeten – insbesondere die sensiblen – Daten erfasst. Der Schutz der Zweckbindung kann außerdem die Ausdifferenzierung unterschiedlicher Zwecke erfordern, weil andernfalls eine globale Zweck-„Bestimmung" das Konzept ad absurdum führen würde. Ferner muss eine Absicherung gegenüber missbräuchlichem Zugriff erfolgen. Dies bezieht sich einerseits auf die technische Ebene, andererseits aber auch auf rechtliche Schutzinstrumente.

4.2.1.2.3 Informationelle Gewaltenteilung

Das Prinzip der informationellen Gewaltenteilung hängt eng mit dem Zweckbindungsgedanken zusammen.[896] Es erlangt bei multifunktionalen Chipkarten besondere Bedeutung. Hinter der informationellen Gewaltenteilung stehen zwei sich ergänzende Grundgedanken. Eine unkontrollierte Verfügbarkeit von Informationen über die Betroffenen kann einerseits zu einer staatlichen Machtkonzentration führen,[897] andererseits die Selbstdarstellung der Betroffenen in unterschiedlichen Kommunikationsbeziehungen (und damit ihre selbstbestimmte Identitätsbildung) erschweren.[898] Um beidem vorzubeugen, hat das Bundesverfassungsgericht verlangt, durch organisatorische Vorkehrungen dafür zu sorgen, dass eine Trennung von Datenverarbeitungen zu unterschiedlichen Zwecken in der Verwaltung gewährleistet wird.[899] Der Staat darf nicht als Informationseinheit gesehen werden, in der

892 Dazu Roßnagel-*v. Zezschwitz*, Kap. 3.1, Rn. 7 ff.; *Ehmann/Helfrich* 1999, Art. 6 Rn. 6 ff. Die Regelungen zur Zweckbindung sind einer der Bereiche, in denen das deutsche Datenschutzrecht vor der Novelle im Jahre 2001 hinter der Richtlinie zurückblieb, s. *Gounalakis/Mand*, CR 1997, 431, 436.

893 *Ehmann/Helfrich* 1999, Art. 6 Rn. 6; *Schild*, EuZW 1996, 549, 551.

894 Vgl. näher *Henke* 1986, 103.

895 *Bizer* 2002, 28; s.a. *Roßnagel* 1994b, 269 f.

896 Simitis-*Simitis*, Einl. Rn. 36; Roßnagel-*Topp*, Kap. 8.12, Rn. 44. Daneben ist es ein wesentlicher Teil des Konzepts des Systemdatenschutzes, s. Roßnagel-*Dix*, Kap. 3.5, Rn. 7.

897 So schon *Steinmüller/Lutterbeck/Mallmann/Harbort/Kolb/Schneider* 1971, 40 f., 128; s.a. Roßnagel-*Dix*, Kap. 3.5, Rn. 3 f.; *Bull*, DÖV 1979, 689 ff.; *Kirchberg*, ZRP 1977, 137, 139; *Heußner*, BB 1990, 1281, 1283 f.

898 *Roßnagel/Pfitzmann/Garstka* 2001, 126; AK GG-*Podlech*, Art. 2 Abs. 1 Rn. 45; Roßnagel-*v. Zezschwitz*, Kap. 3.1, Rn. 1; s. zur Frage der Identitätsbildung oben 1.

899 BVerfGE 65, 1 (69); BVerfG, NJW 1988, 959, 961.

beliebige Informationsflüsse möglich sind; das Wissen einer Behörde soll nicht zugleich das (fiktive) Wissen aller anderen Zweige der Verwaltung bedeuten.[900]

Als Terminus findet sich die informationelle Gewaltenteilung nicht in internationalen Rechtsnormen. Aufgrund des Bezugs zur Zweckbindung lässt sich das Prinzip jedoch im Grundsatz auch in diesen verankern. In der deutschen Diskussion ist es allerdings nicht unumstritten. Die beschriebene Form der organisatorischen Trennung von Verarbeitungsbereichen wird zum Teil als anachronistisch und undurchführbar bezeichnet.[901] Dies ist jedoch nicht zutreffend. Gerade die moderne Technikentwicklung bei Chipkarten ist ein Beispiel dafür, wie informationelle Gewaltenteilung (etwa durch die Definition unterschiedlicher Datenfelder mit entsprechenden Zugriffsrechten) technisch abgesichert werden kann.

4.2.1.2.4 Profilbildung und allgemeines Personenkennzeichen

Der Missbrauch von erstellten Persönlichkeitsprofilen ist eines der größten Probleme im Datenschutzrecht. Solche Profile entstehen dann, wenn über das Zusammenführen von Einzeldaten hinaus zusätzliche, bisher nicht vorhandene Erkenntnisse über die Persönlichkeit der betroffenen Person gewonnen und zu einem (Teil-)Abbild der Persönlichkeit zusammengeführt werden.[902] Das kann zwar auch im Interesse des Betroffenen liegen. Die Gefahr besteht aber darin, dass ein derart umfangreiches Wissen über einen sozialen Interaktionspartner dessen selbstbestimmte Persönlichkeitsdefinition unmöglich macht. Das hat zwei Folgen:

- Zum einen werden aus der Perspektive des Einzelnen die Möglichkeiten der Selbstbeschreibung zunehmend eingeschränkt.[903] Dies kann die Identität eines Menschen – hier verstanden als die „gesellschaftsvermittelte Möglichkeit...seine eigene Vergangenheit der Gesellschaft oder in für ihn relevanten Sektoren der Gesellschaft so darzustellen, dass er diese Darstellung in der Gegenwart bejahen kann“[904] – beeinträchtigen.
- Zum anderen stellen Daten-Profile aus systemtheoretischer Sicht ein Instrument des jeweiligen Systems dar, um seine Herrschaftsambitionen gegenüber seiner Umwelt durchzusetzen. Das ist deshalb problematisch, weil dabei Verhaltensmodelle aufoktroyiert werden. Dies kann zu einer Störung der sozialen Integration führen.[905]

---

900 *Denninger*, KJ 1985, 215, 222; *Mückenberger*, KJ 1984, 1, 19 ff.; *Roßnagel/Wedde/Hammer/Pordesch* 1990, 121 f.; Simitis-*Simitis*, Einl. Rn. 36; *ders.*, NJW 1986, 2795, 2800 et passim; *Tinnefeld/Ehmann* 1998, 88; AK GG-*Podlech*, Art. 2 Abs. 1 Rn. 80; Roßnagel-*Topp*, Kap. 8.12, Rn. 44.

901 M/D-*Di Fabio*, Art. 2 Abs. 1 Rn. 184; kritisch auch *Scholz/Pitschas* 1984, 120 ff. et passim; *Vogelgesang* 1987, 227 ff.; *Götz*, HdbStR III (1996), § 79 Rn. 41.

902 *Wittig*, RDV 2000, 59; s.a. *Roßnagel/Pfitzmann/Garstka* 2001, 118.

903 Roßnagel-*Roßnagel*, Kap. 1, Rn. 4; *Roßnagel/Wedde/Hammer/Pordesch* 1990, 121; s.a. *Schmidt*, JZ 1974, 241, 245 f.; *Gusy*, VerwA 1983, 91, 92 f.; *Rössler* 2001, 209 m.w.N.; im privaten Bereich bildet die Anfertigung kommerziell verwertbarer Profile den Hintergrund der Problematik, s. Simitis-*Simitis*, § 28 Rn. 173 f.; *Weichert*, NJW 2001, 1463, 1464; kritisch gegenüber der Betonung der Gefahr von Profilen *Ladeur*, DuD 2000, 12, 13; Roßnagel-*Trute*, Kap. 2.5, Rn. 25 ff.; vgl. zu dieser Kritik aber *Roßnagel/Pfitzmann/Garstka* 2001, 118.

904 AK GG-*Podlech*, Art. 1 Abs. 1 Rn. 34 ff., Art. 2 Abs. 1 Rn 45 in Anlehnung an *Luhmann* (1965, 60 ff.); vgl. zur Privatheit als Bedingung autonomer Lebensführung *Rössler* 2001, 127 ff., 136 ff., 201 ff et passim; zum Bezug zu den Überlegungen Foucaults zur panoptischen Gesellschaft s. ebd., 216 ff. m.w.N.; s. zum Zusammenhang zwischen Identifizierung und Identitätsbildung bereits oben 1.

905 S. *Donos* 1998, 24; zu den Gefahren der Profilbildung auch *TAB* 2002, 45; *Roßnagel/Pfitzmann/Garstka* 2001, 117 ff.; *Denninger*, KJ 1985, 215, 227, 235 ff.

Aus diesen Gründen ist nach Ansicht des Bundesverfassungsgerichts sowohl das totale Registrieren[906] als auch das Anfertigen von Teilprofilen[907] der Persönlichkeit gegen den Willen des Betroffenen verfassungswidrig. Auch in der Literatur wird dies so gesehen.[908] Das Verbot derartiger Profilbildung bildet einen Unterfall des Zweckbindungsgrundsatzes[909] und wurzelt damit letztlich im Verhältnismäßigkeitsprinzip. Allerdings gibt das Bundesverfassungsgericht keine Kriterien dafür an, wann ein verfassungswidriges Teilprofil vorliegt.[910] Jedenfalls kann nicht jede Datensammlung über einen Betroffenen diese Schwelle erreichen. Möglich ist, die Unzulässigkeit eines Profils aus einem langen abgebildeten Zeitraum, einer Vielzahl von erfassten Lebensbereichen, einer Lückenlosigkeit der Dokumentation und einer Verwendbarkeit für sehr unterschiedliche Zwecke abzuleiten.[911] Multifunktionschipkarten bergen hier besondere Risiken. Je zahlreicher die Lebensbereiche werden, in denen ein und dieselbe Chipkarte eines Betroffenen eingesetzt wird und je mehr Datenspuren sie dort hinterlässt, desto größer ist das Risiko, dass eine Dokumentation dieser Einsätze alle Handlungen des Betroffenen festhält.[912] Dem kann mit der Verwendung unterschiedlicher Karten für unterschiedliche (sensible) Lebensbereiche teilweise entgegengewirkt werden.[913] Dies widerspricht allerdings dem allgemeinen Trend der Chipkartenentwicklung, der eher hin zu einer Integration mehrerer Funktionalitäten in eine Karte geht.

Ein Instrument der Profilbildung ist die Verwendung eines einheitlichen Personenkennzeichens. Werden Daten bei unterschiedlichen Stellen erhoben, verarbeitet und genutzt, so wird die Zusammenführung dieser verteilt gespeicherten Datenbestände erleichtert, wenn bei den jeweiligen Stellen bereits eine Verknüpfung mit demselben Personenkennzeichen erfolgte.[914] Daher wird in der deutschen Diskussion ein solches Kennzeichen regelmäßig für unzulässig gehalten. Dieses schlage bewusst oder unbewusst die Brücke zur permanenten Kontrolle der Betroffenen, die bis hin zur Steuerung ihres Verhaltens gehen könne.[915] Ein einheitliches Personenkennzeichen wurde auch vom Bundesverfassungsgericht[916] und vom Rechtsausschuss des Bundestages[917] für verfassungswidrig erklärt. Die Rechtsprechung des Bundesverfassungsgerichts ist Grundlage der Verwendungsbeschränkungen der Seriennummer des Personalausweises. § 3 Abs. 1 PersAuswG verbietet ausdrücklich Seriennummern und Prüfziffern, die Daten über die Person des Ausweisinhabers oder Hin-

906 BVerfGE 27, 1 (6); kritisch gegenüber dieser Rspr. *Roßnagel/Wedde/Hammer/Pordesch* 1990, 247: das Gericht verfehle die alltägliche Bedrohung, weil es ohnehin unmöglich sei, „den" Menschen in seiner „ganzen" Persönlichkeit zu registrieren.

907 BVerfGE 65, 1 (53 f.).

908 AK GG-*Podlech*, Art. 2 Abs. 1 Rn. 79, 83 (s. bereits *ders*., DVR 1972/73, 149, 157); *Benda* 1974, 23 ff., insbes. 27 f.; *Kirchberg*, ZRP 1977, 137, 138 f.; *Lisken*, NJW 1982, 1481, 1486; M/D-*Di Fabio*, Art. 2 Abs. 1 Rn. 184; BK-*Zippelius*, Art. 1 Rn. 98; *Roßnagel/Wedde/Hammer/Pordesch* 1990, 207.

909 S. Roßnagel-*v. Zezschwitz*, Kap. 3.1, Rn. 1; Roßnagel-*Roßnagel*, Kap. 3.4, Rn. 71.

910 Vgl. *Denninger*, KJ 1985, 215, 227.

911 Roßnagel-*Weichert*, Kap. 9.5, Rn. 45.

912 *Bizer* 2002, 28; Roßnagel-*Weichert*, Kap. 9.5, Rn. 44.

913 Roßnagel-*Weichert*, Kap. 9.5, Rn. 44.

914 S. bereits *Kirchberg*, ZRP 1977, 137 ff.; zur informationstechnischen Verwendung *Steinmüller*, DVR 1983, 205, 215 ff.

915 Simitis-*Simitis*, Einl. Rn. 12; mit anderem Akzent *Steinmüller*, DVR 1983, 205, 242 ff., der danach differenziert, ob die Verwendung eines Personenkennzeichens zu einer nicht mehr hinnehmbaren Intransparenz der Datenverarbeitung führt.

916 BVerfGE 27, 1 (6); 65, 1, 53 (57).

917 Vgl. BT-Drs. 7/5277, 3. Hintergründe waren Pläne in den frühen siebziger Jahren des vorigen Jahrhunderts, ein einheitliches Personenkennzeichen in Deutschland einzuführen; s. näher *Kirchberg*, ZRP 1977, 137 m.w.N.; *Weichert*, RDV 2002, 170, 172; *Albrecht* 2003a, 178 m.w.N.

weise auf solche Daten enthalten. Damit soll gerade eine Funktion als Personenkennziffer verhindert werden.[918] Auch in der aktuellen Diskussion um ein einheitliches Identifikationsmerkmal im Steuerrecht wird die Problematik betont.[919]

Auf der anderen Seite zeigt der Blick ins Ausland, dass Länder mit vergleichbaren Datenschutzstandards – wie etwa Schweden, Dänemark, Estland und Finnland – seit langer Zeit ein derartiges Merkmal verwenden.[920] Auch Österreich verarbeitet in seinem Zentralen Melderegister eine so genannte ZMR-Zahl.[921] Japan führt zurzeit im Zusammenhang mit dem dortigen Ausweisprojekt ein entsprechendes Register ein.[922] Darüber hinaus wird die Verwendung einer „nationale[n] Kennziffer oder andere[r] Kennzeichen allgemeiner Bedeutung" in Art. 8 Abs. 7 DSRL ausdrücklich der Regelungskompetenz der Mitgliedstaaten unterstellt.[923] Im Unterschied zu anderen datenschutzrechtlichen Grundsätzen ist die Unzulässigkeit eines einheitlichen Personenkennzeichens also keineswegs international anerkannt.[924]

Gleichzeitig fragt sich, ob ein Verbot eines solchen Kennzeichens unter den Bedingungen der modernen Datenverarbeitung tatsächlich ein geeignetes Sicherungsmittel gegen Datenzusammenführungen und Profilbildungen darstellt.[925] In der Tat wird dazu heutzutage kein einheitliches System benötigt, das über die ohnehin gespeicherten Daten hinausgeht. Jede Stelle, die personenbezogene Daten speichert, speichert per definitionem den Namen des Betroffenen oder kann diesen zumindest bestimmen. In kaum einem Fall bleibt es indes beim Namen; in aller Regel werden zumindest auch der Geburtstag und -ort erfasst. Da bei der Verwendung dieser vier Daten identische Datensätze kaum vorkommen dürften, ist es mit diesen Angaben regelmäßig ohne größere Probleme möglich, verteilt gespeicherte Daten zusammenzuführen.

Der Befund aus der Praxis ist insoweit allerdings uneinheitlich. In der DDR spielte die dortige Personenkennzahl eine entscheidende Rolle bei der Überwachung der Bevölkerung mit Hilfe von Datenzusammenführungen.[926] Dies fand jedoch unter grundlegend anderen informationstechnischen Bedingungen statt. Für die aktuelle Leistungsfähigkeit der Systeme wird einerseits betont, jüngste Versuche der Datenzusammenführung ohne einheitliches Ordnungsmerkmal zeigten, dass diese aufgrund der Fehleranfälligkeit der eingesetzten Software und des Umgangs mit den Daten nach wie vor erheblich erschwert sei.[927] Andererseits gibt es gerade im Sicherheitsbereich hinreichend Beispiele dafür, dass Datensätze aus unterschiedlichsten Verwendungszusammenhängen auch ohne einheitliches Personenkennzeichen zusammengeführt werden können.[928]

---

918 Vgl. *Medert/Süßmuth* 1998, § 3 Rn. 4.

919 S. etwa *Weichert*, RDV 2002, 170 ff.; http://www.heise.de/newsticker/meldung/42628.

920 Roßnagel-*Burkert*, Kap. 2.3, Rn. 68, 73, 75; gegen eine Vergleichbarkeit *Weichert*, RDV 2002, 170, 176.

921 Nach § 16 Abs. 4 des Meldegesetzes (BGBl. Nr. 9/1992, zuletzt geändert durch Gesetz v. 27.2.2004, BGBl. I Nr. 10/2004).

922 S.o. 3.4.2.5.

923 Dazu *Dammann/Simitis* 1997, Art. 8 Rn. 32; *Ehmann/Helfrich* 1999, Art. 8 Rn. 62 ff.

924 Andererseits ist man sich der Problematik im Ausland bewusst, s. Simitis-*Simitis*, Einl. Rn. 12 m.w.N.

925 Zweifelnd bereits *Kauß* 1984, 69; ebenso *Roßnagel/Wedde/Hammer/Pordesch* 1990, 141; *Bizer*, DuD 2004, 45. Nach AK GG-*Podlech*, Art. 2 Abs. 1 Rn. 79 käme das Verbot eines Personenkennzeichens bei dem heutigen Stand der Datenverarbeitung einem Verbot derselben gleich.

926 S. Kilian/Heussen-*Weichert*, Nr. 130 Rn. 35 (unter Verweis auf die Vorauflage, Stand 1993, Rn. 35); *ders.*, RDV 2002, 170.

927 *Weichert*, RDV 2002, 170, 173.

928 Bspw. bei der zu präventiven Zwecken durchgeführten Rasterfahndung, s. *Bizer*, DuD 2004, 45.

Im Ergebnis wird man davon ausgehen können, dass zum gegenwärtigen Zeitpunkt die Einführung eines einheitlichen Ordnungsmerkmals für die gesamte staatliche Tätigkeit Datenzusammenführungen (noch) erleichtern würde. Mit der zunehmenden Leistungsfähigkeit und Standardisierung der Verarbeitungsprozesse und der verwendeten Software wird dies jedoch zunehmend weniger der Fall sein. Da Chipkartenausweise gerade erst am Beginn ihrer Entwicklung stehen, dürften sie in weiten Bereichen in einem Umfeld eingesetzt werden, in dem Datenzusammenführungen technisch relativ unproblematisch sind.

Unter diesen Bedingungen ist eine Konzentration auf das Problem des einheitlichen Personenkennzeichens wenig weiterführend. Ohnehin verschleiert die Debatte den Blick auf den Einsatz entsprechender Surrogate. So ist beispielsweise die Debatte um die Verwendung der Seriennummer des Personalausweises[929] inhaltlich irreführend, weil bereits der aktuelle Personalausweis selbst funktionell ein einheitliches Personenkennzeichen ist.[930]

Eine Lösung kann nur darin liegen, nicht die Verwendung eines Datums zu untersagen, das als derartiges Kennzeichen eingesetzt werden kann, sondern die Verwendung gerade als allgemeines Kennzeichen. Das gilt beispielsweise für die neue einheitliche Krankenversichertennummer nach § 290 SGB V.[931] Diese darf nicht zur Zusammenführung von Informationen aus dem Gesundheitswesen mit Daten aus anderen Verarbeitungsbereichen verwendet werden. Im Kern geht es damit um die strikte Einhaltung der Regeln der Zweckbindung und der informationellen Gewaltenteilung.[932] Diese rechtlichen Nutzungsbeschränkungen sind – soweit möglich – technisch und organisatorisch zu sichern.

4.2.1.2.5 Transparenz

Die Transparenz der Datenverwendung gehört zu den verfassungsrechtlich gewährleisteten Grundpositionen des Betroffenen.[933] Das Bundesverfassungsgericht hat betont, dass mit dem Recht auf informationelle Selbstbestimmung eine Gesellschafts- und Rechtsordnung nicht vereinbar wäre, „in der Bürger nicht mehr wissen, wer was wann und bei welcher Gelegenheit über sie weiß“.[934]

Dieser Gedanke hat zwei Komponenten. Zum einen fordert er allgemein Transparenz im Sinne von Durchschaubarkeit der Rechtsordnung.[935] Zum anderen soll der einzelne Betroffene in seinen Rechten geschützt werden. Intransparente Informationssammlungen verursachen ein Machtgefälle zu Lasten des Betroffenen.[936] Die Unsicherheit darüber, was die Daten verwendende Stelle über ihn weiß, kann zu angepasstem Verhalten, und damit zu einer Verletzung des Rechts auf freie Entfaltung der Persönlichkeit führen. Denkbar ist auch, dass Betroffene Leistungen nicht in Anspruch nehmen, weil sie nicht überblicken können, was mit den Informationen geschieht, die sie hierfür preisgeben müssen.[937]

---

929 *Medert/Süßmuth* 1998, § 3 Rn. 4 und 11 ff. (s.a. den Bericht des BT-Innenausschusses, BT-Drs. 8/3498, 9); *Bizer*, DuD 2004, 45.

930 *Steinmüller*, DVR 1983, 205, 304 f.; *Podlech*, Leviathan 1984, 85, 87; *Kauß* 1984, 69.

931 Vgl. dazu *Der Bundesbeauftragte für den Datenschutz* 2005, 165 f.

932 S.a. *Weichert*, RDV 2002, 170, 173.

933 *Gola/Schomerus*, § 33 Rn. 1; AK GG-*Podlech*, Art. 2 Abs. 1 Rn. 81.

934 BVerfGE 65, 1 (43). Die Formulierung ist tlw. an *Podlech* (1982, 455) angelehnt.

935 Roßnagel-*Trute*, Kap. 2.5, Rn. 33.

936 S. *Roßnagel/Wedde/Hammer/Pordesch* 1990, 38 f.

937 Das ist insbesondere im Gesundheitswesen relevant (*Roßnagel/Wedde/Hammer/Pordesch* 1990, 192 ff.), kann aber auch im Bereich von Sozialleistungen Bedeutung erlangen, wenn dort von den Antragstellern die Offenbarung weitreichender Informationen über materielle und soziale Verhältnisse verlangt wird.

Das Bundesverfassungsgericht hat ausgeführt, dass der Wesensgehalt eines Grundrechts betroffen ist, „wenn jeglicher Störungsabwehranspruch, den die Rechtsordnung zu[m] Schutz des Grundrechts einräumt, materiellrechtlich beseitigt oder wenn verfahrensrechtlich verwehrt wird,…[den Anspruch] wirkungsvoll geltend zu machen, mag er oder das Grundrecht, zu dessen Schutz er gewährt ist, auch...materiellrechtlich bestehen bleiben“.[938] Ohne eine Kenntnisnahme von der Datenverwendung besteht weder Anlass noch Möglichkeit für den Betroffenen, deren Rechtmäßigkeit zu überprüfen oder seine Rechte auf Unterlassung, Berichtigung und Löschung geltend machen.[939] Dies steht im Widerspruch zur Wesensgehaltsperre des Art. 19 Abs. 2 GG. Dem kann nur durch eine umfassende Geltung des Transparenzprinzips entgegengewirkt werden, das deshalb nicht auf die Transparenz der Existenz der Daten beschränkt ist, sondern ebenso die Struktur der Datenverarbeitung und ihre Zwecksetzung erfasst.[940]

Auch auf internationaler Ebene finden sich in den jeweiligen Rechtsgrundlagen Ausprägungen des Transparenzprinzips, die die Auslegung des deutschen Datenschutzrechts beeinflussen.[941] Im Rahmen der Vorarbeiten für die europäische Datenschutzrichtlinie wurde die Wichtigkeit größtmöglicher Transparenz für die Durchsetzbarkeit von Betroffenenrechten betont.[942] Die wichtigsten Umsetzungen des Prinzips sind das Auskunftsrecht (Art. 12 DSRL)[943] und die Meldepflicht (Art. 18 DSRL). Die Beachtung des Transparenzgrundsatzes bildet außerdem einen wesentlichen Gesichtspunkt in der Entscheidung der Kommission vom 15. Juni 2001 hinsichtlich Standardvertragsklauseln für die Übermittlung personenbezogener Daten in Drittländer.[944] Auch die OECD-Richtlinien fordern in Nr. 7, 2. Halbsatz die Datenerhebung mit Wissen oder Zustimmung des Betroffenen. Des Weiteren baut das Übereinkommen des Europarats von 1981 auf dem Transparenzprinzip auf,[945] und die Entscheidung *Leander ./. Schweden* des Europäischen Gerichtshofs für Menschenrechte,[946] die erstmals grundlegend feststellte, dass Art. 8 EMRK vor staatlicher Datenverarbeitung schützt, behandelte einen Fall intransparenter geheimdienstlicher Daten.

Transparenz ist immer dann besonders wichtig, wenn Kommunikationsverhalten potentiell umfassend und unbemerkt dokumentiert werden kann. Durch den technischen Fortschritt wird es vermehrt üblich werden, eine einzige Chipkarte in verschiedenen Lebensbereichen einzusetzen. Dabei erweitern sich auch die Möglichkeiten einer umfassenden Dokumentation. Mit der zunehmenden Komplexität der Karten wird die Umsetzung des Transparenzgebots immer schwieriger werden. Selbst bei einer umfassenden Aufklärung des Karteninhabers dürfte dieser kaum noch in der Lage sein, die Datenverarbeitungsvorgänge auf dem Chip wirklich nachzuvollziehen. Deswegen wird vertreten, es sei unzulässig, über einen bestimmten Komplexitätsgrad hinauszugehen, weil dann eine informierte

938 BVerfGE 61, 82 (113).
939 BVerfGE 100, 313 (361); Roßnagel-*Trute*, Kap. 2.5, Rn. 34; Roßnagel-*Roßnagel*, Kap. 3.4, Rn. 10; *Roßnagel/Pfitzmann/Garstka* 2001, 82; zur Problematik der aus einer Intransparenz resultierenden Rechtsschutzdefizite vgl. *Kutscha*, NVwZ 2003, 1296 ff.
940 *Roßnagel/Pfitzmann/Garstka* 2001, 87 f.
941 S. zum Verhältnis oben Einl. zu 4.1.1.
942 Vgl. die Stellungnahme des Europäischen Parlaments zum ersten Richtlinienentwurf („Hoon-Report“), S. 64 (zitiert nach: *Ehmann/Helfrich* 1999, Art. 6 Rn. 9); s.a. Erwägungsgrund 38.
943 Der Rat sah hierin einen entscheidenden Bestandteil des Transparenzprinzips, s. Begründung des Rates zum gemeinsamen Standpunkt, ABl. EG C 93 v. 13.4.1995, 23.
944 Abrufbar unter http://www.datenschutz-berlin.de/doc/eu/kommission/de_final_clean.htm.
945 *Henke* 1986, 101.
946 Urteil v. 26.3.1987, abrufbar unter http://www.echr.coe.int/Eng/Judgments.htm.

Einwilligung des Betroffenen nicht mehr angenommen werden könne.[947] Es dürfte allerdings in der Praxis schwer feststellbar sein, wo diese Grenze liegt.

Einfachgesetzliche Ausprägungen des Transparenzprinzips sind unter anderem der Grundsatz der Direkterhebung (§ 4 Abs. 2 BDSG und vorrangige spezialgesetzliche Regelungen, beispielsweise § 14 Abs. 1 Satz 1 SigG[948]), Aufklärungs- und Unterrichtungspflichten wie das Auskunftsrecht des Betroffenen[949] und die Regelung über mobile personenbezogene Speicher- und Verarbeitungsmedien in § 6c BDSG.[950]

4.2.1.2.6 Staatliche Schutzpflichten

Die Grundrechte haben nicht nur die Funktion, den Einzelnen vor Eingriffen des Staates zu schützen. Vielmehr fordern sie unter der Geltung des Grundgesetzes vom Staat, sich „schützend und fördernd" vor die in den Grundrechten genannten Rechtsgüter zu stellen, und sie vor rechtswidrigen Eingriffen von Seiten anderer zu bewahren.[951] Diese Schutzpflicht des Staates wurde vom Bundesverfassungsgericht für das Grundrecht auf Leben und körperliche Unversehrtheit entwickelt.[952] Sie gilt jedoch auch für die übrigen durch die Verfassung geschützten Grundrechte.[953] Gleichzeitig billigt das Gericht dem Gesetzgeber einen politischen Gestaltungsspielraum hinsichtlich der Ausgestaltung der jeweiligen Schutzinstrumente zu,[954] allerdings dann nicht mehr, wenn die Verfassung bestimmte Mittel zum Schutz vorschreibt. Der Gesetzgeber darf überdies nicht ganz untätig bleiben oder eindeutig zu wenig zum Schutz unternehmen.[955] Liegt eine Verletzung der staatlichen Schutzpflicht vor, so ist damit gleichzeitig das jeweilige subjektive Grundrecht verletzt.[956]

Diese Regeln gelten auch für die informationelle Selbstbestimmung.[957] Das Bundesverfassungsgericht hat deshalb gefordert, der Gesetzgeber müsse weitgehende „organisatorische und verfahrensrechtliche Vorkehrungen" zum Schutz des Grundrechts treffen.[958] Auch nach der Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte sind „geeignete und angemessene Schutzvorkehrungen" zu ergreifen, um eine Verletzung der in

---

947 Roßnagel-*Weichert*, Kap. 9.5, Rn. 48; zur Intransparenz von Chipkarten auch *BT-Enquetekommission Zukunft der Medien* 1998, 53 f.

948 Dieser ist für die Datenerhebung durch den Zertifizierungsdiensteanbieter vorrangig, wenn auf dem jeweiligen Ausweis Signaturverfahren ablaufen. Hier greifen auch noch weitere Unterrichtungspflichten nach § 6 SigG und § 6 SigV bezüglich der Handhabung, der Archivierung und der rechtlichen Folgen der elektronischen Signatur ein; s. RMD-*Roßnagel*, § 6 SigG 1997, Rn. 24 ff. und unten 5.1.

949 Dieses ist unabdingbarer Teil des Transparenzprinzips, s. *Gola/Schomerus*, § 33 Rn. 2; s.a. *Roßnagel/Pfitzmann/Garstka* 2001, 82 ff.

950 S. *Hornung*, DuD 2004, 15 ff. und unten 4.3.3.

951 Ob dies bereist aus dem subjektiven Abwehranspruch der Grundrechte oder aus ihrer objektivrechtlichen Dimension folgt ist str., s. v. Münch/Kunig-*v. Münch*, Vorb. Rn. 22 m.w.N.; zumindest besteht ein enger Zusammenhang zur Drittwirkungsproblematik, s. *Pieroth/Schlink* 2003, Rn. 183 m.w.N.

952 BVerfGE 39, 1 (41 ff.); 46, 160 (164); 49, 89 (140 ff.); 53, 30 (57); weitere Bsp. bei v. Münch/Kunig-*v. Münch*, Vorb. Rn. 22; s. zur Rspr. des BVerfG *Szczekalla* 2002, 92 ff.

953 *Götz*, HdbStR III (1996), § 79 Rn. 10; *Stern* 1988, 944 m.w.N.; *Pieroth/Schlink* 2003, Rn. 94 ff.; Sachs-*Murswiek*, Art. 2 Rn. 25 m.w.N.; zu Kriterien für die Begründung von Schutzpflichten s. Mangoldt/Klein/Starck-*Gusy*, Art. 10 Rn. 62; *Isensee*, HdbStR V (2000), § 111 Rn. 77 ff.; speziell zur Menschenwürde vgl. v. Münch/Kunig-*Kunig*, Art. 1 Rn. 25 ff., 30 ff.

954 BVerfGE 56, 54 (80 f.); s. v. Münch/Kunig-*Kunig*, Art. 2 Rn. 56 m.w.N.; näher *Hesse* 1994, 553 ff.

955 BVerfGE 46, 160 (164 f.); 92, 26 (46); Sachs-*Murswiek*, Art. 2 Rn. 30; v. Münch/Kunig-*Kunig*, Art. 2 Rn. 56.

956 BVerfGE 77, 170 (214); *Isensee*, HdbStR V (2000), § 111 Rn. 183 ff.; einschränkend v. Mangoldt/Klein/Starck-*Starck*, Art. 1 Rn. 160.

957 Sachs-*Murswiek*, Art. 2 Rn. 25; s.a. *Scholz* 2003, 145 m.w.N.

958 BVerfGE 65, 1 (44).

Art. 8 EMRK garantierten Rechte zu verhindern.[959] Dieser Schutzpflicht muss der Staat insbesondere auch dann nachkommen, wenn das Recht auf informationelle Selbstbestimmung dadurch beeinträchtigt wird, dass Privatpersonen rechtswidrig Daten des Betroffenen verwenden: Zur Sicherung der Selbstbestimmung ist die Ausgestaltung eines Freiheitsbereiches auch im gesellschaftlichen Umfeld erforderlich.[960]

4.2.2 Die verfassungsrechtliche Zulässigkeit des digitalen Personalausweises

Angesichts der ausdrücklich unvollständigen Regelung des Personalausweisgesetzes[961] kann sich die verfassungsrechtliche Analyse des digitalen Personalausweises nicht auf seine grundsätzliche Zulässigkeit und die Verfassungsmäßigkeit der bisherigen Bestimmungen beschränken, sondern muss zusätzlich Anforderungen an eine zu schaffende Rechtsgrundlage mit in den Blick nehmen.

Die folgende Darstellung beschränkt sich, soweit sie sich auf biometrische Daten bezieht – trotz der Regelung in § 1 Abs. 4 Satz 1 PersAuswG, die „biometrische Merkmale von Fingern oder Händen oder Gesicht" nennt – im Wesentlichen auf die Merkmale Gesicht, Fingerabdruck und Iris. Diese werden von der ICAO als prinzipiell geeignet empfohlen[962] und auch in den Staaten, die eine Einführung biometrischer Daten in Identitätspapiere in Erwägung ziehen, favorisiert.[963] Die in § 1 Abs. 4 Satz 1 PersAuswG ebenfalls genannte Erkennung der Handgeometrie dürfte für den digitalen Personalausweis bereits deshalb ausscheiden, weil das Merkmal nur beim Erwachsenen hinreichend beständig ist.[964] Der Ausweis wird jedoch ab dem 17. Lebensjahr ausgegeben.

4.2.2.1 Grundsätzliche Verfassungsmäßigkeit

4.2.2.1.1 Verfassungsmäßigkeit der Personalausweispflicht

§ 1 Abs. 1 Satz 1, 1. Halbsatz PersAuswG verpflichtet jeden meldepflichtigen Deutschen ab dem 17. Lebensjahr zum Besitz eines Personalausweises.[965] Daran wird sich auch bei der Einführung des digitalen Personalausweises nichts ändern.

Im Unterschied zur Diskussion im angloamerikanischen Raum wurde und wird die grundsätzliche Zulässigkeit der Datenerhebung, -verarbeitung und -nutzung für den Personalausweis in Deutschland nicht in Frage gestellt. In den USA, Kanada und Großbritannien wird eine Ausweispflicht von weiten Teilen der Bevölkerung, aber auch von namhaften Rechtswissenschaftlern als unzulässig abgelehnt.[966] In Großbritannien wurde die zu Kriegszeiten eingeführte Personalausweispflicht im Jahre 1952 nach einem Gerichtsurteil

---

959 Z ./. Finnland, Urteil v. 25.1.1997, Abs. 95; M.S. ./. Schweden, Urteil v. 27.8.1997, Abs. 41 (beide abrufbar unter http://www.echr.coe.int/Eng/Judgments.htm); zu den Schutzpflichten nach der EMRK s. *Szczekalla* 2002, 712 ff. m.w.N.; zum Europarecht vgl. ebd., 459 ff. m.w.N.

960 *Hoffmann-Riem*, AöR 1998, 513, 523.

961 S. zum gegenwärtigen Regelungssystem oben 2.2.1.

962 *ICAO* 2004a, 16.

963 Die EU-Mitgliedstaaten werden z.B. in Art. 1 Abs. 2 der Verordnung (EG) Nr. 2252/2004 (dazu oben 3.1.2) zur Speicherung von Gesichts- und Fingerabdrucksdaten in ihren Reisepässen verpflichtet.

964 *TAB* 2002, 21.

965 Eine Ausnahme besteht nach § 1 Abs. 1 Satz 1, 2. Halbsatz PersAuswG für Inhaber eines Reisepasses, die sich durch diesen ausweisen können.

966 S. bereits oben 3.4.1.1, 3.5.2.1, 3.5.2.2. Wenn in einem Mitgliedstaat der EU keine Ausweispflicht besteht, so folgt aus Art. 49 EGV, dass auch für Angehörige der anderen Mitgliedstaaten eine solche nicht begründet werden darf, s. EuGH, DVBl. 2005, 495.

über die Rechtswidrigkeit einer allgemeinen Vorlagepflicht bei der Polizei[967] wieder abgeschafft. Im Unterschied dazu blieb die in Deutschland im Jahre 1938 begründete Ausweispflicht[968] von den Alliierten unangetastet und wurde im Jahre 1951 in das neue Gesetz über Personalausweise überführt.[969] Soweit ersichtlich, ist die Zulässigkeit der Personalausweispflicht selbst seitdem nie bestritten worden.[970] Auch die teilweise heftige Diskussion in den 80er Jahren des letzten Jahrhunderts wurde nicht um den Ausweis an sich, sondern um die Einführung der Maschinenlesbarkeit geführt.[971]

Nichtsdestotrotz ist eine allgemeine Personalausweispflicht nur dann rechtmäßig, wenn sie verhältnismäßig, also geeignet, erforderlich und angemessen zur Erreichung eines rechtmäßigen Zieles ist. Der Ausweis dient mehreren Zielen. Zunächst findet er im Rahmen von Personenkontrollen im Bereich präventiver polizeilicher Arbeit Anwendung. Sodann erleichtert die Existenz eines Personalausweises die Tätigkeit der Strafverfolgungsbehörden. Innerhalb der Europäischen Union ist der Ausweis außerdem ein vollgültiges Reisedokument. Nach § 4 Abs. 1 PersAuswG kann er schließlich auch im privaten Bereich als Legitimationsdokument verwendet werden. Alle diese Ziele sind legitim und die allgemeine Personalausweispflicht ist zu ihrer Erreichung geeignet.

Zur Erreichung der Ziele der Gefahrenabwehr und Strafverfolgung ist ein allgemeiner Ausweis auch erforderlich, da er durch eine hohe Fälschungssicherheit eine sichere Identifikation aller Personen ermöglicht. Diese ist zur effektiven Durchführung von präventiven und repressiven Maßnahmen durch Polizei und Staatsanwaltschaft notwendig. Als milderes, das heißt den Betroffenen weniger belastenden Mittel käme nur ein Rückgriff auf andere Identitätsdokumente in Betracht. Diese sind aber mit höherer Unsicherheit behaftet, da nur hinter dem Personalausweis der Schutz durch modernste Sicherheitsmerkmale und ein staatliches Ausgabeverfahren steht. Was schließlich die Verhältnismäßigkeit im engeren Sinne angeht, so stellt die Pflicht zum Besitz eines Ausweises eine relativ geringe Belastung für den Inhabers dar, weil dieser den Personalausweis nicht ständig mit sich führen muss.[972] Weitere Aspekte, etwa die Gefahr einer Profilbildung durch die automati-

---

967 *Willcock v Muckle*, decision of 26 June 1951 (by Acting Lord Chief Justice *Goddard*); s. näher *Agar* 2001, 110 f.; *Thomas*, MLR 1995, 702, 705 f. Das Gericht bestätigte zwar die Verurteilung des Angeklagten, nachdem dieser nicht wie vorgeschrieben einen Ausweis vorgelegt hatte, sah jedoch von einer Strafe ab und entschied, es sei „unreasonable", wenn die Polizei routinemäßig einen Ausweis kontrolliere, der unter den besonderen Bedingungen des Krieges eingeführt worden war. Das bezieht sich auf den sog. „Wednesbury unreasonableness"-Test, benannt nach der Entscheidung *Associated Provincial Picture Houses Ltd v Wednesbury Corp* [1947] 2 AllER 680. Dieser lässt der Verwaltung erheblich mehr Spielräume als die deutsche Ermessensfehlerlehre. In *Council of Civil Service Unions v Minister for the Civil Service* (1985) AC 374, 410 definierte Lord *Diplock* unreasonable als "so outrageous in its defiance of logic or of accepted moral standards that no sensible person who had applied his mind to the question to be decided could have arrived at it". Zwar gibt es Entwicklungen hin zu mehr Kontrolle, s. *Lord Irvine*, Public Law 1996, 59, 73 ff.; *ders.*, Public Law 1998, 221, 232 ff.; *Laws*, Public Law 1993, 59, 69 m.w.N. Davon waren die Gerichte 1951 jedoch noch weit entfernt, weshalb die Entscheidung in *Willcock v Muckle* sehr bemerkenswert ist.

968 Durch die Verordnung v. 22.7.1938, RGBl. I, 913 wurde ein allgemeiner Inlandsausweis eingeführt. Eine Mitführungspflicht bestand mit Inkrafttreten der Verordnung v. 10.9.1939, RGBl I, 913; s.o. 2.2.1.1.

969 V. 19.12.1950, BGBl. 807. Das Gesetz trat am 1.1.1951 in Kraft.

970 Es gab zwar vereinzelte Forderungen nach ihrer Abschaffung (so 1986 von der Bundestagsfraktion DIE GRÜNEN, s. BT-Drs. 10/1316), diese wurden aber politisch begründet.

971 S. ausführlich unten 7.3.2.2.

972 Der Ausweis muss einer Behörde lediglich in angemessener Frist vorgelegt werden können, s. *Medert/Süßmuth* 1998, § 1 Rn. 17. Wird er nicht mitgeführt, so kann das allerdings zur Unmöglichkeit einer rechtmäßigen Identitätsfeststellung führen. Nach den Landespolizeigesetzen ist die Polizei in solchen

sche Lesbarkeit, betreffen nicht die Ausweispflicht an sich, sondern den weiteren Umgang mit den erhobenen Daten. Gegenüber dem Ziel der Unterstützung der staatlichen Polizeiarbeit steht die Personalausweispflicht deshalb nicht außer Verhältnis. Sie ist damit rechtmäßig.

Für den nicht-hoheitlichen Bereich fehlt es dagegen an der Erforderlichkeit, weil die freiwillige Ausgabe von Ausweispapieren nur an solche Bürger, die tatsächlich Auslandsreisen vornehmen beziehungsweise im Rechtsverkehr auf einen staatlichen Ausweis angewiesen ist, ein milderes, gleich geeignetes Mittel darstellt. Die Einsatzmöglichkeit im privaten Umfeld ist jedoch nur ein zusätzliches, freiwilliges Einsatzfeld für den verpflichtenden Personalausweis und berührt dessen Rechtmäßigkeit nicht.

4.2.2.1.2 Grundsätzliche Verfassungsmäßigkeit des Einsatzes von Biometrie

Der staatliche Einsatz biometrischer Ausweisdaten wäre grundsätzlich unzulässig, wenn er gegen die Menschenwürde (Art. 1 Abs. 1 GG) verstieße. Solange § 3 Abs. 1 Satz 1 PersAuswG a.F. die Aufnahme von Fingerabdrücken in den Personalausweis verbot,[973] bejahten die wenigen Kommentatoren, die sich aus verfassungsrechtlicher Sicht mit diesem Thema befassten, überwiegend auch einen Verstoß gegen die Menschenwürde.[974] Fraglich ist, ob dieser Ansicht – verallgemeinert auf alle biometrischen Merkmale – zuzustimmen ist.[975]

Die Menschenwürde ist der „höchste Rechtswert“[976] und ein „tragendes Konstruktionsprinzip“[977] der deutschen Rechtsordnung. Die Regelung des Art. 1 Abs. 1 GG hat ein Vorbild in Art. 1 der Allgemeinen Erklärung der Menschenrechte. Ebenso ist das erste Kapitel der Charta der Grundrechte der Europäischen Union mit „Würde des Menschen“ überschrieben. Die Europäische Menschenrechtskonvention enthält zwar keine ausdrückliche Schutzbestimmung. Die Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte hat jedoch in vielfältiger Weise auf die Menschenwürde Bezug genommen.[978]

Die Besonderheit des grundgesetzlichen Menschenwürdeschutzes besteht darin, dass es keinerlei Legitimation, keine Rechtfertigung für einen Eingriff gibt. Verletzt der Staat diesen engsten Bereich menschlicher physischer und psychischer Integrität, so ist der Eingriff stets rechtswidrig.[979]

Dieser Absolutheitsanspruch ist einer der Gründe dafür, dass verfassungsrechtliche Rechtsprechung und Schrifttum kaum je zu umfassenden oder fassbaren Definitionen der Menschenwürde gefunden haben.[980] Die Unschärfe des Schutzbereiches liegt auch in dem

---

Situationen regelmäßig zur vorläufigen Sistierung berechtigt, s. etwa *Würtenberger/Heckmann/Riggert* 2002, Rn. 331.

973 Die Norm wurde durch das Terrorismusbekämpfungsgesetz (BGBl. I 2002, 361) geändert, s.o. 2.2.1.2.

974 *Dürig*, AöR 1956, 117, 129; M/D-*Dürig* (Stand: 42. Lieferung Februar 2003), Art. 1 Rn. 37; s.a. VG Berlin, NJW 1955, 964, 965; anders nunmehr nach Änderung des PersAuswG M/D-*Herdegen*, Art. 1 Abs. 1 Rn. 88.

975 Vgl. zum Folgenden (knapp) *Roßnagel/Hornung*, in: Reichl/Roßnagel/Müller 2005, 109 f.

976 BVerfGE 45, 187 (227), ähnlich BVerfGE 32, 98 (108); 50, 166 (175); 54, 341 (357); hierzu v. Münch/Kunig-*Kunig*, Art. 1 Rn. 4 m.w.N.

977 BVerfGE 87, 209 (228).

978 Vgl. *Meyer-Ladewig*, NJW 2004, 981 ff. m.w.N.

979 Ganz h.M., s. v. Münch/Kunig-*Kunig*, Art. 1 Rn. 4; v. Mangoldt/Klein/Starck-*Starck*, Art. 1 Abs. 1 Rn. 30; AK GG-*Podlech*, Art. 1 Abs. 1 Rn. 73; *Pieroth/Schlink* 2003, Rn. 365 (jeweils m.w.N.).

980 Zu unterschiedlichen Deutungsversuchen (oder dem Verzicht darauf) s. *Häberle*, HdbStR II (2004), § 22 Rn. 5 ff., 31 ff.; v. Münch/Kunig-*Kunig*, Art. 1 Rn. 22; AK GG-*Podlech*, Art. 1 Abs. 1 Rn. 10 f. Schlagwortartig lässt sich zwischen „Mitgifttheorie“ und „Leistungstheorie“ unterscheiden. Nach ersterer besteht die Menschenwürde in einem dem Menschen von Gott oder der Natur mitgegebenen in-

Begriff an sich. So ist davon gesprochen worden, auf ihm lasteten „zweieinhalbtausend Jahre Philosophiegeschichte“.[981] Die Offenheit des Begriffs ist allerdings gleichzeitig seine Stärke: Er aktualisiert sich durch immer neue Bedrohungen der menschlichen Würde, zu denen gesellschaftlicher Wandel und technologische Entwicklung beitragen.[982]

Dementsprechend hat das Bundesverfassungsgericht betont, es lasse sich nicht generell ausdrücken, unter welchen Umständen die Menschenwürde verletzt sein könne, sondern immer nur in Ansehung des konkreten Falles.[983] Gleichzeitig findet sich in seiner Rechtsprechung mit der so genannten Objektformel ein negativer Deutungsversuch, der den Schutzbereich anhand möglicher Gefährdungs- oder Eingriffslagen bestimmt. Danach widerspricht es der menschlichen Würde, wenn der Mensch „zum bloßen Objekt staatlichen Handelns“ wird.[984] Die Versuche, diese Formel mit Leben zu füllen, variieren. Teilweise wird eine Einteilung in fünf Gruppen vorgenommen.[985] Danach schützt die Menschenwürde die physische Identität und Integrität des Menschen, wie auch seine psychische Identität und Integrität. Außerdem sind die notwendigen Grundlagen menschlichen Lebens und die Regeln elementarer Rechtsgleichheit erfasst. Schließlich begrenzt Art. 1 Abs. 1 GG die staatliche Gewaltanwendung. Ob und in wieweit auch nach der Finalität des Eingriffs zu fragen ist, ist umstritten.[986] Wegen der Unmöglichkeit einer Rechtfertigung besteht aber weitgehend Einigkeit darüber, dass lediglich der absolute Kernbereich menschlicher Existenz von Art. 1 Abs. 1 GG geschützt wird.[987]

Was die Verwendung biometrischer Systeme und hier speziell eine Verwendung im Rahmen eines Gesamtsystems „digitaler Personalausweis“ betrifft, so sind weder Lebensgrundlagen noch elementare Gleichheitsrechte oder die Begrenzung staatlicher Gewaltanwendung betroffen. Zwar kann es durchaus zu Ungleichbehandlungen verschiedener Bevölkerungsgruppen kommen. Diese führen im Rahmen des Eingriffs in die informationelle Selbstbestimmung zum Erfordernis effektiver Rückfallsysteme, ohne die der Einsatz von Biometrie rechtswidrig ist.[988] Die Ungleichbehandlungen sind jedoch nicht so gravierend,

---

neren Wert, nach letzterer in seiner eigenen Leistung der Identitätsbildung; s. zusammenfassend *Pieroth/Schlink* 2003, Rn. 354 ff. m.w.N.

981 *Pieroth/Schlink* 2003, Rn. 353; s. zur geistesgeschichtlichen Verankerung mit unterschiedlichen Akzenten AK GG-*Podlech*, Art. 1 Abs. 1 Rn. 2 ff.; v. Münch/Kunig-*Kunig*, Art. 1 Rn. 19 ff.; v. Mangoldt/Klein/Starck-*Starck*, Art. 1 Abs. 1 Rn. 3 ff., jeweils m.w.N.; zusammenfassend zur (insbesondere durch die Neukommentierung von M/D-*Herdegen*, Art. 1 Abs. 1 angestoßenen) aktuellen Diskussion *Nettesheim*, AöR 2004, 71 ff.

982 V. Münch/Kunig-*Kunig*, Art. 1 Rn. 7.

983 BVerfGE 30, 1 (25); BVerfG, NJW 1993, 3315.

984 BVerfGE 50, 166 (175); s.a. BVerfGE 5, 85 (204); 9, 89 (95); 72, 105 (116); 87, 209 (228); s. zuvor schon BVerwGE 1, 159 (161); *Dürig*, AöR 1956, 117, 127 ff. Das lässt sich auf *Kant* zurückführen: „Der Mensch kann von keinem Menschen (weder von anderen noch sogar von sich selbst) bloß als Mittel, sondern muss jederzeit zugleich als Zweck gebraucht werden, und darin besteht eben seine Würde (die Persönlichkeit), dadurch er sich über alle anderen Weltwesen, die nicht Menschen sind und doch gebraucht werden können, mithin über alle Sachen erhebt.“ (1797, 462; s.a. ebd., 434 f.; *ders*. 1785, 434 f., 439 f.); zur Kritik an der Objektformel *Nettesheim*, AöR 2004, 71, 79 ff. m.w.N.

985 AK GG-*Podlech*, Art. 1 Abs. 1 Rn. 23 ff.; *Maihofer* 1968, 56 ff.; *Häberle*, HdbStR II (2004), § 22 Rn. 45 (s. aber den Ansatz ebd., Rn. 46 ff.); *Pieroth/Schlink* 2003, Rn. 361 (s.a. 12. Auflage 1996, Rn. 389 ff.); ähnlich Sachs-*Höfling*, Art. 1 Rn. 19 ff.; Jarass/Pieroth-*Jarass*, Art. 1 Rn. 7; Dreier-*Dreier*, Art. 1 I Rn. 59 ff.

986 S. hierzu v. Münch/Kunig-*Kunig*, Art. 1 Rn. 24. Zumindest im Grundsatz ist dies nicht der Fall. Es kann keinen Unterschied machen, ob die Menschenwürde „in guter Absicht“ verletzt wird, s. Sondervotum BVerfGE 30, 33 (40); Dreier-*Dreier*, Art. 1 I Rn. 53 m.w.N.; *Pieroth/Schlink* 2003, Rn. 360.

987 Sachs-*Höfling*, Art. 1 Rn 16 m.w.N.; Jarass/Pieroth-*Jarass*, Art. 1 Rn. 10; BK-*Zippelius*, Art. 1 Rn. 16.

988 S. ausführlich unten 4.2.2.4.7.

dass ein Menschenwürdeverstoß vorliegt. Es besteht auch kein Eingriff in die körperliche Integrität, da die hier untersuchten biometrischen Verfahren nicht mit körperlichen Verletzungen verbunden sind. Hinsichtlich der geistigen Identität und Integrität gibt es jedoch mehrere mögliche Ansatzpunkte für eine Verletzung der Menschenwürde, nämlich die Verwendung des menschlichen Körpers, das Problem der Profilbildung und die Bestimmbarkeit des ursprünglichen Geschlechts nach einer medizinisch indizierte Geschlechtsumwandlung.

Zunächst kann eine Herabwürdigung des Menschen zum Objekt darin gesehen werden, dass der menschliche Körper zur Informationsgewinnung verwendet wird. Überdies geschieht dies auf verpflichtender Basis. Denkbar ist ein Vergleich mit der Verwendung von Polygraphen im Strafprozess.[989] Dieser wurde vom Bundesverfassungsgericht für unzulässig erklärt, auch wenn dies nicht unter Berufung auf die Menschenwürde, sondern auf das allgemeine Persönlichkeitsrecht geschah.[990] In der Literatur wird in diesem Zusammenhang dagegen Art. 1 Abs. 1 GG herangezogen.[991]

Jedoch kann wegen der angesprochenen Beschränkung auf den Kernbereich menschlicher Existenz nicht jede Verwendung menschlicher Körperteile in den Schutzbereich der Menschenwürde fallen. Die Unzulässigkeit des Polygraphentests im Strafverfahren folgt denn auch nicht allein aus der Verwendung des menschlichen Körpers und seiner Reaktionen zur Datengewinnung, sondern erst aus der Kombination dieses Verfahrens mit einer für den Einzelnen unbeeinflussbaren und nicht nachvollziehbaren Vorgehensweise, die darüber hinaus mit sehr weitreichenden, an die gewonnenen Ergebnisse geknüpften Folgen verbunden wird.[992] Die Bestimmung der Identität des Betroffenen mittels biometrischer Merkmale hat aber nicht gleichermaßen gravierende Folgen.

Darüber hinaus kennt die Rechtsordnung bereits Verfahren, bei denen der menschliche Körper als Basis für eine Datenerhebung benutzt wird. So werden bei herkömmlichen erkennungsdienstlichen Maßnahmen Fingerabdrücke und Gesichtsbilder genommen, bei der körperlichen Untersuchung nach § 81a StPO durch eine Blutabnahme Angaben über den körperlichen Zustand erhoben und im Rahmen der molekulargenetischen Untersuchung im Strafprozess (§§ 81e, 81f, 81g StPO)[993] und der Untersuchung zur Feststellung der Abstammung (§§ 1600c, 1600d BGB in Verbindung mit § 372a ZPO)[994] genetische Daten verglichen. Diese Verfahren greifen nicht in den oben angesprochenen Kernbereich menschlicher Existenz ein. Deshalb ist Art. 1 Abs. 1 GG nicht betroffen.

Vergleicht man die bloße Reidentifikation mittels biometrischer Merkmale mit den genannten Fällen und wendet das Kriterium des Kernbereiches auf biometrische Identifikationssysteme an, so ergibt sich ein entsprechendes Bild: Die bloße Wiedererkennung auf

---

989 *Bäumler/Gundermann/Probst* 2001, 24; Roßnagel-*Gundermann/Probst*, Kap. 9.6, Rn. 56 ff.

990 BVerfG, NJW 1982, 375; unzutreffend insoweit v. Münch/Kunig-*Kunig*, Art. 1 Rn. 36 und BK-*Zippelius*, Art. 1 Rn. 86, wonach das BVerfG den Lügendetektor als mit Art. 1 Abs. 1 GG unvereinbar angesehen habe.

991 *Benda* 1974, 35; AK GG-*Podlech*, Art. 1 Abs. 1 Rn. 47; v. Mangoldt/Klein/Starck-*Starck*, Art. 1 Abs. 1 Rn. 54; BK-*Zippelius*, Art. 1 Rn. 86; s.a. *Luhmann* 1965, 75; in dieser Richtung auch BGHSt 5, 332 (333 ff.); BVerwGE 17, 342 (346). Der BGH geht nunmehr allerdings im Fall freiwilliger Mitwirkung nicht mehr von einer rechtlichen Unzulässigkeit aus, s. BGHSt 44, 308 (319 ff.); ablehnend gegenüber dieser Rspr. AK GG-*Podlech*, Art. 1 Abs. 1 Rn. 47a. Da das Gericht den Polygraphen aber gleichzeitig als ein „völlig ungeeignetes Beweismittel" ansieht, gibt es weiterhin keine Verwendungsmöglichkeit. Das gilt auch im Zivilprozess, s. BGH, RDV 2003, 292.

992 Roßnagel-*Gundermann/Probst*, Kap. 9.6, Rn. 59; *Bäumler/Gundermann/Probst* 2001, 25.

993 S. *Faber*, RDV 2003, 278, 280 ff.

994 Genetische Test haben sich im Rahmen von § 372a ZPO noch nicht allgemein durchgesetzt, sind auf dieser Basis aber möglich, vgl. Musielak-*Huber*, § 372a Rn. 10.

dieser Basis verletzt den Kernbereich menschlicher Existenz nicht. Im Ergebnis ist damit festzuhalten, dass die Verwendung des menschlichen Körpers im Rahmen biometrischer Systeme an sich keinen Verstoß gegen die Garantie der Menschenwürde darstellt. Dies kann sich dann anders darstellen, wenn das verwendete Merkmal Überschussinformationen enthält, die sehr gravierende Folgen nach sich ziehen können. Zu weitgehend ist es allerdings, dies schon bei Rückschlüssen auf Nahrungsaufnahme und mangelnde Hygiene in Betracht zu ziehen.[995]

Ein zweiter Ansatzpunkt für eine Verletzung der Menschenwürde könnte sich dann ergeben, wenn der Einsatz biometrischer Verfahren zu einer umfassenden Persönlichkeitserfassung des Menschen führen würde. Das Bundesverfassungsgericht hat ausgeführt, dass es „mit der Menschenwürde...nicht zu vereinbaren [wäre], wenn der Staat das Recht für sich in Anspruch nehmen könnte, den Menschen zwangsweise in seiner ganzen Persönlichkeit zu registrieren und zu katalogisieren".[996]

Eine umfassende Katalogisierung des Einzelnen würde in biometrischen Systemen bei einer Erfassung des menschlichen Körpers in seiner Gänze erfolgen. Denn eine Speicherung sämtlicher in Betracht kommender Merkmale würde bei entsprechendem technischem Fortschritt eine totale Überwachung in allen Lebenslagen ermöglichen.[997] Ein derartiges Vorgehen wäre wegen eines Verstoßes gegen Art. 1 Abs. 1 GG verfassungswidrig. Es steht beim digitalen Personalausweis aber nicht in Rede.

Es fragt sich jedoch, ob es nicht zu eng ist, einen Verstoß gegen die Menschenwürde lediglich bei einer Erfassung sämtlicher biometrischer Merkmale zu bejahen. So wird vertreten, die verpflichtende Verwendung bestimmter oder einer geringen Zahl von Merkmalen könne „in die Nähe" eines Würdeverstoßes kommen, die „Erhebung und Verarbeitung eines isolierten biometrischen Merkmals" stelle aber „keinen Würdeverstoß dar".[998] Problematisch an dieser Auffassung ist, dass die Situation einer Erfassung sämtlicher Merkmale schon deswegen kaum jemals eintreten wird, weil aufgrund des technischen Fortschritts ständig mit der Entwicklung weiterer, heute noch unbekannter biometrischer Systeme zu rechnen ist, die wegen fehlender Funktionsfähigkeit noch nicht verwendet werden können, bei entsprechender Serienreife aber unter die obige Definition fallen würden. Auch unterhalb einer Erfassung aller Merkmale kann aber eine Verletzung der Menschenwürde dann gegeben sein, wenn wegen der spezifischen Verwendungsweise einer Gruppe von Merkmalen oder auch eines einzelnen Merkmals eine weitgehende (nicht notwendigerweise totale) Überwachung der Bevölkerung ermöglicht würde. Entscheidend ist nicht die Zahl der verarbeiteten Merkmale, sondern die Auswirkung auf den Betroffenen.

Verdeutlichen lässt sich das am Beispiel der Gesichtserkennung. Hier gibt es aus dem Ausland bereits Beispiele einer weitreichenden Überwachung. Bekanntestes Beispiel ist die Stadt London. Dort soll das bereits im Betrieb befindliche automatisierte System zur Nummernschildkontrolle bei der Einfahrt in den Innenstadtbereich demnächst auch zur automatischen Erfassung der Gesichter der Fahrer und zum Abgleich mit Datenbanken der

995 So aber Roßnagel-*Gundermann/Probst*, Kap. 9.6, Rn. 59; *Bäumler/Gundermann/Probst* 2001, 26.

996 BVerfGE 27, 1 (6); 65, 1 (41 ff.); s. ausführlich oben 4.2.1.2.4; zum Zusammenhang mit der Identitätsbildung oben 1.

997 Roßnagel-*Gundermann/Probst*, Kap. 9.6, Rn. 61; s.a. *OECD* 2004, 12 m.w.N.

998 So Roßnagel-*Gundermann/Probst*, Kap. 9.6, Rn. 61; *Bäumler/Gundermann/Probst* 2001, 26 f.; dem folgend *Albrecht* 2003a, 182; s.a. BK-*Zippelius*, Art. 1 Rn. 98, wonach die Verwendung des Fingerabdrucks verfassungsgemäß sei, solange er nicht zu einer Observierung in „allen" Lebenslagen eingesetzt werde.

Polizei eingesetzt werden.[999] Schon im Jahre 2002 existierten in Großbritannien etwa 2,5 Millionen CCTV Systeme.[1000] Nach einer Schätzung wurde der durchschnittliche Londoner Bürger im Jahre 1999 pro Tag etwa 300-mal durch derartige Systeme gefilmt.[1001] Die Zahl dürfte heute erheblich höher liegen. In einem hypothetischen System einer zentralen Speicherung aller Daten aller Gesichter einer Bevölkerung, die mit einer sehr großen Zahl von – technisch weiterentwickelten – Überwachungskameras im öffentlichen Raum gekoppelt wäre, könnte ein komplettes Bewegungsprofil jedes einzelnen Individuums über einen unbeschränkten Zeitraum erstellt werden. Ein derartiges Vorgehen würde gegen die Menschenwürdegarantie verstoßen, unabhängig davon, dass es sich nur um ein einzelnes Merkmal handelt, und dem Bürger noch die Unüberwachtheit seines privaten Bereichs verbliebe.[1002]

Auch ein solches System steht beim digitalen Personalausweis nicht in Rede. Insoweit gilt erneut, dass die Verwendung eines singulären biometrischen Merkmals zum Zweck der reinen Authentifizierung in einzelnen Kontrollsituationen nicht gegen die Menschenwürdegarantie verstößt. Problematisch ist aber, dass das Merkmal, weil es für den Ausweis von der gesamten Bevölkerung erhoben wird, als allgemeines Personenkennzeichen verwendet werden könnte. Im Grundsatz ist jedes biometrische Merkmal hierzu geeignet.[1003] Daraus folgt nach allgemeinen Kriterien die Unzulässigkeit der Verwendung gerade als allgemeines Ordnungskriterium, nicht jedoch die Rechtswidrigkeit der Verwendung überhaupt.[1004] Dies könnte bei biometrischen Merkmalen anders zu beurteilen sein, weil diese im Unterschied zu sonstigen, lediglich zugeschriebenen Ordnungsmerkmalen nicht veränderbar sind.[1005] So ist es möglich, Namen, Vornamen, Geburtstag und -ort durch Täuschungsmanöver des Betroffenen oder die Vergabe neuer Identitäten im Rahmen von Zeugenschutzprogrammen zu wechseln.[1006] Bei biometrischen Merkmalen besteht dagegen eine grundsätzlich lebenslange Bindung.

Andererseits ist eine Erstellung von Profilen zumindest in automatisierter Form bei der momentanen Leistungsfähigkeit biometrischer Systeme weitgehend unrealistisch. Sowohl eine Falschakzeptanz wie eine Falschzurückweisung würden die Genauigkeit der Profile stören. Solange die Summe aus FAR und FRR im Prozentbereich liegt, besteht kaum ein Risiko der Verwendung als einheitliches Personenkennzeichen. Mit Blick auf die zukünftige technische Entwicklung ist es jedoch erforderlich, bereits heute die Systeme so zu gestalten, dass eine solche Verwendung auch zukünftig ausgeschlossen ist.[1007] Dies kann insbesondere dadurch geschehen, dass biometrische Daten zum einen nur im jeweiligen Ausweis selbst (und nicht in Dateien der verantwortlichen Stelle) gespeichert werden, und

---

999 S. http://observer.guardian.co.uk/politics/story/0,6903,892001,00.html; http://www.heise.de/newsticker/meldung/34407; zur Problematik der Nummernschildkontrolle vgl. *Schieder*, NJW 2004, 778 ff.

1000 In Großbritannien gibt es kein Register für Überwachungskameras; deswegen können nur ungefähre Zahlen angegeben werden; vgl. näher *McCahill/Norris* 2002; zu den Auswirkungen und der Effektivität der Kameraüberwachung in Großbritannien vgl. *Gill/Spriggs* 2005, 19 ff. et passim.

1001 *Norris/Armstrong* 1999, 42.

1002 S.a. *Hornung*, KJ 2004, 344, 351.

1003 *Weichert*, RDV 2002, 170, 174; Roßnagel-*Gundermann/Probst*, Kap. 9.6, Rn. 61; *Golembiewski/Probst* 2003, 24; *Albrecht* 2003a, 180; s.a. *Nanavati/Thieme/Nanavati* 2002, 260 ff.

1004 S.o. 4.2.1.2.4.

1005 Dies gilt allerdings nur für physiologische Merkmale (die bei Chipkartenausweisen favorisiert werden) und nur vorbehaltlich etwaiger operativer Eingriffe.

1006 *Probst* 2002, 120 f.; *Albrecht* 2003a, 186.

1007 Eine Zusammenführung von Daten mittels der biometrischen Merkmale ist in jedem Fall zu verhindern, s. *Golembiewski/Probst* 2003, 28 f.; *Konferenz der Datenschutzbeauftragten* 2002, unter 4; zu den Gefahren der Profilbildung mittels biometrischer Daten auch *Weichert*, RDV 2002, 170, 174 et passim; Roßnagel-*Weichert*, Kap. 9.5, Rn. 44 ff.

zum anderen Matchingvorgänge ausschließlich in Umgebungen erfolgen, in denen auf technischer Ebene sichergestellt wird, dass keine Protokollierung der Daten erfolgt.[1008]

Ein Sonderproblem ergibt sich schließlich dann, wenn aus einem biometrischen Merkmal auf das biologische Geschlecht des Betroffenen geschlossen werden kann.[1009] Die Menschenwürdegarantie des Grundgesetzes gewährleistet das Recht des Menschen, über sich selbst zu verfügen, seine Identität selbst zu definieren und sein Schicksal eigenverantwortlich zu gestalten. Dazu gehört auch das Recht auf eine medizinisch indizierte Geschlechtsumwandlung.[1010] Nach Auffassung des Bundesverfassungsgerichts besteht nach dieser Umwandlung ein verfassungsrechtlicher Anspruch auf Änderung des Geschlechts im Personenstandsregister mit der Folge, dass eine Eheschließung mit Angehörigen des früheren Geschlechts möglich wird.[1011] Aufgrund dieser Rechtsprechung wurde im Transsexuellengesetz[1012] die entsprechende Möglichkeit geschaffen. § 5 Abs. 1 TSG verbietet in diesem Zusammenhang die Offenbarung des früheren Vornamens ohne Zustimmung des Betroffenen.[1013] Vergleichbare Ansprüche ergeben sich auch aus der Europäischen Menschenrechtskonvention. Der Europäische Gerichtshof für Menschenrechte hat anerkannt, dass eine medizinisch indizierte Geschlechtsumwandlung Ausdruck der Persönlichkeit ist, und bejaht (in Abkehrung von der vorherigen Rechtsprechung) seit zwei Entscheidungen aus dem Jahre 2002 auch das Recht, einen Menschen des ursprünglichen biologischen Geschlechts zu heiraten.[1014]

Mit diesen Anforderungen wäre es nicht zu vereinbaren, wenn bei der Erhebung eines biometrischen Datums die kontrollierende Person Kenntnis vom ursprünglichen Geschlecht des Betroffenen erlangen würde. Dieser müsste ständig damit rechnen, Irritationen beim Gegenüber hervorzurufen, würde dem Risiko von Diskriminierungen ausgesetzt und müsste sich gegen eine Rolleneinordnung wehren, die nicht seiner selbstgewählten Persönlichkeitsdefinition entspricht.

Das Problem wird dadurch entschärft, dass vermutlich nur bei der Verwendung von DNA mit entsprechender Sicherheit auf das ursprüngliche Geschlecht des Betroffenen geschlossen werden kann, nicht aber mit den hier in Rede stehenden Merkmalen Gesicht, Fingerabdruck und Iris. Sollte es allerdings in Zukunft möglich sein, auch bei diesen hinreichende Korrelationen herzustellen, wäre als Mindestanforderung zu formulieren, dass Kontrollgeräte zu verwenden sind, die die Angaben über das Geschlecht weder speichern noch gegenüber Kontrollpersonen offenbaren.

1008 Das deckt sich mit den Anforderungen des Verhältnismäßigkeitsprinzips, s.u. 4.2.2.4.3, 4.2.2.4.4.

1009 Hinweis von *H. Biermann* anlässlich eines Vortrags der AG 1 und 6 des TeleTrusT e.V. am 1.4.2003, Bonn.

1010 Sachs-*Höfling*, Art. 1 Rn. 36; AK GG-*Podlech*, Art. 1 Abs. 1 Rn. 50; v. Mangoldt/Klein/Starck-*Starck*, Art. 1 Abs. 1 Rn. 77; näher *Blankenagel*, DÖV 1985, 953 ff.; *Correll*, NJW 1999, 3372 ff.

1011 BVerfGE 49, 286 (298 ff.); 60, 123 (134 f.); 88, 87 (96).

1012 V. 10.9.1980 (BGBl. I, 1654), zuletzt geändert durch Art. 13 des Gesetzes v. 4.5.1998 (BGBl. I, 833).

1013 Aus dem allgemeinen Persönlichkeitsrecht folgt überdies ein Recht auf Anrede mit dem neuen Vornamen, s. BVerfG, NJW 1997, 1632 f.

1014 Goodwin ./. Vereinigtes Königreich, I ./. Vereinigtes Königreich, Urteile v. 17.7.2002 (abrufbar unter http://www.echr.coe.int/Eng/Judgments.htm); s. näher *Peters* 2003, 157 f., 169 f.; *Grabenwarter* 2003, 206, 237, 240 ff. Nach der Rspr. des EuGH (Rs. C-13/94, Slg. 1996, I-2143 – P ./. S; Rs. C-117/01 – K.B. ./. National Health Service Pensions Agency, JZ 2004, 512) liegt ein Fall von Geschlechterdiskriminierung vor, wenn Transsexuelle nach der Geschlechtsumwandlung benachteiligt werden; vgl. dazu *Flynn*, CMLRev 1996, 367 ff.; *Classen*, JZ 2004, 513 ff.

4.2.2.2 Gesetzesvorbehalt und Bestimmtheit der Ermächtigungsgrundlage

An die formellen rechtsstaatlichen Voraussetzungen müssen für einen so weitreichenden Grundrechtseingriff wie die Aufnahme biometrischer Daten in ein staatliches Ausweisdokument im Chipkartenformat hohe Anforderungen gestellt werden.[1015] Zu beachten ist, dass diese umso strenger sind, je sensibler die Art der verwendeten Daten ist und je umfassender sie genutzt werden.[1016] Das Problem der Gesetzesgrundlage stellt sich beim digitalen Personalausweis in zweifacher Hinsicht, nämlich für die Umstellung auf das Chipkartenformat und die Aufnahme biometrischer Merkmale.

Für das Format ordnet § 1 Abs. 2 Satz 1 PersAuswG die Ausstellung der Ausweise nach einheitlichen Mustern mit Lichtbild an, während § 1 Abs. 7 PersAuswG die Bestimmung der Muster durch Rechtsverordnung vorsieht, die das Bundesministerium des Innern mit Zustimmung des Bundesrates erlässt. In der Rechtsverordnung ist die äußere Erscheinung des Ausweises geregelt. Dagegen gibt es keine gesetzliche Bestimmung über die Sicherheitsmerkmale. Deren Gestaltung erfolgt durch die Bundesdruckerei GmbH in Abstimmung mit dem Bundesministerium des Innern und dem Bundeskriminalamt.[1017]

Es ließe sich argumentieren, der Übergang vom bisherigen Format zur Chipkarte sei der Bestimmung der Muster oder der Ausgestaltung der Sicherheitsmerkmale vergleichbar. Im ersten Fall würde eine Regelung in der entsprechenden Rechtsverordnung genügen, im zweiten wäre überhaupt keine gesetzliche Grundlage vonnöten. Bei der Einführung eines Chipkartenausweises handelt es sich jedoch keineswegs um eine nachgeordnete technische Umsetzungsfrage. Durch die Digitalisierung der Ausweisdaten und die gegenüber dem heutigen System der opto-elektronischen Erfassung erleichterte Möglichkeit des Auslesens (insbesondere bei kontaktlosen Chipkartensystemen) und Weiterverarbeitens entsteht eine grundsätzliche neue Gefährdungslage für das informationelle Selbstbestimmungsrecht der Ausweisinhaber. Auch das geltende Recht enthält in § 1 Abs. 3 PersAuswG die Regelung über die Maschinenlesbarkeit des aktuellen Ausweises. Damit ist für den digitalen Personalausweis eine entsprechende Norm hinsichtlich des Chipkartenformats erforderlich.[1018]

Für die Sicherheitsmerkmale des Ausweises ist demgegenüber – wie bisher – eine rechtliche Regelung, auch auf untergesetzlicher Ebene, weder sinnvoll noch erforderlich. Sie ist nicht sinnvoll, weil dadurch eine kontinuierliche Weiterentwicklung der Sicherheitsmerkmale erschwert würde, und (bei exakter Bestimmung und Erläuterung der Merkmale) die Fälschungssicherheit leiden könnte. Und sie ist nicht erforderlich, weil durch ein bestimmtes Sicherheitsmerkmal dem Bürger keinerlei Nachteile entstehen (insbesondere, da kein Personenbezug der Echtheitsmerkmale besteht),[1019] und er deswegen kein Recht hat, Einzelheiten über die Sicherheitsmerkmale zu erfahren.[1020] Deshalb sind bei Bedarf im bishe-

---

1015 Vgl. *Roßnagel/Hornung*, in: Reichl/Roßnagel/Müller 2005, 120 f.; *dies*., DuD 2005, 69.

1016 S. v. Mangoldt/Klein/Starck-*Starck*, Art. 2 Rn. 109.

1017 S. http://www.bundesdruckerei.de/de/iddok/2_1/2_1_5.html. Die Sicherheitsmerkmale des aktuellen Ausweises sind: holographisches Portrait, 3D-Bundesadler, Kinematische Bewegungsstrukturen, Makroschrift und Mikroschrift, Kontrastumkehr, holographische Wiedergabe der maschinenlesbaren Zeilen, maschinell prüfbare Struktur, Oberflächenprägung, Sicherheitsdruck mit mehrfarbigen Guillochen, Laserbeschriftung und Wasserzeichen; s. im Einzelnen mit weiteren Erläuterungen http://www.bundesdruckerei.de/de/iddok/2_1/2_1_6.html.

1018 S.a. *Roßnagel/Hornung*, in: Reichl/Roßnagel/Müller 2005, 117 f. (tlw. offen gelassen).

1019 Eine Ausnahme bildet das holographische Portrait. Da dasselbe Bild jedoch in visueller Form ohnehin auf der Oberfläche des Ausweises aufgedruckt ist, ergibt sich hieraus kein weitergehender Eingriff in das Recht auf informationelle Selbstbestimmung.

1020 Die Sicherheitsmerkmale an sich (d.h. nicht ihre technischen Einzelheiten) werden im Übrigen durch die Bundesdruckerei GmbH veröffentlicht, s.o. Fn. 1017.

rigen Verfahren der Abstimmung zwischen Bundesministerium des Innern, Bundeskriminalamt und Hersteller vergleichbare Verfahren zur Fälschungssicherheit zu entwickeln.

Auch bei der Einführung biometrischer Daten sind die Anforderungen der Wesentlichkeitslehre und des Bestimmtheitsgebots zu beachten. Diese sind höher als bei der Einführung einer Chipkarte, da es hier um die Aufnahme neuer und sensibler Angaben geht. Die Intensität des Eingriffs in das Grundrecht auf informationelle Selbstbestimmung ist wegen der zumindest potentiell erheblichen Risiken biometrischer Erkennungsverfahren und der dabei entstehenden Daten als hoch im Sinne der Wesentlichkeitslehre zu bewerten. Damit ist grundsätzlich eine umfassende parlamentarische Gesetzesgrundlage erforderlich.

Das geltende Recht bestimmt, dass der Personalausweis biometrische Merkmale von Fingern oder Händen oder Gesicht enthalten „darf" (§ 1 Abs. 4 Satz 1 PersAuswG), jedoch die Arten der Merkmale, ihre Einzelheiten und die Einbringung in den Ausweis sowie die Art der Speicherung, Verarbeitung und Nutzung durch ein weiteres Gesetz geregelt werden (§ 1 Abs. 5 Satz 1 PersAuswG).

Diese Normen widersprechen sich gegenseitig:[1021] Wenn zur Einführung biometrischer Merkmale noch ein weiteres Gesetz erforderlich ist, so darf der Personalausweis diese Merkmale gerade nicht enthalten. Die Art des gesetzgeberischen Vorgehens hat in der Diskussion für entsprechende Verunsicherung gesorgt. Es werden die Auffassungen vertreten, die Regelung im Personalausweisgesetz enthalte eine Ermächtigungsgrundlage zur Einführung biometrischer Merkmale,[1022] die Einbringung derartiger Daten könne „jetzt vorgenommen" werden[1023] oder es sei „die Möglichkeit geschaffen worden...biometrische Merkmale...in Ausweispapiere...aufzunehmen".[1024] Diese Ansichten sind bereits vor dem Hintergrund der gesetzgeberischen „Ankündigung" in § 1 Abs. 5 Satz 1 PersAuswG klar unzutreffend.

Überdies wäre aber auch ohne diese Einschränkung eine Aufnahme biometrischer Merkmale in den Personalausweis auf der Basis von § 1 Abs. 4 Satz 1 PersAuswG nicht möglich, weil dieser die Voraussetzungen und Umstände der Datenverwendung nicht hinreichend bestimmt regelt. Die Ansicht, im Personalausweisgesetz sei „eine parlamentarische Grundlage [für den Einsatz biometrischer Merkmale] geschaffen, aus der (auch für den Bürger) Voraussetzungen, Ziel und Umfang des Eingriffes in das Recht auf informationelle Selbstbestimmung klar hervorgehen",[1025] ist nicht zutreffend. Zwar wird das Ziel der Personenidentifikation formuliert, hinsichtlich der Voraussetzungen und des Umfangs des Eingriffs enthalten § 1 Abs. 4 und 5 PersAuswG jedoch keinerlei Angaben darüber, welche Daten im Einzelnen verwendet, in welcher Form sie gespeichert und unter welchen Voraussetzungen sie in welcher Art und Weise weiterverarbeitet werden dürfen.

Noch kritikwürdiger sind demgegenüber Auffassungen, die in unzulässiger Weise verfassungsrechtliche Kategorien wie den Gesetzesvorbehalt mit einem Gesetz vermengen, das eine unvollständige, aus grundrechtlicher Sicht nicht hinreichende und weitere gesetzgeberische Schritte ankündigende Bestimmung enthält.[1026] Es wird etwa formuliert, § 1 Abs. 4 Satz 2 PersAuswG stelle es dem Gesetzgeber frei, die Verschlüsselung von Daten vorzusehen,[1027] aus § 1 Abs. 5 Satz 1 PersAuswG ergebe sich, dass die weiteren Einzelhei-

1021 S. zum Folgenden schon *Hornung*, KJ 2004, 344, 356 f.
1022 *Stock* 2002, 7; *TeleTrusT* 2002, 38.
1023 *Petermann*, TAB-Brief Nr. 24 (2003), 19, 21; *TAB* 2004, 5, 10.
1024 *TAB* 2002, 3, 7, 47; *Der Landesbeauftragte für den Datenschutz Brandenburg* 2002, 20.
1025 *TAB* 2002, 7, 47 f.
1026 Vgl. auch die Kritik bei *Nolte*, DVBl 2002, 573, 576; *Koch* 2002, 8 ff. Diese spricht diesen Regelungen des Terrorismusbekämpfungsgesetzes sogar die Gesetzesqualität ab, s. ebd., 14 ff., 29 ff.
1027 *Golembiewski/Probst* 2003, 57.

ten durch Bundesgesetz geregelt werden müssten,[1028] oder sogar, die Norm sehe „einen Gesetzesvorbehalt...vor“.[1029] Der Gesetzesvorbehalt ist jedoch ein verfassungsrechtlicher Grundsatz. Lediglich dann, wenn unter verfassungsrechtlichen Gesichtspunkten die Einführung biometrischer Merkmale keine (oder keine über § 1 Abs. 4 PersAuswG hinausgehende) gesetzliche Grundlage benötigen würde, könnte § 1 Abs. 5 Satz 1 PersAuswG eine Art Sperrwirkung für die Exekutive entfalten, die man dann – allerdings terminologisch ungenau – als „Gesetzesvorbehalt“ bezeichnen könnte. Da jedoch aus verfassungsrechtlicher Sicht eine weitaus genauere Regelung als § 1 Abs. 4 PersAuswG erforderlich ist, besteht für die Einführung der biometrischen Daten unabhängig von § 1 Abs. 5 Satz 1 PersAuswG ein verfassungsrechtlicher Gesetzesvorbehalt.

In weiten Teilen sind diese Ungenauigkeiten in der Argumentation durch den Gesetzgeber verursacht worden. So heißt es in der Gesetzesbegründung, durch besonderes Bundesgesetz könne „*zukünftig* eines von drei *bereits alternativ festgelegten* Biometriemerkmalen eingeführt werden“.[1030] Das ist in zweifacher Hinsicht unzutreffend: einerseits, weil ein solches Merkmal bereits bisher durch Bundesgesetz eingeführt werden konnte,[1031] andererseits, weil die Merkmale zumindest nicht im Sinne einer Bindung des nachfolgenden Bundesgesetzes festgelegt sind.

Im Ergebnis ist § 1 Abs. 4 Satz 1 PersAuswG ohne jede Rechtswirkung: Vor und nach seiner Einführung ist eine Erweiterung der Personalausweisdaten um biometrische Merkmale unzulässig. § 1 Abs. 5 Satz 1 PersAuswG ist hingegen zwar eine zutreffende Formulierung der verfassungsrechtlichen Anforderung einer gesetzlichen Ermächtigungsgrundlage. Er ist jedoch keinesfalls selbst Maßstab für eine solche Regelung, weil aufgrund der lex posterior-Regel[1032] eine einfachgesetzliche Selbstbindung des Gesetzgebers für die Zukunft nicht möglich ist. Da es sich bei § 1 Abs. 5 Satz 1 PersAuswG um ein einfaches, jederzeit änderbares Gesetz handelt, das bereits durch ein später folgendes, gegenteilig lautendes Gesetz verdrängt würde, ist auch diese Regelung ohne rechtliche Wirkung. Das zeigt sich bei den parallelen Normen in Passgesetz: § 4 Abs. 3 und 4 PassG sind durch die Verordnung (EG) Nr. 2252/2004[1033] hinfällig. Deutschland ist wegen der unmittelbaren Geltung der Verordnung auch ohne weitere Entscheidung des Bundestages zur Einführung von Gesichts- und Fingerabdrucksdaten in den Reisepass verpflichtet.[1034]

Aus materiellrechtlicher Sicht sind § 1 Abs. 4 Satz 1 und Abs. 5 Satz 1 PersAuswG im günstigsten Fall überflüssig, ansonsten aber schädlich, da sie in gesetzestechnischer Hinsicht vorgeben, Sicherungsmittel zu sein, ohne jedoch wirklich diese Wirkung zu haben. Ihre Verabschiedung erklärt sich daraus, dass nach den Anschlägen des 11. September

---

1028 *Albrecht* 2003a, 188; *Golembiewski/Probst* 2003, 49, 57; ähnlich *TAB* 2004, 48 („Festlegung auf das Erfordernis einer gesetzlichen Grundlage“).

1029 *TAB* 2002, 7.

1030 BT-Drs. 14/7386, 37 (Hervorhebungen hinzugefügt).

1031 Dies unter der Prämisse, dass die Einführung an sich verfassungsmäßig ist. Zumindest hat das Terrorismusbekämpfungsgesetz aber die verfassungsrechtliche Bewertung nicht verändert.

1032 S. *Röhl* 1994, 601.

1033 Vgl. oben 3.1.2.

1034 Dieser „Umweg“ über die Rechtsetzung durch die EU ist angesichts der Regelung in § 4 Abs. 4 Satz 1 PassG bedenklich, wonach (wie beim Personalausweis) die weiteren Einzelheiten des Grundrechtseingriffs durch Bundesgesetz geregelt werden. Die Verordnung wurde im Verfahren nach Art. 67 EGV, d.h. unter bloßer Anhörung des Europäischen Parlaments (und gegen dessen Votum, s.o. 3.1.2) durch den Rat beschlossen. Wegen dessen umstrittener demokratischer Legitimation (s. dazu *Fischer* 2001, 112 ff. et passim) ist es zumindest problematisch, wenn auf diesem Wege grundsätzliche Modalitäten eines Eingriffs in Grundrechte beschlossen werden. Entsprechend der Begrenzung des Themas der Arbeit auf den Personalausweis bleibt dieser Aspekt im Folgenden außer Betracht; vgl. näher *Roßnagel/Hornung*, DÖV 2005, i.E.

2001 eine politische Mehrheit für eine Aufnahme biometrischer Daten in Ausweisdokumente vorhanden war, in der Eile der Zeit aber keine konkreten Umsetzungsentscheidungen treffen konnte oder wollte. Das rechtfertigt es aber nicht, politische Absichtserklärungen in Gesetzesform zu gießen.[1035] In jedem Fall führt diese Vorgehensweise zu einer Verwirrung über die tatsächliche Rechtslage hinsichtlich der Zulässigkeit biometrischer Daten im Personalausweis.

Eine zu schaffende formelle gesetzliche Grundlage müsste zunächst die eigenständige Entscheidung des Gesetzgebers darüber enthalten, dass biometrische Daten in den Personalausweis aufgenommen werden. Eine Formulierung wie in § 1 Abs. 4 Satz 1 PersAuswG (wonach der Ausweis diese enthalten „darf") ist zu vermeiden, weil sie dahingehend verstanden werden könnte, dass die Entscheidung über die Einführung auf die Exekutive übertragen wird. Dies wäre jedoch unzulässig.[1036]

Des Weiteren ist die Art der Daten genau gesetzlich zu regeln. Hier nennt das Personalausweisgesetz bislang „Merkmale von Fingern oder Händen oder Gesicht" (§ 1 Abs. 4 Satz 1 PersAuswG). Eine solche Formulierung schließt schon rein sprachlich eine Kombination mehrerer Merkmale aus.[1037] Falls kombinierte Verfahren zum Einsatz kommen sollten, müsste dies in einem zukünftigen Gesetz klargestellt werden.

Fraglich ist weiterhin, ob die bisherige Formulierung auch eine Verwendung der Iris mit umfasst. Es ließe sich vertreten, dass das Tatbestandsmerkmal „Gesicht" auch die Iris einschließe.[1038] Dagegen spricht aber, dass es sich um grundlegend verschiedene Methoden handelt. Gesichtserkennungsverfahren arbeiten auf sehr unterschiedliche Art und Weise, im Regelfall jedoch mit lokalen Merkmalen, die an bestimmten Punkten im Gesicht bestimmt werden.[1039] Beim Iris-Scan werden dagegen charakteristische Merkmale wie die Corona, Krypten, Fasern, Flecke, Narben, radiale Furchen und Streifen berücksichtigt.[1040] Zwar ist nicht auszuschließen, dass derartige Verfahren in Zukunft in die Gesichtserkennung integriert werden können. Zum gegenwärtigen Zeitpunkt handelt es sich jedoch um zwei verschiedene Techniken. Darüber hinaus haben diese aus datenschutzrechtlicher Sicht grundlegend unterschiedliche Implikationen insbesondere auf der Ebene des Mitwirkungserfordernisses beim Betroffenen. Da das Gesicht selbst Gegenstand biometrischer Erfassung ist, kann der Begriff des „Gesichts" auch nicht als Oberbegriff für ebendieses Verfahren und den Iris-Scan interpretiert werden. Sollte deshalb letzterer beim digitalen Personalausweis eingesetzt werden, müsste dies gesetzgeberisch klargestellt werden.[1041]

Neben der Entscheidung über die Einführung selbst und die Auswahl des Merkmals muss eine zukünftige gesetzliche Grundlage die Speicherungsform der biometrischen Daten (Volldatensatz oder Templates), ihren Speicherungsort (auf der Karte; ob – und wenn ja – wo und in welcher Form in staatlichen Dateien),[1042] die weitere Verwendung im Rahmen von Kontrollen und eventuelle Zugriffsrechte in einem Parlamentsgesetz re-

1035 Zur Kritik am überschnellen Gesetzgebungsverfahren s.a. *Koch* 2002, 33; *Schaar*, MMR 2001, 713 f.
1036 So auch *Koch* 2002, 8 f.
1037 Auch ausweislich der Gesetzesbegründung sind die genannten Merkmale „alternativ" zu sehen, s. BT-Drs. 14/7386, 37; ebenso *Golembiewski/Probst* 2003, 50 f.
1038 So *Stock* 2002, 7.
1039 S. *Breitenstein* 2002, 41; *Woodward/Orlans/Higgins* 2003, 72 ff.
1040 *Breitenstein* 2002, 47; *TAB* 2002, 15.
1041 *Roßnagel/Hornung*, in: Reichl/Roßnagel/Müller 2005, 119; *dies*., DuD 2005, 69; ebenso *Golembiewski/Probst* 2003, 49 f.; *Konferenz der Datenschutzbeauftragten* 2002, unter 2.5; *Der Landesbeauftragte für den Datenschutz Brandenburg* 2002, 20.
1042 Eine derartige Speicherung außerhalb des Ausweises ist allerdings unzulässig, vgl. unten 4.2.2.4.3.

geln.[1043] Nur bei Einhaltung dieser Anforderungen wird dem verfassungsrechtlichen Grundsatz des Gesetzesvorbehalts genüge getan.[1044]

4.2.2.3 Hinlängliche Reichweite der bestehenden Zweckbindung?

Die lebenslange Bindung biometrischer Merkmale an den Betroffenen und die Möglichkeit einer verdeckten Datenerhebung bei nicht mitwirkungsgebundenen Verfahren führen zu besonderen Gefahren der umfassenden Verwendung. Aus diesem Grund sind für biometrische Daten effektive und umfassende Zweckbindungsregeln erforderlich. § 3 Abs. 5 Satz 1 PersAuswG bestimmt, dass die „im Personalausweis enthaltene[n] verschlüsselte[n] Merkmale und Angaben...nur zur Überprüfung der Echtheit des Dokumentes und zur Identitätsprüfung des Personalausweisinhabers ausgelesen und verwendet werden" dürfen.[1045] Von der Regelung sind nicht nur biometrische Daten erfasst, sondern auch weitere Daten, die in verschlüsselter Form im Chip abgelegt werden.

Fraglich ist allerdings, auf welche Daten sich die Zweckbindung erstreckt.[1046] Dafür ist die Bedeutung des Tatbestandsmerkmals „verschlüsselt" maßgebend. Nur hierauf bezieht sich § 3 Abs. 5 Satz 1 PersAuswG. Drei Auslegungen sind denkbar: „Verschlüsselte Merkmale und Angaben" kann bedeuten, dass diese elektronisch signiert werden, nicht visuell erkennbar sind oder kryptographisch verschlüsselt gespeichert werden.[1047]

Die erste Variante scheidet aus, weil bei einer Absicherung der gespeicherten Daten durch eine elektronische Signatur des Ausweisherstellers oder der ausstellenden Behörde nicht die Merkmale und Angaben verschlüsselt gespeichert, sondern diese in Klarform unter Beifügung eines verschlüsselten Hash-Werts abgelegt werden.[1048] Die zweite Auslegung würde bedeuten, dass alle im Chip gespeicherten Daten erfasst wären, nicht allerdings auf der Oberfläche aufgedruckte biometrische Daten. Für eine automatisierte Gesichtserkennung auf der Basis des bisherigen oder eines veränderten Personalausweisbildes (das heißt ohne Chip) würde § 3 Abs. 5 PersAuswG nicht eingreifen.[1049] Ist mit dem Tatbestandsmerkmal dagegen eine Speicherung unter Verwendung kryptographischer Ver-

---

1043 S. *Roßnagel/Hornung*, in: Reichl/Roßnagel/Müller 2005, 120 f.; *dies*., DuD 2005, 69.

1044 Da das Recht auf informationelle Selbstbestimmung unterschiedslos für Deutsche und Ausländer gilt (v. Münch/Kunig-*Kunig*, Art. 2 Rn. 39; *Kunig*, Jura 1993, 595, 598; AK GG-*Podlech*, Art. 2 Abs. 1 Rn. 60 f.), folgt daraus im Übrigen, dass die Übertragung der Ausgestaltungen der biometrischen Verfahren in Aufenthaltstitel und Ausweisersatz (§ 99 I Nr. 13 i.V.m. § 78 Abs. 3 und 6 AufenthaltsG) sowie der Bescheinigung über die Aufenthaltsgestattung (§ 88 Abs. 2 i.V.m. § 63 Abs. 5 AsylVG) auf eine Rechtsverordnung des Bundesministers des Innern verfassungswidrig sind (ebenso *ULD* 2001, 22; *Golembiewski/Probst* 2003, 47 f.). Auch aus Art. 1 der Datenschutzkonvention des Europarats ergibt sich die Verpflichtung, Datenschutz ungeachtet der Staatsangehörigkeit des Betroffenen sicherzustellen (näher *Henke* 1986, 89 ff.). Auf die Regelungen des Terrorismusbekämpfungsgesetzes zum Einsatz von Biometrie bei Ausländern kann hier nicht eingegangen werden, vgl. etwa *Golembiewski/Probst* 2003, 39 ff., 45 ff.; *TAB* 2004, 53 ff.; *Huber*, NVwZ 2002, 787 ff.; *Weichert*, DuD 2002, 423 ff.; *Art. 29 DPWP* 2004.

1045 Zusammen mit dem Verbot einer bundesweiten Datei in § 1 Abs. 5 Satz 2 PersAuswG ergibt sich hieraus eine gesetzgeberische Entscheidung für die Verifikation anstelle der Identifikation, s.o. 2.2.1.5. Für den Reisepass enthält Art. 4 Abs. 3 der Verordnung (EG) Nr. 2252/2004 eine entsprechende Zweckbestimmung, s.o. 3.1.2; *Roßnagel/Hornung*, DÖV 2005, i.E.

1046 Das gilt parallel für das Auskunftsrecht nach § 3 Abs. 5 Satz 2 PersAuswG (s.u. 4.3.7.2), weil beide an dasselbe Tatbestandsmerkmal anknüpfen.

1047 *Golembiewski/Probst* 2003, 54 ff., die allerdings nur (ausführlich) die drei Varianten darlegen und die Frage nicht beantworten, welchen Inhalt die Norm hat.

1048 Zur Funktionsweise der Signatur s.o. 2.3.2; zur Signatur der Ausweisdaten unten 6.2.1.1.

1049 Diese ist nach momentanem Stand der Technik allerdings für den Personalausweis nicht geeignet, vgl. *BSI/BKA/Secunet* 2004, 9 f., 53.

schlüsselungsverfahren gemeint, so sind im Chip gespeicherte (biometrische und andere) Identifikationsdaten dann nicht erfasst, wenn sie dort im Klartext abgelegt werden. Eine Ausnahme könnte für biometrische Templates gelten, sofern diese unter Verwendung kryptographischer Algorithmen bestimmt werden.

Die wörtliche Auslegung des Tatbestandsmerkmals ergibt zunächst, dass sich „verschlüsselt" im allgemeinen Sprachgebrauch auf kryptographische Verfahren bezieht. Andernfalls würde man eher von „verborgen" als von „verschlüsselt" sprechen. Die Gesetzesbegründung ist an dieser Stelle unklar. Sie nennt lediglich die Notwendigkeit, zusätzliche biometrische Merkmale aufzunehmen und diese sowie die übrigen Angaben auch in verschlüsselter Form zu integrieren. Danach heißt es in der Begründung in wörtlicher Wiederholung des Gesetzestextes, diese dürften „nur zur Überprüfung der Echtheit des Dokuments und zur Identitätsprüfung...ausgelesen und verwendet werden".[1050] Diese Formulierung zur Reichweite der Zweckbindung kann sich sowohl auf den gesamten vorherigen Satz als auch lediglich auf die im zweiten Halbsatz angesprochenen verschlüsselten Merkmale beziehen.

Sinn und Zweck von § 3 Abs. 5 Satz 1 PersAuswG ist es, die verfassungsrechtlich gebotene Zweckbindung und Transparenz bei der Verwendung insbesondere sensibler Daten sicherzustellen. Wenn man aber unter „verschlüsselt" lediglich kryptographisch verarbeitete Daten verstünde, hätte dies zur Folge, dass diese datenschutzrechtlich weniger problematische Form der Speicherung biometrischer Daten einer engen Zweckbindung unterläge, die weitaus gefährlichere Variante der Speicherung im Klartext jedoch nicht. Dieses Ergebnis widerspricht in grobem Maße dem Zweckbindungsprinzip. Da dieses verfassungsrechtlich begründet ist,[1051] muss in Anwendung des Gebots verfassungskonformer Auslegung[1052] eine weite Interpretation von § 3 Abs. 5 Satz 1 PersAuswG gewählt werden, die alle nicht unmittelbar wahrnehmbaren Daten in den Anwendungsbereich fallen lässt.[1053] Etwas anderes würde nur gelten, wenn hierdurch absolute Auslegungsgrenzen, insbesondere die des noch möglichen Wortsinns,[1054] verletzt würden. Da der Wortlaut der Norm jedoch – wie beschrieben – unklar ist, greift diese Ausnahme nicht ein. Allerdings sollte die Vorschrift aus Gründen der Gesetzesklarheit dahingehend abgeändert werden, dass alle biometrischen Daten im Ausweis ausschließlich zur Überprüfung der Echtheit des Dokumentes und zur Identitätsprüfung des Personalausweisinhabers ausgelesen und verwendet werden dürfen.

4.2.2.4 Fragen der Verwendung biometrischer Daten

4.2.2.4.1 Rechtliche Kriterien für die Merkmalsauswahl

Die Wahl des biometrischen Merkmals kann nur in einer Gesamtschau aus rechtlichen Anforderungen, technischen Umsetzungsmöglichkeiten und finanzieller Machbarkeit getroffen werden. Aus rechtlicher Sicht sind dabei aufgrund des Verhältnismäßigkeitsprinzips insbesondere hinreichend niedrige Fehlerraten (Eignung des Eingriffs) und eine mög-

1050 BT-Drs. 14/7386, 48.
1051 S.o. 4.2.1.2.2.
1052 S. dazu allgemein *Zippelius* 2005, 41, 53; *Rüthers* 2005, 488 ff.; *Lüdemann*, JuS 2004, 27 ff. m.w.N. (s. zur dogmatischen Begründung ebd., 29).
1053 Vgl. *Roßnagel/Hornung*, in: Reichl/Roßnagel/Müller 2005, 140.
1054 S. BVerfGE 71, 115; 87, 224; 90, 263 (275); *Zippelius* 2005, 47; *Rüthers* 2005, 489.

lichst geringe Beeinträchtigung des Grundrechts auf informationelle Selbstbestimmung (Erforderlichkeit des Eingriffs) entscheidend.[1055]

4.2.2.4.1.1 Hinreichend niedrige Fehlerraten

Um zur Verbesserung der Fälschungs- und Identifikationssicherheit geeignet zu sein, darf das biometrische Ausweisprüfsystem in der konkreten Einsatzumgebung (stationäre und mobile Kontrollstellen, widrige Umweltbedingungen, etc.) nur geringe Fehlerraten aufweisen.[1056] Die Falschakzeptanzrate darf nicht zu hoch sein, weil sich der kontrollierende Beamte sonst nicht auf ein positives Matchingergebnis verlassen könnte und eine zu hohe Zahl von Nichtberechtigten passieren würde. Eine hohe Falschrückweisungsrate stellt demgegenüber zwar kein Sicherheitsproblem dar. Je mehr Ausweisinhaber jedoch fälschlicherweise vom System abgelehnt werden, desto häufiger sind manuelle Nachkontrollen erforderlich. Bereits bei Fehlerraten, die für heutige Systeme durchaus ambitioniert sind, kann es schnell zu hohen Fallzahlen kommen. Die zeigt folgendes Beispiel: Im Jahre 2002 wurden am Frankfurter Flughafen 48,2 Millionen Gäste (ohne Transitreisende) abgefertigt.[1057] Wären sie mittels eines biometrischen Systems kontrolliert worden, welches 1 % fälschlicherweise abgelehnt hätte, so wären – bei einem Anteil der Reisenden in Mitgliedstaaten des Schengen-Acquis, die keinen Ausweis vorzeigen müssen, von 28,9 % – über 340.000 Fehlalarme pro Jahr, das heißt 939 Fehlalarme pro Tag, verursacht worden. Die Fallzahlen sind noch höher, wenn man berücksichtigt, dass im Interesse der Flugsicherheit Reisende in Schengen-Staaten zumindest beim Einchecken ebenfalls ihre biometrischen Daten präsentieren sollten. Werden schließlich Falschabweisungsraten von bis zu 10 % als „eindrucksvoll gering“ bezeichnet,[1058] so muss man sich vor Augen führen, dass dies allein am Frankfurter Flughafen zu einer täglichen Zahl von Fehlalarmen im fünfstelligen Bereich führen würde.

Aufgrund der Unzulässigkeit zentraler biometrischer Datenbanken im System des digitalen Personalausweises[1059] ist für die folgenden Erörterungen nicht die Eignung biometrischer Verfahren zur Identifikation, sondern nur zur Verifikation maßgeblich. Es sei deshalb nur angemerkt, dass aufgrund der Fehleranfälligkeit, der Dauer des Matchingprozesses und der Kosten die Identifikation zumindest gegenwärtig für Massenverfahren, etwa an der Grenze, nicht geeignet ist.[1060] Insbesondere die Gesichtserkennung wurde sowohl vom Bundesamt für Sicherheit in der Informationstechnik,[1061] als auch im Rahmen des Face Recognition Vendor Tests 2002[1062] für einen Abgleich mit großen Datenbanken im Identifikationsmodus als gegenwärtig nicht brauchbar bewertet.

Um eine geringe Fehleranfälligkeit zu gewährleisten, sind zunächst hohe Anforderungen an das Enrolment zu stellen, weil die Qualität der dabei gewonnenen Referenzdaten großen Einfluss auf die Fehlerraten hat.[1063] Für diese Raten lassen sich allerdings kaum feste Obergrenzen der verfassungsrechtlichen Eignung festlegen. Als Richtwerte dürften

---

1055 Vgl. zusammenfassend und aus mehr internationaler Perspektive *Hornung* 2004b, 50 f.

1056 S. zum Folgenden *Roßnagel/Hornung*, in: Reichl/Roßnagel/Müller 2005, 121 f.; 226 f.; *dies*., DuD 2005, 69.

1057 Zahlen laut Auskunft von *P. Schmidt*, Fraport AG, v. 11.4.2003.

1058 So *TAB* 2004, 37.

1059 Diese ergibt sich de lege lata aus § 1 Abs. 5 Satz 2 PersAuswG, ist jedoch auch verfassungsrechtlich begründet, s.u. 4.2.2.4.3.

1060 *International Biometric Group* 2003, 5.

1061 Vgl. *BSI* 2003, 10.

1062 Vgl. *Phillips*/*Grother*/*Micheals*/*Blackburn*/*Tabassi*/*Bone* 2002.

1063 *Albrecht* 2001, 57; *Kuip* 2002, 374; *Nolde* 2002, 22; *JRC/IPTS* 2005, 46.

wohl eine FAR und FRR von 1 % gelten.[1064] Jenseits dieser Werte kann kaum von einer Eignung gesprochen werden. Die hoheitliche Identifizierung ist damit grundsätzlich anders zu behandeln als biometrische Anwendungen im Freizeitbereich. Hier überwiegt der Gesichtspunkt der Nutzerfreundlichkeit,[1065] der für eine Systemkonfiguration im niedrigen FRR-Bereich spricht. Gleichzeitig ist eine hohe FAR hinnehmbar, weil es sich nicht um Hochsicherheitsanwendungen handelt und deshalb eine Falschakzeptanz für die Betreiber akzeptabel, gleichzeitig Überwindungsversuche aufgrund der niedrigen Anreize wenig wahrscheinlich sind.

Eine Bewertung der Leistungsfähigkeit biometrischer Verfahren und Systeme für Chipkartenausweise ist aus mehreren Gründen nur schwer möglich:

- Zunächst mangelt es an einheitlichen Testkriterien für die Beurteilung der Leistungsfähigkeit biometrischer Systeme.[1066]
- Sodann ist den Angaben der Hersteller über die Zuverlässigkeit meist mit Vorsicht zu begegnen.[1067] Nach Aussage des Bundesamt für Sicherheit in der Informationstechnik waren etwa im Projekt BioFace „die Erkennungsleistungen...bei weitem nicht so gut wie sie die Werbung der Systemhersteller ihnen zubilligt[e].“[1068]
- Des Weiteren können Fehlerraten desselben Systems in unterschiedlichen Einsatzbedingungen erheblich voneinander abweichen. Wenn ein System für eine Gruppe von interessierten, technisch kompetenten Personen unter 40 Jahren geeignet ist, die es täglich verwenden, so indiziert dies nicht automatisch die Eignung bei Menschen, die älter sind, der Technik gegenüber Vorbehalte haben und ihr Merkmal nur im Abstand von mehreren Jahren präsentieren. Der digitale Personalausweis muss jedoch auch in diesen Bevölkerungsgruppen einsetzbar sein.
- Deshalb haben auch Pilotprojekte, die mit freiwilligen Probanten arbeiten, nur geringe Aussagekraft für die Einsetzbarkeit biometrischer Systeme in der Gesamtbevölkerung. Das trifft auf die allermeisten bisherigen Testreihen zu. Im Projekt BioP I wurde beispielsweise mit 241 freiwilligen Probanden (Mitarbeiter des Bundeskriminalamts) gearbeitet, die zu 95 % im Alter zwischen 25 und 59 Jahren und überdurchschnittlich gut ausgebildet waren.[1069] Echte Erkenntnisse könnten dagegen beispielsweise aus dem Iris-Scan Programm des UN-Flüchtlingskommissariats in Pakistan gewonnen werden, weil dort tatsächlich ein Querschnitt der Bevölkerung in das System aufgenommen wird.[1070]
- Für die Mehrzahl der Bürger, die ihren Ausweis eher selten einsetzen, fällt überdies der Lerneffekt meist weg. Bei einer Vielzahl von Verfahren ist eine Einlernphase jedoch von entscheidender Bedeutung für den fehlerfreien Betrieb.[1071] Es gibt von

1064 *Roßnagel/Hornung*, in: Reichl/Roßnagel/Müller 2005, 121 f.; *dies*., DuD 2005, 69.
1065 *Albrecht* 2001, 61.
1066 *Albrecht* 2003a, 60; *dies*. 2001, 75 f. m.w.N.; s.a. unten 6.1.3, dort auch zu bisher aufgestellten Kriterien; zum Forschungsbedarf vgl. *Rejman-Greene* 2003a, 11 ff.
1067 Vgl. etwa die Bsp. bei *Albrecht* 2001, 39; *Breitenstein* 2002, 39; s.a. *TeleTrusT* 2002, 9. Bisweilen erfolgen nur Angaben zu einer Fehlerrate (FAR oder FRR), die ohne die jeweils andere Rate keinen Vergleich zulassen.
1068 *BSI* 2003, 9.
1069 *BSI/BKA/Secunet* 2004, 21. Auch das Pilotprojekt zur irisgestützten Grenzkontrolle am Frankfurter Flughafen setzt Freiwillige ein, s. http://www.bundesgrenzschutz.de/Auto_Grenzkontrolle/ndex.php.
1070 Die Ergebnisse des Programms sind noch nicht verfügbar, es werden jedoch eine FER und eine FRR von je 0,9 % genannt, s. *Woodward/Orlans/Higgins* 2003, 288.
1071 *Ashbourn* 2000, 95 ff.; *Albrecht* 2002c, 139 f.; *dies.* 2001, 57; *Schnabel*, Spektrum der Wissenschaft 7/2003, 79; *Woodward/Orlans/Higgins* 2003, 41; *Reid* 2004, 207 ff.

Seiten der Anwender immer wieder Berichte, wonach biometrische Systeme zwar nach einer Zeit der Eingewöhnung und Schulung reibungslos ablaufen, in der Anfangsphase jedoch erhebliche Probleme auftreten.[1072] Aus diesem Grund ist auch der Aussagewert von Pilotprojekten mit Vielfliegern und anderen Probanden, die häufig Grenzkontrollen passieren, sehr begrenzt (selbst wenn es sich dabei um einen repräsentativen Querschnitt handeln würde). Der durchschnittliche Ausweisinhaber wird das biometrische System nicht so häufig nutzen. Das kann sowohl die Fehlerraten als auch den Zeitaufwand an der Grenze erhöhen. Der Verweis darauf, durch Anwenderschulungen könnten Fehlerraten bei Ausweisdokumenten verbessert werden,[1073] geht deshalb ebenso fehl wie die Feststellung, die Gesamtfehlerraten des Projekts BioP I seien niedriger, wenn man die ersten drei Wochen der Feldtestphase unberücksichtigt lasse.[1074] Für die Abschätzung der Fehlerraten eines biometrischen Ausweissystems sind vielmehr die ersten Tage eines solchen Feldtests die aussagekräftigsten, weil die Mehrzahl der Ausweisinhaber sich bei der Kontrolle nicht mehr an die Handhabung des Systems erinnern wird.

Wenn an dieser Stelle einige Fehlerraten genannt werden, so sind diese dementsprechend mit großer Vorsicht zu betrachten. Nichtsdestotrotz sind die referierten Ergebnisse zumindest für die Einschätzung der Größenordnung der Fehleranfälligkeit von Interesse. Betrachtet werden nur die drei national und international favorisierten Merkmale Iris, Fingerabdruck und Gesicht. Verallgemeinernd lässt sich sagen, dass die Fehleranfälligkeit in eben dieser Reihenfolge zunimmt:

- Bei der Iris liegt die Wahrscheinlichkeit, für zwei Betroffene dasselbe Template zu errechnen bei $1:10^{78}$. Dies ist zumindest die Eigenangabe des Patentinhabers *Daugman*.[1075] Fehlerraten werden mit 0,01 - 1,0 % (FAR) und 0,1 - 2,0 % (FRR) angegeben.[1076] Bisweilen wird auch betont, es sei noch nie eine Falschakzeptanz eines Iriserkennungssystems beobachtet worden.[1077] In jedem Fall schneidet die Iriserkennung damit bezüglich der Leistungsfähigkeit in Vergleichstest durchgängig am besten ab.[1078]
- Der Fingerabdruck ist das Verfahren, bei dem die größten Erfahrungen vorliegen.[1079] Das Büro für Technikfolgenabschätzung nennt für eine FAR von 0,01 % eine FRR von 5 %.[1080] Die unabhängige vergleichende Fingerprint Verification Competition kam im Jahre 2002 zu dem Ergebnis, dass Equal Error Rates um 1 %

1072 Im Projekt BioP I gingen bspw. die Fehlerraten in den ersten drei Wochen signifikant zurück, s. *BSI/BKA/Secunet* 2004, 54; s.a. *Rejman-Greene* 2003b, 131.

1073 *Booz Allen Hamilton/Bundesdruckerei/ZN Vision* 2003, 70 (zitiert nach *TAB* 2004, 32). Das gilt zumindest dann, wenn man den Hinweis auf die Schulung der Merkmalsträger bezieht. Eine Schulung des Kontrollpersonals trägt selbstverständlich zur Senkung von Fehlerraten bei.

1074 *BSI/BKA/Secunet* 2004, 63.

1075 Vgl. *Breitenstein* 2002, 49.

1076 *TAB* 2002, 20. Andere Feldtests ergaben eine FRR zwischen 1,9 und 6 %, s. *Fenner* 2003 (dort allerdings ohne Angabe einer FAR); s.a. *Bolle/Connell/Pankanti/Ratha/Senior* 2004, 114 f.

1077 S. etwa *Daugman* 2001, 131; *Kuip* 2002, 373. Ob das zutrifft, ist indes schwer zu beurteilen.

1078 S. etwa *Mansfield/Kelly/Chandler/Kane* 2001, 10 f.; *Woodward/Orlans/Higgins* 2003, 93; *JRC/IPTS* 2005, 93 f. Ein Grund ist die hohe Unterscheidbarkeit. Die Iris ist ein phänotypisches Merkmal, sodass sich sogar rechtes und linkes Auge eines Menschen voneinander unterscheiden, s. *Breitenstein* 2002, 47; *Daugman* 2001, 143 f.

1079 *Breitenstein* 2002, 35; *Woodward/Orlans/Higgins* 2003, 64; *Bolle/Connell/Pankanti/Ratha/Senior* 2004, 146.

1080 *TAB* 2002, 20.

erreichbar seien.[1081] 90 Studenten der Universität von Bologna (mit einem Altersdurchschnitt von 20 Jahren) gaben ihre Fingerabdrücke zum Testen der Algorithmen ab. Hieran zeigt sich allerdings erneut der eingeschränkte Wert derartiger Studien. Das Projekt BioFinger zeigte denn auch, dass nur die besten 8 % der am Markt verfügbaren Systeme eine EER von unter 1 % aufwiesen.[1082]

- Bei Gesichtserkennungsverfahren stellte der aus dem Jahre 2002 stammende Face Recognition Vendor Test für das beste System bei einer FAR von 1 % eine FRR von 10 % fest.[1083] Allerdings stieg diese im Außenbereich auf 50 % an.[1084] Deshalb dürften mobile Kontrollstellen der Sicherheitsbehörden unrealistisch sein. Bei Grenzstationen ist zu unterscheiden: Während im Flughafenbereich der Lichteinfall kontrollierbar ist, ist dies an Grenzstationen zu Land kaum zu bewerkstelligen, weil dazu beispielsweise jeder PKW-Fahrer aus seinem Fahrzeug aussteigen müsste. Für die Fehlerraten ergab die Studie BioP I, dass herstellerabhängige Templates signifikant besser abschneiden als Volldaten.[1085]

Die Gesichtserkennung weist danach die höchsten Fehlerraten auf. Die Unterschiede sind zumindest im Außenbereich so signifikant, dass die Aussage, die augenblicklich erreichbare Leistung von Fingerabdrucks- und Gesichtserkennungsverfahren bei Verifikationsanwendungen sei ungefähr gleich einzustufen,[1086] nicht zutreffend ist. Auch im hoheitlichen Bereich kamen Feldversuche für die biometrische Verwendung des Gesichts zu sehr zweifelhaften Ergebnissen. So wurde das Pilotprojekt zur elektronischen Passbild-Überprüfung von Flugreisenden am Nürnberger Flughafen gestoppt, weil nach Aussage eines Sprechers des bayerischen Innenministeriums das geschulte Auge des Polizisten mehr leistete als das Identifikationssystem.[1087] Feldversuche in den USA am Flughafen Boston ergaben, dass die Gesichtserkennungssysteme nicht gut genug arbeiteten, um ein effektives Sicherheitsinstrument sein zu können.[1088] Die Fehlerraten waren offenbar so hoch, dass die Evaluationsergebnisse über ein Jahr geheim gehalten wurden.[1089] Das automatisierte Gesichtserkennungssystem in Tampa (Florida), das erste seiner Art in den USA, wurde nach zwei Jahren eingestellt, weil es zu keiner einzigen Verbrechererkennung führte.[1090] Hinsichtlich der Alterungsprozesse beim Gesicht gibt es widersprüchliche Ergebnisse. Das Bundesamt für Sicherheit in der Informationstechnik stellte in der Studie BioFace zwar ein Absinken der Matchingscores fest, beurteilte dies jedoch als für den Verifikationsmodus nicht erheblich.[1091] Die ICAO hat demgegenüber festgehalten, dass die Leis-

1081 S. die Ergebnisse unter http://bias.csr.unibo.it/fvc2002/. Der Wettbewerb wurde vom Biometric System Lab der Universität Bologna, dem U.S. National Biometric Test Center der San Jose State University und dem Pattern Recognition and Image Processing Laboratory der Michigan State University organisiert.

1082 S. *BSI/BKA/IGD* 2004, 2.

1083 *Phillips*/*Grother*/*Micheals*/*Blackburn*/*Tabassi*/*Bone* 2002, 2 f. Das wird von Ergebnissen der US-Einwanderungsbehörde bestätigt, s. http://www.heise.de/newsticker/meldung/34466.

1084 Dies entspricht den Ergebnissen des Projekt BioP I (*BSI/BKA/Secunet* 2004, 10) und Studien des amerikanischen National Institute for Standards and Technology (NIST), s. *Fenner* 2003; zu den relativ hohen Fehlerraten der Gesichtserkennung auch *Breitenstein* 2002, 43 ff.; *Rejman-Greene* 2003b, 93 ff.; *JRC/IPTS* 2005, 55.

1085 *BSI/BKA/Secunet* 2004, 9 f., 49.

1086 *TAB* 2004, 6, 37.

1087 Vgl. http://www.heise.de/newsticker/meldung/35464; *Golembiewski/Probst* 2003, 16 f.

1088 S. http://www.aclu.org/Privacy/Privacy.cfm?ID=13430&c=130.

1089 S. *Jodda* 2003; http://futurezone.orf.at/futurezone.orf?read=detail&id=183269&tmp=1623.

1090 http://www.heise.de/newsticker/meldung/39635.

1091 *BSI* 2003, 7.

tungsfähigkeit von Gesichtserkennungssystemen in erheblichem Umfang von Alterungseffekten abhängt.[1092] Auch der erwähnte Face Recognition Vendor Test kommt zu dem Ergebnis, dass selbst bei den besten Systemen ein Absinken der Erkennungsrate von 5 % pro Jahr zu erwarten ist.[1093] Dies dürfte die höchste Rate unter den drei Merkmalen sein[1094] und zumindest bei der gegenwärtigen Laufzeit des Personalausweises von zehn Jahren zur Ungeeignetheit des Gesichtes als biometrisches Merkmal führen. Das Bundesamt für Sicherheit in der Informationstechnik kam im Jahre 2003 insgesamt zu dem Ergebnis, die Tauglichkeit der getesteten Gesichtserkennungssysteme zur Verifikation sei nicht beweis- oder widerlegbar.[1095]

Im Ergebnis scheinen Einschätzungen gerechtfertigt, nach denen die Zuverlässigkeit biometrischer Systeme bisher noch nicht seriös abschätzbar ist,[1096] bislang keines der eingesetzten Verfahren alle Anforderungen der Praxis erfüllt,[1097] noch keine allgemeingültigen Evaluierungskriterien existieren,[1098] und bisher vorliegende Studien häufig unvollständig, vorläufig, subjektiv und nicht überprüfbar sind.[1099] Auf dieser Basis wäre – auch unter Berücksichtigung einer Einschätzungsprärogative des Gesetzgebers hinsichtlich der Eignung einer Maßnahme – die Einführung eines biometrischen Verfahrens bei Chipkartenausweisen unzulässig.

Grundvoraussetzung für diese Einführung ist jedenfalls ein groß angelegter und wissenschaftlich begleiteter Feldversuch,[1100] weil es bislang für kein Merkmal praktische Erkenntnisse über Fehlerraten im Betrieb mit Teilnehmerzahlen im zweistelligen Millionenbereich gibt. Testserien wie das Projekt BioP I, das auf den Ergebnissen von 241 Teilnehmern aufbaut, von denen letztlich 152 in die statistische Auswertung gelangten, können ein erster Schritt sein. Diese Testpopulation jedoch als „schon relativ groß“[1101] zu bezeichnen, verkennt die Dimension der Einsatzbedingungen für einen digitalen Personalausweis.

Falls sich im Ergebnis keines der Verfahren als hinreichend geeignet erweisen sollte, ergeben sich weitere Möglichkeiten durch die Kombination mehrerer biometrischer

---

1092 Vgl. das Papier der Tagung in Kairo im Frühjahr 2004, http://www.icao.int/icao/en/atb/fal/fal12/documentation/fal12wp063_en.pdf.

1093 *Phillips*/*Grother*/*Micheals*/*Blackburn*/*Tabassi*/*Bone* 2002, 2. Auch in der Studie BioP I wurde ein Abnehmen der Erkennungsleistung mit zunehmendem Ausweisalter festgestellt, s. *BSI/BKA/Secunet* 2004, 11, 70.

1094 Dagegen soll nach *TAB* 2004, 6, 33 die Langzeitstabilität des Fingerabdrucks „aufgrund bestimmter Einschränkungen kritisch zu beurteilen“ sein. Die Einschränkungen werden allerdings nicht genannt. Nach den Ergebnissen des Projekts BioFinger könnte es alle zehn Jahre zu einer Verdoppelung der Fehlerraten kommen, s. *BSI/BKA/IGD* 2004, 3, 88 ff. Die Datenbasis war aber zu klein, um belastbare Aussagen treffen zu können, vgl. ebd., 97.

1095 *BSI* 2003, 7.

1096 *TAB* 2002, 4, 49; *Konferenz der Datenschutzbeauftragten* 2002, unter 3.2; ähnlich *Albrecht* 2003a, 51.

1097 *TAB* 2002, 4, 9. Kriterien waren Universalität, Einzigartigkeit, Beständigkeit und Erfassbarkeit für die biometrischen Merkmale, sowie technische Umsetzbarkeit, Robustheit, Empfindlichkeit, Überwindungsresistenz, ökonomische Machbarkeit und Nutzerfreundlichkeit für die Verfahren und Systeme.

1098 Roßnagel-*Gundermann/Probst*, Kap. 9.6, Rn. 17; *TAB* 2002, 5 f.; zu ersten Ansätzen s. *Munde* 2002, 145 ff.; *Albrecht* 2002c, 135 f.; *Bolle/Connell/Pankanti/Ratha/Senior* 2004, 105 ff. m.w.N.

1099 *TAB* 2002, 21; *Konferenz der Datenschutzbeauftragten* 2002, unter 3.2; s.a. *OECD* 2004, 18 m.w.N.

1100 *Konferenz der Datenschutzbeauftragten* 2002, unter 8; *Roßnagel/Hornung*, in: Reichl/Roßnagel/Müller 2005, 227; *dies*., DuD 2005, 69, 70; für die USA *International Biometric Group* 2003, 2; dies ist auch die Auffassung der Bundesregierung, s. Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten *Jelpke* und der Fraktion der PDS, BT-Drs. 14/8839, 3 f.; zu den Problemen großer Nutzergruppen vgl. *Rejman-Greene* 2003b, 79 ff.

1101 *BSI/BKA/Secunet* 2004, 62.

Merkmale auf einem Ausweisdokument.[1102] Dies bringt zwar die Nachteile höherer Anforderungen an den verwendeten Chip und einer Verdoppelung der Infrastruktur zum Enrolment und zum Matching mit sich. Gleichzeitig kann jedoch die Eignung des Gesamtsystems verbessert werden. Die Verordnung (EG) Nr. 2252 vom 13. Dezember 2004[1103] schreibt für den europäischen Reisepass die Verwendung von Gesichts- und Fingerabdrucksdaten vor, und das National Institute for Standards and Technology (NIST) hat der US-Regierung dasselbe empfohlen.[1104]

Kombiniert man zwei biometrische Verfahren zu einem Gesamtsystem, so sind die Fehlerraten der Einzelverfahren mathematisch zwei unabhängige Variablen. Die Auswirkungen auf das Erkennungsverfahren richten sich danach, ob man für eine erfolgreiche Prüfung eine oder zwei biometrische Übereinstimmungen verlangt. In letzterem Fall sind die Fehlerraten der beiden Systeme miteinander zu multiplizieren. Haben zum Beispiel beide eine FAR von 1 %, so ist die Wahrscheinlichkeit, dass das Gesamtsystem einen unberechtigten Nutzer fälschlicherweise zulässt, nur noch 0,01 %. Gleichzeitig steigt aber die Zurückweisungswahrscheinlichkeit, da bereits eine einzelne Abweisung hierfür ausreicht. Beträgt die FRR der Einzelsysteme zum Beispiel 5 %, so ergibt sich für die FRR des Gesamtsystems bereits ein Wert von 9,75 %. Ebenso wie die FRR verhält sich die Rate derjenigen, die im Gesamtsystem nicht enroled werden können. Auch diese steigt signifikant an.

Unter diesen Umständen dürfte es vorzugswürdig sein, die Erkennung durch eins der beiden Verfahren ausreichen zu lassen. In diesem Fall bestünde auf der individuellen Ebene der Vorteil, dass es sehr wenige Ausweisinhaber geben wird, die für beide verwendeten Merkmale nicht geeignet sind. Gleichzeitig kann die Kontrolle beschleunigt werden, wenn im ersten Zugriff ein ungenaueres, aber schnelleres Verfahren verwendet wird. Erfolgt eine Ablehnung oder soll eine genauere Kontrolle durchgeführt werden, kann auf das zweite, aufwendigere System zurückgegriffen werden.

4.2.2.4.1.2 Geringstmöglicher Eingriff in Grundrechte

Im Rahmen der Erforderlichkeitsprüfung ist zu bestimmen, welches von mehreren gleichermaßen geeigneten Mitteln die geringste Eingriffsintensität aufweist. Da aufgrund des zu erwartenden technischen Fortschritts in absehbarer Zeit mit einer – zumindest grundsätzlichen – Eignung aller drei in Frage kommenden biometrischen Merkmale gerechnet werden kann, ist demnach zu prüfen, welches von ihnen die am wenigsten belastende Alternative ist.

Biometrische Systeme unterscheiden sich dabei in mehrfacher Hinsicht. Drei Hauptkriterien lassen sich ausmachen:[1105]

- Der Eingriff eines Systems in das Grundrecht auf informationelle Selbstbestimmung ist umso stärker, je größer die Gefahr einer Datenerhebung ohne die Mitwirkung und das Wissen des Betroffenen ist, weil dieser so in seinem Verhalten über-

1102 Vgl. zu diesem Aspekt *Roßnagel/Hornung*, in: Reichl/Roßnagel/Müller 2005, 122 f.; 226; *dies*., DuD 2005, 69, 70; *JRC/IPTS* 2005, 65 ff.

1103 S.o. 3.1.2.

1104 S. http://www.heise.de/newsticker/meldung/34466. Auch die *International Biometric Group* (2003, 8 f.) fordert für die USA die Kombination mehrerer Verfahren. Mittlerweile scheint dies auch der Plan der Regierung zu sein, s. http://europa.eu.int/idabc/en/document/3827/194.

1105 S. *Roßnagel/Hornung*, in: Reichl/Roßnagel/Müller 2005, 123 f.; 227 f.; *dies*., DuD 2005, 69, 70; *Hornung* 2004b, 50 f.; *Hornung*, KJ 2004, 344, 352.

wacht werden kann, ohne dass er es bemerkt.[1106] Demzufolge ist bei einer derartigen Datenverwendung auch das Transparenzprinzip betroffen.[1107] Aus diesem Grund sind nicht-kooperative Systeme bedenklicher als kooperative (mitwirkungsgebundene).[1108]

- Ein zweites Kriterium ist die Gefahr überschießender Informationen, die in biometrischen Daten enthalten sein können.[1109] Diese Zusatzinformationen sind zum Vorgang der Authentifikation nicht erforderlich und werden deshalb von biometrischen Systemen im ordnungsgemäßen Betrieb normalerweise nicht weiterverarbeitet. Dennoch verursachen sie Gefahren für die Betroffenen, weil sie zweckentfremdet werden können. Überschießende Informationen führen deshalb zu einer höheren Eingriffsintensität. Zwar ist wissenschaftlich umstritten, inwieweit man aus bestimmten Merkmalen Rückschlüsse auf den Gesundheitszustand vornehmen kann. Außerdem lassen sich in jedem Fall nur bestimmte Korrelationen feststellen; ein direkter Schluss auf eine Krankheit ist nicht möglich.[1110] Andererseits reicht eine hinreichend große Wahrscheinlichkeit einer Erkrankung aus, um für die Betroffenen erhebliche Nachteile zu verursachen. Außerdem könnten die heute gespeicherten Daten bei entsprechendem wissenschaftlichem Fortschritt in der Medizin zukünftig Erkenntnismöglichkeiten über den Gesundheitszustand eröffnen, die heute noch nicht bestehen. Demzufolge sind solche Merkmale vorzuziehen, die keine oder wenig Zusatzinformationen enthalten.
- Biometrische Merkmale unterscheiden sich schließlich hinsichtlich ihrer Flüchtigkeit.[1111] Wird ein Merkmal mehr oder weniger zwangsläufig an Stellen hinterlassen, an denen auch nach längerer Zeit noch eine Überprüfung vorgenommen werden kann, so ist die Eingriffsintensität größer als bei einem flüchtigen Merkmal, das in Abwesenheit des Betroffenen nicht erhoben werden kann.

Betrachtet man unter diesen Kriterien zunächst die Gesichtserkennung, so ist diese ein flüchtiges Merkmal. Aus Gesichtsbildern lassen sich einige Zusatzinformationen gewinnen, beispielsweise das Geschlecht oder die ethnische Zugehörigkeit. Bedenklich ist die Gesichtserkennung insbesondere auch deshalb, weil Gesichtsdaten nicht-kooperativ erhoben werden können. Dies führt zu einem Konflikt mit dem Prinzip der Direkterhebung.[1112]

1106 Einige Anbieter werben sogar explizit mit der Möglichkeit der Verhaltenskontrolle, s. z.B. *G&D* 2003, 3; *Kuip* 2002, 377.

1107 Dieses verlangt im Grundsatz nicht nur eine Erhebung direkt beim Betroffenen, sondern auch, dass dieser hiervon Kenntnis erlangt, s. *Auernhammer*, § 13 Rn. 12; *Bergmann/Möhrle/Herb*, § 13 Rn. 13; Simitis-*Sokol*, § 4 Rn. 20; näher oben 4.2.1.2.5.

1108 *Weichert*, CR 1997, 369, 374; *Köhntopp* 1999, 183; *Konferenz der Datenschutzbeauftragten* 2002, unter 7; *TeleTrusT* 2002, 32; *Nanavati/Thieme/Nanavati* 2002, 246 ff.; *Der Landesbeauftragte für den Datenschutz Brandenburg* 2002, 20 f.; *Golembiewski/Probst* 2003, 53, 64.

1109 *Köhntopp* 1999, 182; *TeleTrusT* 2002, 32; Roßnagel-*Gundermann/Probst*, Kap. 9.6, Rn. 26 f.; *Golembiewski/Probst* 2003, 64 f.; *Albrecht* 2003a, 172; *Art. 29 DPWP* 2003, 7 f. Ein vergleichbares Problem stellt sich bei der Verwendung genetischer Daten im Strafprozess. Das BVerfG hat einen Eingriff in den absolut geschützten Kernbereich des Persönlichkeitsrechts hier ausdrücklich deshalb verneint, weil keine Rückschlüsse auf persönlichkeitsrelevante Merkmale wie Erbanlagen, Charaktereigenschaften oder Krankheiten möglich seien, s. BVerfGE 103, 21 (32). Dies ist allerdings nach neueren Erkenntnissen durchaus zweifelhaft, s. *Faber*, RDV 2003, 278, 280 f. m.w.N.

1110 *Albrecht* 2003a, 173 m.w.N.

1111 *Golembiewski/Probst* 2003, 53.

1112 *Weichert*, CR 1997, 369, 374; *Konferenz der Datenschutzbeauftragten* 2002, unter 7; *Der Landesbeauftragte für den Datenschutz Brandenburg* 2002, 20 f.; *Albrecht* 2003a, 169 ff. m.w.N.; *Golembiewski/Probst* 2003, 53. Dies wird international durchaus anders gesehen; s. etwa die Entscheidung

Es ermöglicht außerdem im Grundsatz den unbemerkten Abgleich mit Datenbanken.[1113] Zwar eignen sich Gesichtserkennungsverfahren bislang noch nicht zum Abgleich mit großen Referenzdatenmengen. Dies spricht gegenwärtig unter Verhältnismäßigkeitsgesichtspunkten für den Einsatz des Gesichts. Die Verwendungsmöglichkeiten werden sich jedoch in Zukunft voraussichtlich ändern. Einige Hersteller werben bereits mit der Möglichkeit einer Identifikation im 1:n Modus.[1114] Damit droht ein Szenario, in dem alle Gesichtsbilder einer größeren Menschenmenge (etwa einer Demonstration) aufgenommen und die Daten mit Datenbanken abgeglichen werden können. Genau an dieser Stelle greift jedoch die Mahnung des Bundesverfassungsgerichts, die Ungewissheit über derartige Datenerhebungen könne die Bürger davon abhalten, ihre Grundrechte wahrzunehmen.[1115] Deshalb ist die Verwendung der Gesichtserkennung grundsätzlich bedenklich.[1116]

Andererseits könnte für das Merkmal „Gesicht" sprechen, dass schon der bisherige Ausweis ein Photo enthält.[1117] Es ließe sich argumentieren, unter Erforderlichkeitsgesichtspunkten sei zunächst dieses Datum einzusetzen; jedes weitere biometrische Datum wäre dann ein nicht erforderlicher zusätzlicher Eingriff. Hierbei wird jedoch übersehen, dass das bisherige Gesichtsbild nicht automatisiert ausgewertet werden kann und für biometrische Verfahren „absolut ungeeignet"[1118] ist. Auch ein biometrisch verbessertes Bild (Frontalaufnahme) ist hierzu wohl nicht, jedenfalls aber signifikant schlechter geeignet als in elektronischer Form gespeicherte Daten.[1119] Die biometrische Verwendung des Gesichts wäre deshalb ebenso wie die des Fingerabdrucks oder der Iris ein zusätzlicher Eingriff in die informationelle Selbstbestimmung.

In der Diskussion wird darüber hinaus des öfteren das Argument vorgebracht, beim Gesicht handele es sich um ein so genanntes „offenes Merkmal", bei dem sich eine Datenerhebung durch Unbekannte praktisch nicht verhindern lasse.[1120] Insofern seien die Daten datenschutzrechtlich wenig oder nicht schutzbedürftig. Diese Ansicht ist jedoch unzutreffend. Das liegt zum einen an der Qualität der Bilder, die beim Enrolment erhoben werden. Hierfür gibt es ausführliche und komplizierte Vorgaben,[1121] die bei Nichteinhaltung zu signifikant höheren Fehlerraten führen. Im Unterschied zu Allerweltsbildern, die tatsächlich relativ problemlos angefertigt werden können, sind Bilder dieses Typs keineswegs „offen". Darüber hinaus verkennt das Argument die datenschutzrechtliche Bedrohungsperspektive. Ein motivierter, mit entsprechenden Ressourcen ausgestatteter Angreifer kann in der Tat auch ein qualitativ hochwertiges Gesichtsbild des Betroffenen erlangen. Insofern stellen biometrische Merkmale kein Geheimnis im eigentlichen Sinne dar. Daraus folgt, dass die Sicherheit biometrischer Verfahren nicht von einer Geheimhaltung biometrischer

---

des amerikanischen Supreme Court *US v Dionisio* 410 US 1 (1973), in der die geheime Aufnahme von Gesicht und Stimme für grundsätzlich zulässig erklärt wurde.

1113 Zwar ist die Einrichtung einer allgemeinen bundesweiten Datei unzulässig, s.u. 4.2.2.4.3. Denkbar wäre aber auch ein Abgleich mit Fahndungsdatenbanken.

1114 S. das Verfahren von NEC, http://www.nec-cebit.com/pdf/Fiore_3D_d.pdf und den Bericht unter http://www.heise.de/newsticker/meldung/45937.

1115 BVerfGE 65, 1 (43); s. dazu oben 4.1.1.2.

1116 *Albrecht/Probst* 2001, 32; *Woodward* 2001, 7 ff.; *Privacy International et. al.* 2004, 2 f.; s. für die USA *Agre* 2003; *McCormack*, B.U. J. Sci. & Tech. L. 2003, 128, 135 ff.; *Nguyen*, Va. J.L. & Tech. 2002, 2 ff.

1117 S. *Golembiewski/Probst* 2003, 61 f.; in dieser Richtung auch *ICAO* 2004a, 17.

1118 *BSI/BKA/Secunet* 2004, 53.

1119 *BSI/BKA/Secunet* 2004, 49. Deshalb ist die Erweiterung des Ausweises um ein Speichermedium erforderlich, s. ebd., 92.

1120 Z.B. *Probst* 2002, 126; *Rankl/Effing* 2002, 511; *Woodward* 2001, 6; *ICAO* 2004a, 17.

1121 Vgl. den Standard ISO/IEC 19794-5; s. näher *Struif/Scheuermann/Küblbeck/Heusinger/Ronge/Schneider/Kitamura*, in: Reichl/Roßnagel/Müller 2005, 81 ff.

Daten abhängen darf.[1122] Das ist aber ein grundlegend anderer Aspekt als die Frage der Möglichkeit eines generellen Überwachungsszenarios. Es ist nämlich unrealistisch, dass ein Datenakquisitionsangriff, wie ihn ein hoch motivierter Angreifer im Einzelfall durchführen wird, auf die ganze, oder einen Großteil der Bevölkerung ausgeübt wird. Würde der digitale Personalausweis dagegen mit Gesichtsdaten arbeiten, so würden Daten der Gesamtbevölkerung in hoher Qualität durch staatliche Stellen erhoben, weiterverarbeitet und zu täglichen Kontrollen genutzt. Hierdurch ergäbe sich bei entsprechendem technischem Fortschritt die Möglichkeit eines Einsatzes als Massenkontrollmittel. Genau darin besteht die datenschutzrechtliche Problematik der Gesichtserkennung.

Der Fingerabdruck ist hingegen ein mitwirkungsgebundenes Merkmal: Eine Datenerhebung an Kontrollstellen ist nicht ohne Kenntnisnahme des Betroffenen möglich. Inwieweit der Fingerabdruck Zusatzinformationen enthält, ist wissenschaftlich umstritten. Genannt werden Zusammenhänge mit chronischen Magen-Darm-Beschwerden, Leukämie, Rubella-Syndrom und Brustkrebs.[1123] Auch sollen Rückschlüsse auf die ethnische Herkunft möglich sein.[1124] Davon abgesehen ist der Fingerabdruck ein nicht-flüchtiges Merkmal: Der Inhaber hinterlässt ihn unwillentlich in seiner Umgebung. Deshalb besteht das Risiko einer Datenerhebung von Abdrücken, die sich auf Alltagsgegenständen befinden. Das ist auch nach längerer Zeit noch möglich.

Die Iriserkennung vermeidet demgegenüber die Hauptnachteile der anderen beiden Verfahren. Sie ist ein flüchtiges Merkmal und gleichzeitig mitwirkungsgebunden. Zwar gibt es inzwischen Systeme, die eine Datenerhebung aus bis zu einem Meter Entfernung zulassen.[1125] Auch hierbei muss der Betroffene jedoch zumindest eine kurze Zeit in einem definierten Abstand in eine vorgegebene Richtung blicken. Eine Erhebung des Merkmals im Vorbeigehen ist nicht möglich. Auf der anderen Seite ist die Iris offenbar[1126] das Merkmal, welches die meisten Zusatzinformationen, insbesondere über den Gesundheitszustand, enthält. Genannt werden Zusammenhänge mit Erkrankungen wie Diabetes, Arteriosklerose und Bluthochdruck.[1127] Aus atypischen Veränderungen der Iris kann außerdem mit einer gewissen Wahrscheinlichkeit auf eine AIDS-Erkrankung und Alkohol- oder Drogenmissbrauch geschlossen werden.[1128] Es erscheint überdies nicht unrealistisch, in Zukunft noch mehr Informationen aus dem Irisbild gewinnen zu können.

Im Ergebnis weist jedes der drei Merkmale ein spezifisches datenschutzrechtliches Risiko auf: Das Gesicht lässt sich ohne Mitwirkung aufnehmen, der Fingerabdruck wird in der Alltagsumgebung hinterlassen, die Iris enthält offenbar die meisten Gesundheitsinformationen. Fingerabdruck und Iris haben den Vorteil, dass sie kein Szenario einer massenhaften Kontrolle zulassen.[1129] Daher erscheint die Verwendung der Iris unter dem Kriterium der Eingriffsintensität vorzugswürdig, weil sie auch die Gefahr einer Rückverfolgbar-

1122 S. *Albrecht/Probst* 2001, 37.

1123 Johns Hopkins Physician Update: Gastoenterology: Fingerprinting GI Disease, S. 5 (zitiert nach: Roßnagel-*Gundermann/Probst*, Kap. 9.6, Rn. 26); *Woodward* 1999, 393; *Woodward/Orlans/Higgins* 2003, 202 f.; s.a. *JRC/IPTS* 2005, 52.

1124 *Gundermann/Köhntopp*, DuD 1999, 143, 150.

1125 *Behrens/Roth* 2001a, 14; *TAB* 2002, 15.

1126 Die Zusammenhänge sind umstritten, ablehnend etwa der Patentinhaber für Iriserkennungssysteme *Daugman* (1999, 117 m.w.N.); s.a. *JRC/IPTS* 2005, 18, 55.

1127 *Woodward* 1999, 393 m.w.N.; *Woodward/Orlans/Higgins* 2003, 203.

1128 *Albrecht* 2003a, 173.

1129 Vgl. für den Fingerabdruck *Konferenz der Datenschutzbeauftragten* 2002, 7.

keit im Einzelfall vermeidet.[1130] Allerdings verringern sich die Unterschiede zwischen den einzelnen Merkmalen durch andere Anforderungen an die Datenverwendung beim digitalen Personalausweis deutlich. Da der Einsatz biometrischer Daten verfassungsrechtlich nur zu rechtfertigen ist, wenn die Daten nach der Produktion des Ausweises umgehend gelöscht werden, keine Speicherung außerhalb des Kartenchips stattfindet[1131] und zum Matching Geräte verwendet werden, die ein Speichern der Daten schon technisch ausschließen,[1132] reduzieren sich die beschriebenen potentiellen Risiken der einzelnen Merkmale. Gleiches gilt dann, wenn die Verfahren mit Templates arbeiten.

4.2.2.4.2 Art der Datenspeicherung: Verwendung von Templates?

Der Grund dafür, dass biometrische Verfahren bislang regelmäßig Templates verwenden, liegt im geringeren Speicherbedarf dieser Datensätze gegenüber Volldaten. So benötigt das Gesamtbild eines Fingerabdrucks etwa 250 Kilobyte Speicherplatz, ein Template dagegen lediglich 900 bis 1.200 Bytes.[1133] Als unbeabsichtigte, aber datenschutzrechtlich vorteilhafte Nebenfolge werden bei der Berechnung von Templates Informationen des Rohdatensatzes entfernt. Diese sind zur Authentifikation nicht erforderlich, können aber die soeben beschriebenen Zusatzinformationen enthalten.

Es ist jedoch damit zu rechnen, dass die Leistungsfähigkeit von Chipkarten in Zukunft keinen begrenzenden Faktor für die Verwendung von Volldaten mehr darstellen wird. Deshalb ergibt sich an dieser Stelle die Frage, ob nicht unter dem Blickwinkel der verfassungsrechtlichen Erforderlichkeit der Einsatz von Templates das mildere Mittel und damit zwar nicht aus technischen, wohl aber aus rechtlichen Gründen vorzuziehen ist.

Bisherige Tests deuten darauf hin, dass diese Betriebsart gegenüber dem Einsatz von Volldaten geringere Fehlerraten aufweist und damit besser zur Authentifikation geeignet ist. Im Projekt BioP I wurden mit herstellerspezifischen Templates gegenüber Volldaten die „mit Abstand besten Erkennungsleistungen“ erzielt.[1134] Falls dieses Ergebnis auch bei weiterem technischem Fortschritt Bestand haben sollte, wären – vorbehaltlich des Problems der mangelnden internationalen Standardisierung[1135] – Templates bereits aus diesem Grund zu bevorzugen.

Unterstellt man eine zumindest ähnliche Eignung von Volldaten und Templates zur Authentifikation, so verlagert sich die Beurteilung auf die Erforderlichkeitsebene. Die Verwendung von Templates stellt insbesondere dann das mildere Mittel dar, wenn in ihnen tatsächlich bestimmte Überschussinformationen nicht mehr enthalten sind. Das hängt zunächst vom Aufbau des jeweiligen Templates ab. Wenn dieses den Teil der Volldaten abbildet, der die sensiblen Informationen enthält, ist der Eingriff gleich schwer. Allerdings dürften insbesondere Datenbereiche, die Informationen über die Gesundheit enthalten, häufig für das Template ungeeignet sein, weil dessen Beständigkeit gefährdet ist, wenn sich die Informationen in relativ kurzen Abständen verändern können.[1136] Daher ist eher

1130 In dieser Richtung auch *Garstka*, NJ 2002, 524, 525. Die Iriserkennung ist gleichzeitig das Verfahren mit den geringsten Fehlerraten, s.o. 4.2.2.4.1.1. Sie hat allerdings entscheidende Nachteile bezüglich der Kosten und der bestehenden Beschränkung auf nur einen Patentinhaber weltweit.

1131 S.u. 4.2.2.4.3.

1132 S.u. 4.2.2.4.4.

1133 *Behrens/Roth* 2001a, 6 ff.; *TAB* 2002. 12. Die Größe eines Iris-Templates liegt bei 512, die des Gesichtstemplates bei bis zu 1.300 Bytes (ebd., 15, 17).

1134 *BSI/BKA/Secunet* 2004, 10, 49; s.a. *Scheuermann*, DuD 2005, 66, 67.

1135 S.u. in diesem Abschnitt.

1136 Dagegen können dauerhafte Gesundheitsinformationen, etwa chronische Krankheiten, durchaus zur Authentifikation geeignet sein, vgl. *Bromba* 2003.

davon auszugehen, dass zumindest variable Überschussinformationen regelmäßig nicht in Templates enthalten sind. Auch ansonsten dürften einige Informationen wegfallen, beispielsweise bei der Gesichtserkennung die Farbe des Gesichts. Es wäre dann nicht mehr möglich, aus einer Datenbank mit Templates die Betroffenen dunkler Hautfarbe herauszufiltern. Die Verwendung von Templates erschwert also die kategoriale Einteilung der Betroffenen und damit auch das Erstellen von Profilen. Sie ist deshalb im Grundsatz das mildere Mittel gegenüber der Verwendung von Volldaten.[1137]

Dies gilt allerdings nur dann, wenn aus dem im Ausweis gespeicherten Template nicht der Volldatensatz zurückermittelt werden kann, weil andernfalls unter Erforderlichkeitsgesichtspunkten kein grundsätzlicher Unterschied zwischen den beiden Verfahren besteht. Die bisherige datenschutzrechtliche Diskussion ging insoweit durchweg von der Prämisse aus, dass eine Rückwärtskonstruktion biometrischer Volldaten aus Templates nicht möglich ist.[1138] Dies trifft jedoch in dieser Allgemeinheit nicht zu. Durch eine Abfolge von Matchingversuchen mit immer leicht modifizierten Test-Templates ist es in einer so genannten „Hillclimbing-Attacke" vielmehr möglich, einen Volldatensatz zu konstruieren, der ein Template liefert, welches dem in der Karte gespeicherten so ähnlich ist, dass das System ein positives Matchingergebnis ermittelt.[1139]

Diese Möglichkeit schmälert den datenschutzrechtlichen Vorteil von Templates. Allerdings setzt die beschriebene Form des Angriffs einen erheblichen Aufwand voraus. Der Angreifer muss über den Ausweis und eine Matching-Einheit verfügen, die exakt die Bedingungen des Echtbetriebs simulieren kann; darüber hinaus ist je nach Merkmal, verwendetem Algorithmus und noch vorhandenen Informationen eine große Zahl von Iterationen erforderlich. Auch wenn diese Voraussetzungen gegeben sind, können Informationen, die im Template vollständig nicht mehr enthalten sind, nicht aus diesem ermittelt werden.[1140] So genügt es zwar für einen Angriff auf ein Fingerabdruck-System, willkürliche Linien um ein bekanntes Muster von Finger-Minutien[1141] zu zeichnen. Werden dabei keine zusätzlichen Minutien hinzugefügt, so liefert dieses Bild ein Template, welches zur Überwindung des Systems geeignet ist. Dieses ist jedoch in keiner Weise mit dem Gesamtfingerbild des Betroffenen vergleichbar. Besteht ein Gesichtstemplate ausschließlich aus Informationen über den Abstand bestimmter Gesichtspartien zueinander, lässt sich zwar ein Gesicht konstruieren, welches dasselbe Template liefert. Es ist jedoch beispielsweise nicht möglich, die Hautfarbe des Betroffenen aus diesem Template zu bestimmen. Entsprechendes gilt, wenn Informationen über den Gesundheitszustand in Datenbereichen enthalten sind, die bei der Berechnung des Templates gelöscht werden. Damit ist die Möglichkeit der

---

1137 S.a. *Roßnagel/Hornung*, in: Reichl/Roßnagel/Müller 2005, 136; 231 f.; *dies*., DuD 2005, 69, 71; *Hornung* 2004b, 53.

1138 *AKT*, DuD 1997, 709, 713; *Gundermann/Köhntopp*, DuD 1999, 143, 150; *Bäumler/Gundermann/Probst* 2001, 16; Roßnagel-*Gundermann/Probst*, Kap. 9.6, Rn. 48; *Albrecht* 2003a, 158; *OECD* 2004, 16; *JRC/IPTS* 2005, 36. An dieser Stelle sei nochmals auf die hier verwendete Terminologie verwiesen, die zwischen Templates und Volldatensätzen unterscheidet und unter ersteren nur extrahierte Datensätze versteht, s.o. 2.3.3.2.

1139 Bei diesem Angriff wird ein willkürlicher Template-Datensatz an die Matching-Einheit gesandt und die Übereinstimmungsrate mit dem Referenzdatensatz gemessen. Danach wird der Testdatensatz in einigen definierten Bereichen leicht verändert und der Vorgang wiederholt. Steigt die Übereinstimmungsrate, so wird mit dem veränderten Datensatz und einem anderen Bereich weitergearbeitet; andernfalls mit dem ursprünglichen Datensatz. Dieser Vorgang wird in einer Vielzahl von Iterationen solange wiederholt, bis die vom System vorgegebene Übereinstimmungsrate erreicht ist, s. ausführlich *Adler* 2003; *Soutar*, Secure 2002, 46 ff. Als mögliche Gegenmaßnahme kommt die Geheimhaltung der Übereinstimmungsraten in Betracht.

1140 *Bromba* 2003.

1141 Endende Täler, Verzeigungslinien und Schweißporen, s. *Breitenstein* 2002, 37 f.

Rückwärtskonstruktion von Templates zwar ein Sicherheitsproblem biometrischer Verfahren im Einzelfall. Sie ändert jedoch nichts an der datenschutzrechtlichen Vorzugswürdigkeit von Templates gegenüber Volldatensätzen, sofern bei der Templateberechnung sensible Zusatzinformationen entfernt werden.

Im Ergebnis stellt die Verwendung von Templates damit immer dann ein milderes Mittel dar, wenn bei ihrer Berechnung Teile der Rohdaten endgültig entfernt werden. Auch in diesem Fall werden allerdings zum Matching erneut Rohdaten erhoben, in denen diese Teile enthalten sind. Deshalb sind abgeschottete Matching-Einheiten zu verwenden, die eine dauerhafte Speicherung der Rohdaten bereits technisch ausschließen.[1142]

Ein gravierendes Problem verbleibt, wenn der jeweilige Ausweis möglichst universell einsetzbar sein soll.[1143] Bislang werden Templates desselben biometrischen Merkmals nämlich teilweise je nach Hersteller auf unterschiedliche (proprietäre) Art und Weise berechnet. Wird ein Ausweis weltweit eingesetzt, so ist damit zu rechnen, dass Matching-Einheiten unterschiedlicher Hersteller zum Einsatz kommen werden. Der digitale Personalausweis wird als – zumindest europäisches – Reisedokument verwendet werden und muss demzufolge auch im Ausland zur Identitätsprüfung einsetzbar sein. In den Reisedokumenten verschiedener Staaten können nicht jeweils unterschiedliche Templates eingesetzt werden, weil dann an jeder Kontrollstelle jedes Staates eine Vielzahl von Verfahren bereitgehalten werden müsste. Deshalb ist die Auffassung, wonach es für die Funktionsweise biometrischer Verfahren nicht erforderlich sei, biometrische Volldaten zu speichern,[1144] nur teilweise richtig. Sie trifft zwar auf ein bestimmtes Verfahren eines bestimmten Betreibers zu, nicht jedoch auf eine Situation, in der sich die Beteiligten nicht auf einen Template-Standard einigen können.

Die internationale Standardisierung biometrischer Datensätze findet unter dem Dach des Common Biometric Exchange Formats Framework (CBEFF) statt und ist unterschiedlich weit fortgeschritten.[1145] Die größten Fortschritte wurden bisher beim Fingerabdruck erzielt. Dieses Merkmal ist das einzige, bei dem es echte Fortschritte bei der Normierung von Templates gibt (ISO/IEC 19794-2 und 3). Für die Gesichtserkennung (ISO/IEC 19794-5) und den Iris-Scan (ISO/IEC 19794-6) wird es in absehbarer Zeit nur Standards für Volldaten geben. Bei der Iris besteht insofern ein de facto-Standard für Templates, als es weltweit nur einen Patentinhaber für dieses Verfahren gibt.

Sofern auf dem digitalen Personalausweis ein Merkmal gespeichert wird, für das noch kein Standard existiert, könnte nur eine proprietäre Template-Struktur verwendet werden. Da dies – wie beschrieben – undurchführbar ist, hat sich die ICAO, die den Einsatz von Gesichtsdaten in internationalen Reisedokumenten favorisiert, für die Verwendung von Volldatensätzen ausgesprochen.[1146] So könnte jeder Staat entweder diese Daten vergleichen oder aus den gespeicherten Volldaten mit dem jeweils eigenen Algorithmus ein Template errechnen und dieses mit dem neu erhobenen Datensatz des Betroffenen vergleichen.

Damit stellt sich die Frage des Verhältnisses zwischen der grundsätzlich verfassungsrechtlich gebotenen Verwendung von Templates und den internationalen Entscheidungen, die insbesondere durch die ICAO getroffen werden. Zunächst sind letztere völkerrechtlich

1142 S.a. unten 4.2.2.4.4.

1143 Vgl. dazu *Roßnagel/Hornung*, in: Reichl/Roßnagel/Müller 2005, 231 f.; s.a. *dies*., DuD 2005, 69, 71.

1144 So *Golembiewski/Probst* 2003, 13 (in der dortigen Terminologie „Rohdaten").

1145 Vgl. zum Stand Januar 2004 *Struif/Scheuermann*, in: Reichl/Roßnagel/Müller 2005, 41 ff.; s.a. unten 6.1.2; s.a. *Scheuermann*, DuD 2005, 66, 67.

1146 *ICAO* 2004a, 19, 31 ff.

nicht bindend, sondern nur unverbindliche Empfehlungen.[1147] Schon deshalb können sie keine Anforderung des deutschen Grundgesetzes außer Kraft setzen. Die Problematik einer Einsetzbarkeit von Templates ist jedoch auch Teil der Verhältnismäßigkeitsprüfung. Da der digitale Personalausweis auch im Ausland eingesetzt werden soll, muss er einschließlich der gespeicherten biometrischen Daten zu diesem Einsatz geeignet sein. Wenn dies aufgrund mangelnder Standardisierung nicht der Fall ist, so scheidet die Verwendung von Templates aus. Zum gegenwärtigen Zeitpunkt wäre der Einsatz von Iris-Templates möglich, weil es hier aufgrund der Beschränkung auf nur einen Patentinhaber einen de facto-Standard gibt. Für das Gesicht und den Fingerabdruck ist ein weltweiter Einsatz eines Templates zurzeit nicht machbar. Dies dürfte sich für den Fingerabdruck in absehbarer Zeit ändern. Im Unterschied zum Reisepass würde allerdings für den digitalen Personalausweis eine europäische Standardisierung ausreichen, weil dieser kein weltweites, sondern nur ein europäisches Reisedokument sein wird. Es ist nicht absehbar, ob eine solche europäische Einigung auf eine Template-Struktur möglich ist. Sie könnte etwa im Rahmen der Schengen-Konsultationen angestrebt werden.

Sollte eine europäische Normung nicht möglich sein und damit der Einsatz von Templates verhindert werden, so bedeutet dies allerdings nicht notwendigerweise, dass bei Gesicht und Fingerabdruck deshalb der Einsatz von Volldatensätzen zulässig wäre. Zunächst muss dieses Datenformat zur Authentifikation geeignet sein. Das ist zumindest für das Kriterium einer EER von 1 % bei Gesichtsvolldatensätzen nicht der Fall.[1148] Aufgrund der besonderen Gefährdungslage bei der Verwendung von Volldaten muss die Bundesrepublik sich darüber hinaus auf internationaler Ebene für eine Standardisierung von Template-Formaten einsetzen.

Immer dann, wenn ein Chipkartenausweis seiner Zweckbestimmung nach innerhalb einer – auch großen – geschlossenen Benutzergruppe eingesetzt wird, ist die Verwendung von Templates auch dann geeignet, wenn es sich dabei um eine proprietäre Lösung handelt. Da die Verwendung von Templates das mildere Mittel gegenüber der von Volldaten darstellt, sind für derartige Ausweise Templates zu verwenden.

4.2.2.4.3 Ort der Datenspeicherung

Nach geltendem Recht ist eine Speicherung biometrischer Daten außerhalb des Personalausweises unzulässig.[1149] Einzige Ausnahme ist das Gesichtsbild im Personalausweisregister. Unabhängig von diesem Verbot ist de lege ferenda die verfassungsrechtliche Zulässigkeit einer solchen Speicherung unter Verhältnismäßigkeitsgesichtspunkten zu prüfen, insbesondere vor dem Hintergrund von Forderungen nach der Einrichtung einer bundes- oder sogar europaweiten Datenbank mit den biometrischen Daten sämtlicher Bürger.[1150]

Solange Daten nur auf der Karte vorhanden sind, hat der Einzelne die physische Datenhoheit und kann über die Preisgabe im Einzelfall entscheiden. Verallgemeinernd lässt sich deshalb festhalten, dass eine Speicherung außerhalb eines Chipkartenausweises grundsätz-

1147 S.o. 3.1.1; s. zum Folgenden bereits *Roßnagel/Hornung*, in: Reichl/Roßnagel/Müller 2005, 231 f.

1148 Vgl. die Testergebnisse für komprimierte Volldatensätze gemäß den ICAO Richtlinien bei *BSI/BKA/Secunet* 2004, 42 ff.

1149 Das folgt für bundesweite Dateien aus § 1 Abs. 5 Satz 2 PersAuswG, für das Personalausweisregister aus dem abschließenden § 2a PersAuswG, für übrige Register aus § 3 Abs. 2 PersAuswG.

1150 Eine EU-weite Fingerabdrucks-Datenbank wird etwa vom Bund Deutscher Kriminalbeamter gefordert, vgl. http://www.heise.de/newsticker/meldung/41642; http://www.heise.de/newsticker/meldung/57565; s.a. *Stock* 2002, 7 f. Trotz des Verbots in § 1 Abs. 5 Satz 2 PersAuswG arbeitet z.B. das Pilotprojekt zur Iriserkennung am Frankfurter Flughafen, das Mitte Februar 2004 gestartet wurde, mit einer zentralen Datenbank.

lich eine stärkere Beeinträchtigung des Grundrechts auf informationelle Selbstbestimmung darstellt als eine ausschließliche Ablage auf der Karte selbst. Die Intensität des Eingriffs steigt außerdem dann, wenn eine zentrale Speicherung erfolgt. Eine solche Datensammlung erhöht die Attraktivität für interne und externe Angriffe, weil der Angreifer im Erfolgsfall mehr und aussagekräftigere Daten erlangt. Sie erleichtert darüber hinaus Profilbildungen[1151] und Zweckentfremdungen bei der Weiterverwendung und Übermittlung.[1152]

Hieraus folgt nicht, dass eine Speicherung in dezentraler oder zentraler Form außerhalb des jeweiligen Ausweises stets unzulässig wäre. Diese Frage ist nur im Zusammenhang mit den technischen Möglichkeiten und dem konkreten Zweck des Ausweises zu beantworten. Technische Gegebenheiten können eine Vorhaltung in der Peripherie erzwingen, Verarbeitungszwecke eine zentrale Datenbank als sinnvoll erscheinen lassen. Ob beides verhältnismäßig ist, entscheidet sich im Einzelfall. Das ist auch der Grund dafür, dass eine Speicherung außerhalb der Chipkarte in einem Fall zulässig, im anderen unzulässig sein kann.

Aufgrund des hohen Eingriffsgrades einer zentralen Speicherung biometrischer Daten hat diese zu unterbleiben, wenn eine zentrale Datenbank für die Funktionsfähigkeit des Systems nicht erforderlich ist.[1153] Nach der Begründung zum Terrorismusbekämpfungsgesetz hat die Aufnahme biometrischer Merkmale die Funktion, die Identitätsfeststellung gegenüber dem visuellen Vergleich zwischen Lichtbild und Person durch einen computergestützten Vergleich zu verbessern.[1154] Ziel ist es, die zweifelsfreie Feststellung der Übereinstimmung der Identität des Ausweisinhabers mit der Identität der zu kontrollierenden Person zu ermöglichen. Aus der Regelung in § 3 Abs. 5 PersAuswG (Verbot einer bundesweiten Datei) ergibt sich, dass der Gesetzgeber selbst davon ausgegangen ist, zur Erreichung dieser Ziele seien Verfahren der biometrischen Verifikation hinreichend und eine biometrische Identifikation nicht erforderlich.[1155] Das ist zutreffend, weil sich das staatliche Interesse darauf beschränkt, die eindeutige Zuordnung einer Person zu einem Identifikationspapier festzustellen. Die weiteren Angaben über deren Identität ergeben sich dann aus diesem Papier.[1156] Für Kontrollvorgänge selbst ist eine zentrale Datenbank damit nicht erforderlich.

Dem Zweck der Identifikation kann es darüber hinaus dienen, wenn eine solche Datenbank zur Verhinderung so genannter „Doppelidentitäten", also der Mehrfachbeantragung eines Ausweises unter falschem Namen, errichtet wird. Im Ausland wird in einer Reihe von Ländern ein solches System praktiziert, beispielsweise in Malaysia, Oman und Brunei. Dies wird auch in Großbritannien[1157] und den USA[1158] diskutiert. Zentrale Systeme und der Abgleich bei der Ausweisbeantragung sind möglicherweise in den Staaten erforderlich, die

---

1151 Es können etwa Abfragevorgänge protokolliert und so Bewegungsprofile erstellt werden; allgemein zum Problem der Profilbildung oben 4.2.1.2.4.

1152 *Bizer* 2002, 21 f.; *Bultmann/Wellbrock/Biermann/Engels/Ernestus/Höhn/WehrmannRüdiger/Schurig* 2002, 16; *Konferenz der Datenschutzbeauftragten* 2001; für den Bereich der Biometrie vgl. *Albrecht* 2003a, 162 ff.; *Bizer*, DuD 2002, 44; *Art. 29 DPWP* 2003, 6 f.; *Golembiewski/Probst* 2003, 69 f., 72; *Woodward/Orlans/Higgins* 2003, 40.

1153 *Köhntopp* 1999, 183; *TAB* 2002, 25; *Nanavati/Thieme/Nanavati* 2002, 249 f., 253 f.; *Konferenz der Datenschutzbeauftragten* 2002, unter 5; *OECD* 2004, 38; *Hornung*, KJ 2004, 344, 352; s.a. *Probst* 2002, 121 (die dezentrale Speicherung sei „stark anzuraten"); zur Problematik auch *LSE* 2005, 66 ff.

1154 BT-Drs. 14/7386, 48.

1155 Auch die Bundesregierung plant, an dem Verbot einer zentralen Datenbank festzuhalten, s. die Antwort auf die Kleinen Anfrage der FDP-Fraktion im Januar 2005, BT-Drs. 15/4616, 3.

1156 Dies unter der Prämisse, dass das Papier selbst nicht gefälscht wurde. Dieses Problem wird aber durch die hohe Fälschungssicherheit des bundesdeutschen Personalausweises verringert.

1157 S. *Mansfield/Rejman-Greene* 2003, 9.

1158 *Woodward/Orlans/Higgins* 2003, 364 ff.

parallel erstmals zentrale oder dezentrale Einwohnerdatenbanken aufbauen. In Deutschland besteht dagegen aufgrund des hochentwickelten Meldewesens keine entsprechende Notwendigkeit. Es ist nicht ersichtlich, dass „Doppelidentitäten" deutscher Bürger bislang ein Problem darstellen. Aufgrund der fehlenden Erforderlichkeit hat die zentrale Speicherung biometrischer Ausweisdaten zum Zwecke einer Identifizierung im Einzelfall damit aus Verfassungsgründen zu unterbleiben.[1159]

Fraglich ist weiter, ob, wie bisher bei Ausweisdaten, eine dezentrale Speicherung im Personalausweisregister zulässig wäre. Auch dies ist nur verhältnismäßig, sofern eine reine Ablage der Referenzdaten auf dem Personalausweis selbst zum angestrebten Zweck nicht ausreichend ist. Da zur Personenkontrolle – wie ausgeführt – eine Speicherung auf dem Ausweis selbst ausreicht, ist auch eine dezentrale Speicherung außerhalb des digitalen Personalausweises nicht erforderlich.[1160] Für die Vermeidung von Doppelidentitäten fehlt es bereits an der Eignung, weil hierzu ein Abgleich mit sämtlichen Daten nötig ist.

Eine dezentrale Speicherung könnte auch dazu verwendet werden, die Echtheit der biometrischen Ausweisdaten durch einen Vergleich mit den Registerdaten festzustellen. Hierzu gibt es jedoch technische Alternativen, insbesondere die elektronische Signatur der Ausweisdaten durch den Hersteller oder die Personalausweisbehörde.[1161] Dadurch wird eine dauerhafte Überprüfbarkeit der Datenintegrität gewährleistet.

Weiter könnte eine Speicherung bei der Neubeantragung (etwa der Ausstellung eines neuen Ausweises nach Gültigkeitsablauf) die Möglichkeit eröffnen, auf bereits vorhandene Daten zurückgreifen. Hierzu bietet sich aber als milderes Mittel die Neuerhebung an. Diese ist schon aus Gründen der Merkmalsveränderung über die Zeit[1162] und wegen der zu erwartenden technischen Veränderungen der Verfahren erforderlich. Darüber hinaus stellt die Erleichterung für die Verwaltung bei der Neuausgabe eines Ausweises verglichen mit den erheblichen Risiken für das Grundrecht auf informationelle Selbstbestimmung einen sehr geringen Vorteil dar. Unter Verhältnismäßigkeitsgesichtspunkten wäre die Speicherung damit auch objektiv unzumutbar.

Es ist also zunächst festzuhalten, dass für die Verwirklichung der Zwecke der durch das Terrorismusbekämpfungsgesetz in das Personalausweisgesetz aufgenommenen Regelungen jede Speicherung biometrischer Daten außerhalb des Personalausweises unverhältnismäßig wäre und deshalb zu unterbleiben hat. Einzige Ausnahme ist die kurzzeitige Speicherung der Daten im Rahmen des Enrolments. Wie bei der Speicherung von Ausweisdaten bei der Bundesdruckerei GmbH zu Herstellungszwecken (§ 3 Abs. 3 Satz 2 PersAuswG) ist die Speicherung verfassungsrechtlich zulässig, wenn die Daten nach der Herstellung unmittelbar gelöscht werden.

Zu klären bleibt, ob ein bislang nicht vom Gesetzgeber intendierter Zweck die Einrichtung zentraler oder dezentraler Datenbanken rechtfertigen könnte.[1163] Hier läge insbesondere eine Verwendung zur Verbrechensbekämpfung nahe. Denkbar wäre etwa der Ab-

---

1159 Vgl. *Roßnagel/Hornung*, in: Reichl/Roßnagel/Müller 2005, 136 ff.; *dies*., DuD 2005, 69, 72; *Hornung*, KJ 2004, 344, 357; ebenso *Golembiewski/Probst* 2003, 69 f., 72; zu den Risiken einer zentralen Speicherung auch *Art. 29 DPWP* 2003, 6 f.; *Privacy International et. al.* 2004, 2; *Albrecht* 2003a, 163 (die allerdings eine eindeutige Aussage zur Verfassungsmäßigkeit vermeidet: es sei „zu prüfen", ob eine bundesweite Datei unzulässig wäre). Eine bundesweite Datei, die bei jedem dezentralen Kontrollvorgang zur Überprüfung herangezogen würde, wäre darüber hinaus auch technisch nicht praktikabel, s.o. 4.2.2.4.1.1.

1160 *Golembiewski/Probst* 2003, 70.

1161 S. zur technischen Umsetzung unten 6.2.1.1.

1162 Die Langzeitstabilität ist insbesondere ein Problem der Gesichtserkennung, s.o. 4.2.2.4.1.1.

1163 S. bereits *Roßnagel/Hornung*, in: Reichl/Roßnagel/Müller 2005, 138; *dies*., DuD 2005, 69, 72; *Hornung*, KJ 2004, 344, 357.

gleich von Fingerabdruckssspuren oder Videoaufnahmen[1164] eines unbekannten Täters mit der Gesamtdatenbank zum Zweck der Aufklärung einer schweren Straftat. Umgekehrt könnte bei der Fahndung nach einer namentlich bekannten Person das biometrische Datum von der Personalausweisbehörde an die Polizei übermittelt und dann in den Fahndungsbestand eingespeist werden. Es darf zwar nicht übersehen werden, dass biometrische Erkennungsverfahren bislang nicht dieselbe Leistung erbringen können wie herkömmliche erkennungsdienstliche Maßnahmen. Das wird am Beispiel des Fingerabdrucks deutlich: Während das polizeiliche AFIS mit dem abgerollten Bild aller zehn Finger arbeitet, verwenden andere biometrische Systeme nur den Ausschnitt eines einzigen Fingers. Daraus resultiert eine erheblich eingeschränkte Verwendbarkeit dieser Verfahren im kriminalistischen Bereich. Dennoch ist ein Einsatz hierfür denkbar.

Soll eine biometrische Datenbank der Verbrechensbekämpfung dienen, so bedürfte sie zunächst einer hierfür hinreichenden gesetzlichen Grundlage. Ist dies noch relativ unproblematisch, so ist doch fraglich, ob eine Datenbank verhältnismäßig wäre, die alle biometrischen Daten aller in Deutschland lebenden Personen zum Zwecke der Verbrechensbekämpfung enthielte. Eine Eignung liegt insoweit vor; es dürfte eine Reihe von Straftaten geben, bei denen eine Aufklärung heutzutage unterbleibt, weil am Tatort gefundene Fingerabdrücke kein positives Ergebnis im AFIS erbringen. Die Maßnahme wäre auch erforderlich, weil zumindest in manchen Fällen kein anderes Mittel zur Aufklärung verfügbar ist. Zweifelhaft ist jedoch die objektive Zumutbarkeit.

Problematisch ist insbesondere, dass es sich bei einem derartigen System notwendigerweise um eine zentrale Datenbank handeln würde. Selbst wenn die Daten tatsächlich dezentral (etwa bei den Personalausweisbehörden) gespeichert wären, müsste ein automatisiertes Abfragesystem eingerichtet werden, welches funktional einer zentralen Speicherung entsprechen würde. In Fahndungsfällen übermitteln bereits heute die Personalausweisbehörden auf der Basis von § 2b Abs. 2 PersAuswG Daten an die Strafverfolgungsbehörden. Dies könnte in Zukunft auch als Massenabfrage durchgeführt werden,[1165] sofern die biometrischen Daten bei den Personalausweisbehörden gespeichert werden. Da die Daten digital abgelegt werden, ist eine Vernetzung dieser Datenbanken technisch relativ einfach zu bewerkstelligen.[1166]

Vor- und Nachteile einer solchen Speicherung sind gegeneinander abzuwägen. Einerseits würde ein derartiges System in einer Zahl von Kriminalfällen zu zusätzlichen Fahndungserfolgen führen. Diesem Vorteil steht jedoch der Nachteil der Einrichtung einer zentralen Datenbank gegenüber, die von jedem deutschen Bürger Zeit seines Lebens ein unveränderbares und zur allgemeinen Überwachung geeignetes Kennzeichen vorhalten würde. Dies ist deshalb unzumutbar, weil nur eine kleine Zahl von Bürgern straffällig wird. Die Möglichkeit zusätzlicher Fahndungserfolge rechtfertigt nicht, die konkrete Gefahr der Verwendung biometrischer Merkmale als allgemeines Personenkennzeichen in Kauf zu nehmen.[1167]

1164 Eine Verwendung der Iris erscheint insoweit unrealistisch.

1165 Das wäre nach der aktuellen Gesetzeslage allerdings rechtswidrig, weil diese eine Überprüfung der Erforderlichkeit einer Anfrage bei den Personalausweisbehörden im Einzelfall verlangt; s.o. 2.2.1.4.

1166 Die technischen Voraussetzungen hierfür dürften ohnehin in absehbarer Zeit vorhanden sein, weil durch die Reform des Melderechts-Rahmengesetzes aus dem Jahre 2002 (BGBl. I, 1342) eine Vernetzung aller Meldestellen in Deutschland angestrebt wird.

1167 *Konferenz der Datenschutzbeauftragten* 2002, unter 4 und 5; *Der Landesbeauftragte für den Datenschutz Brandenburg* 2002, 21.

Nicht umsonst hat das Bundesverfassungsgericht für den Aufbau einer begrenzten Gendatenbank Vorbestrafter hohe Anforderungen formuliert.[1168] Für die hier in Rede stehende zentrale Datenbank müssen aus zwei Gründen noch höhere Anforderungen an die objektive Zumutbarkeit gestellt werden: einerseits, weil die gesamte Bevölkerung betroffen wäre, andererseits, weil im Unterschied zu einer Datenbank Vorbestrafter die übergroße Mehrheit der Betroffenen keinen Anlass für die Datenspeicherung gegeben hätte. Auch dies spricht für die Unverhältnismäßigkeit der Maßnahme.

Überdies stellt die Einrichtung einer solchen Datenbank eine grundsätzlich unzulässige Vorratsdatenspeicherung dar. Wird durch einen allgemeinen „Generalverdacht" ein Überwachungsinstrument für die gesamte Bevölkerung geschaffen, so wird eine entscheidende Grenze im Verhältnis zwischen Staat und Bürger überschritten. Ein solches allgemeines Misstrauen des Staates gegenüber seinen Bürgern widerspricht fundamental dem Menschenbild des Grundgesetzes. Bei aller Problematik dieses Begriffs[1169] lässt sich aus bestimmten tragenden Prinzipien der Verfassung (Grundentscheidung für den Schutz der Menschenwürde, ausdifferenziertes System von Grundrechten, effektiver Mechanismus zu ihrer Überwachung mit der Möglichkeit einer gerichtlichen Normenkontrolle) ein Grundverständnis vom Verhältnis des Staates zu seinen Bürgern ableiten, nach dem diese im Kern freie, selbstbestimmte und unüberwachte Individuen sind. Auch wenn die Nichtaufklärbarkeit von Verbrechen in jedem Einzelfall ungerechtfertigt sein mag, so muss ein freiheitlicher Staat doch mit einem derartigen Restrisiko leben, wenn er seine Bürgerrechte nicht aufs Spiel setzen will. Im Ergebnis ist die Einrichtung einer allgemeinen Datei mit biometrischen Daten zum Zweck der Verbrechensbekämpfung objektiv unzumutbar und hat damit zu unterbleiben.

4.2.2.4.4 Ort des Matchings

Die Frage des Ortes, an dem das Matching der biometrischen Daten stattfindet, hängt eng mit der Frage des Speicherortes der Referenzdaten zusammen:[1170]

- Eine grundsätzliche Möglichkeit besteht darin, die erhobenen Daten an eine zentrale Datenbank zu senden und dort entweder gegen den kompletten Datenbestand (1:n) oder gegen ein spezifisches Datum (1:1) zu matchen. Da die Daten jedoch nicht außerhalb des digitalen Personalausweises gespeichert werden dürfen,[1171] scheidet diese Variante aus.
- Demgegenüber findet beim Matching-On-Card der Datenabgleich auf dem Chip selbst statt, indem entweder die Karte selbst über einen Sensor verfügt oder die Daten des Peripherie-Sensors an den Chip gesendet werden, dieser die Daten vergleicht und das Ergebnis nach außen übermittelt.[1172] Matching-On-Card ist bislang aufgrund der Speicher- und Rechenleistung der Chips nur mit Templates möglich. In Zukunft dürfte jedoch auch eine Verwendung von Volldatensätzen machbar sein.
- Zwischen den Extremen einer zentralen Datenbank und einem Matching auf der Karte liegen dezentrale Lösungen mit Systemen, bei denen die Referenzdaten aus

1168 S. BVerfGE 103, 21 ff.; hierzu *Faber*, RDV 2003, 278, 280 ff.

1169 So ist bspw. kritisiert worden, dass dieser in der Rspr. (des BVerwG) „wahlweise...als Grundrechtsschranke...oder gleichsam gegenläufig als Verstärkung des Grundrechts auf körperliche Integrität ausgemünzt" werde, s. *Dreier* 2003, 222; vgl. eingehend *Häberle* 1988 (insbes. 32 ff.); *Becker* 1996 (insbes. 191 ff.).

1170 Vgl. zum Folgenden *Struif/Scheuermann*, in: Reichl/Roßnagel/Müller 2005, 172 f.

1171 S.o. 4.2.2.4.3.

1172 S. näher oben 2.3.3.2.

dem Chip ausgelesen und vor Ort (beispielsweise an der Grenze oder bei einer Polizeikontrolle) verglichen werden. Hierbei lässt sich unterscheiden zwischen größeren Datenverarbeitungsanlagen (etwa einem Zentralcomputer an der Grenzstation) und Einheiten, die ausschließlich über eine Funktion zum Abgleich der biometrischen Daten verfügen und ansonsten abgeschottet von der Außenwelt arbeiten.

Der Gesetzgeber hat bislang keine Regelung darüber getroffen, wo das Matching erfolgen soll. Es wird zwar vertreten, aus der Tatsache, dass § 1 Abs. 3 PersAuswG die Daten der Zone für das automatische Lesen abschließend benennt und keine biometrischen Daten erwähnt, könne „nur geschlossen werden, dass der Gesetzgeber ausschließen wollte, dass die biometrischen Merkmale automatisiert gelesen werden können“.[1173] Deshalb müsse der Abgleich auf dem Ausweis selbst erfolgen. Es gibt indes keinerlei Indizien dafür, dass der Gesetzgeber sich bereits auf ein Verfahren festgelegt hat. Der Ort des Matchings wird in der Gesetzesbegründung nicht erwähnt. Außerdem sollen gemäß § 1 Abs. 5 PersAuswG die Einbringung der biometrischen Merkmale und die Art ihrer Verarbeitung und Nutzung ausdrücklich durch ein besonderes Bundesgesetz geregelt werden. Hieraus ergibt sich – im Gegensatz zu der genannten Auffassung – eindeutig, dass der Gesetzgeber keine technische Umsetzungsvariante ausschließen wollte.

Unter Verhältnismäßigkeitsgesichtspunkten ist bei der Auswahl dasjenige System zu bevorzugen, bei dem möglichst wenige Daten außerhalb des Verfügungsbereichs des Ausweisinhabers entstehen. Aus datenschutzrechtlicher Sicht ist nicht so sehr entscheidend, wo der Vorgang des Datenvergleichs stattfindet, sondern, wer, wann, wo über welche Daten verfügen kann.

Der geringste Eingriff entsteht bei einem Sensor auf der Karte, weil dann die anfallenden biometrischen Rohdaten auf dem Chip, und damit unter ausschließlicher Kontrolle des Ausweisinhabers, verbleiben. Das stellt zwar keine totale Datenvermeidung dar, kommt dieser aber sehr nahe. Bedauerlicherweise ist die Entwicklung von Karten mit Sensoren in absehbarer Zeit nur für den Fingerabdruck realistisch, weil Kameras zur Iris- oder Gesichtserkennung nicht in die Chipkarte integriert werden können. Auch beim Fingerabdruck, für den erste Prototypen existieren,[1174] treten noch technische Schwierigkeiten auf. Ein Problem entsteht dadurch, dass die Prozessorleistung, die zur Merkmalsextraktion erforderlich ist, die Kapazität des Kartenchips übersteigen kann. Andererseits wird der datenschutzrechtliche Vorteil zunichte gemacht, wenn die Karte die Daten zur Extraktion an die Peripherie sendet und von dort das Template zum Matching empfängt. Eine Lösung besteht darin, hierzu einen zweiten Chip auf der Karte zu verwenden.[1175] Mit dem technischen Fortschritt dürften künftige Kartengenerationen außerdem über die erforderliche Leistung verfügen. Eine weitere Schwierigkeit ist die durch den Sensor verursachte Kartendicke, die zumeist außerhalb der ISO-Standards liegt. Diese Aufgabe scheint technisch lösbar zu sein; Biegebelastungen und thermische Zyklen verursachen jedoch schnell einen Ausfall des Sensors.[1176] Dies ist mit Blick auf die Laufzeit des digitalen Personalausweises nicht akzeptabel. Schließlich entstehen deutlich höhere Produktionskosten sowie die Gefahr einer Herstellung eines gefälschten Chips, der stets ein positives Ergebnis an die

1173 *ULD* 2004, unter II.

1174 Vgl. *TAB* 2002, 12; *Janke* 2002, 206 ff. Forschungsarbeit findet in den Projekten FINGER_Card (http://pi.ijs.si/ProjectIntelligence.Exe?Cm=Project&Project=FINGER_CARD) und E-POLL (http://www.e-poll-project.net/) statt. Die Integration in USB-Token ist demgegenüber schon erheblich weiter fortgeschritten, vgl. http://www.cardtechnology.com/cgi-bin/readstory.pl?story=20040715IDNN722.xml.

1175 So z.B. die Systeme von BAI und Astro Datensysteme; s.a. *Janke* 2002, 207; *Struif/Scheuermann*, in: Reichl/Roßnagel/Müller 2005, 175.

1176 *Kallmeyer/Bittlinger/Struif/Scheuermann/Köppen*, in: Reichl/Roßnagel/Müller 2005, 73 ff.

Peripherie meldet. Im Ergebnis erscheint eine Lösung mit Sensor auf der Karte für den digitalen Personalausweis nicht geeignet.[1177]

Damit verbleiben die Möglichkeiten eines Matching-On-Cards mit externem Sensor und eines Matchings in der Peripherie, bei dem die Daten aus dem digitalen Personalausweis ausgelesen werden. Beiden ist gemein, dass biometrische Daten durch die kontrollierende Stelle mittels eines externen Sensors erhoben werden. Darauf gründet sich in beiden Fällen die Gefahr des Missbrauchs, sodass im Rahmen des normalen Kontrollvorgangs unter Verhältnismäßigkeitsgesichtspunkten kein Unterschied besteht. Der Vorteil des Matching-On-Cards besteht allerdings darin, dass die biometrischen Daten überhaupt nicht, also auch nicht außerhalb eines berechtigten Kontrollvorgangs aus der Karte ausgelesen werden können: Da der Chip nur Daten empfängt, vergleicht und Ergebnisse des Matchings sendet, ist dies unmöglich.[1178] Auch diese Variante des Matching-On-Cards ist damit ein geringerer Eingriff in die informationelle Selbstbestimmung als ein Matching in der Peripherie. Der Unterschied zwischen den Verfahren kann allerdings durch Schutzmaßnahmen entscheidend vermindert werden, insbesondere durch die verschlüsselte Speicherung der biometrischen Daten und die Überprüfung und Zertifizierung der verwendeten Kontrollgeräte.[1179] Wenn die Zertifikate im Rahmen einer gegenseitigen Authentisierung durch die Karte überprüft werden, so kann deren Funktionsweise technisch auf eine Übermittlung der Daten des Chips an derartig zertifizierte Geräte beschränkt werden. In Anbetracht dieser Sicherungsmöglichkeiten und unter Berücksichtigung der Sicherheitsprobleme (die auch diese Form des Matching-On-Cards verursacht) ist eine Matching-On-Card Lösung aufgrund der nur geringfügig geringeren Eingriffsintensität nicht zwingend erforderlich.

Bei allen biometrischen Vorgängen, die außerhalb des digitalen Personalausweises zum Anfall biometrischer Daten führen, ist schließlich sicherzustellen, dass diese nicht missbräuchlich verwendet werden können.[1180] Das Verhältnismäßigkeitsprinzip verlangt den Einsatz kleiner autonomer Einheiten zum Matching, die schon rein technisch keine dauerhafte Speicherung oder anderweitige Übermittlung der vom Sensor kommenden (Roh-)Daten zulassen. So entsteht ein geringerer Eingriff als beim Einsatz größerer Datenverarbeitungsanlagen, bei denen eine Speicherung dieser Daten technisch möglich und lediglich rechtlich unzulässig ist. Zwar verbleibt das Problem des Missbrauchs, weil auch an abgeschotteten Kontrolleinheiten so manipuliert werden kann, dass doch eine Speicherung der Daten möglich wird. Hierzu sind jedoch technische Kenntnisse und eine hohe kriminelle Energie erforderlich, sodass ein deutlicher datenschutzrechtlicher Vorteil verbleibt.

4.2.2.4.5 Kontaktlose Schnittstellen

Kontaktlose Schnittstellen haben aus technischer Sicht gegenüber kontaktbehafteten Systemen die Vorteile höherer Übertragungsraten und geringerer Verschleißerscheinungen. Deshalb hat sich auch die ICAO für derartige RF-Chips ausgesprochen.[1181] Aus daten-

1177 In Einsatzfeldern mit anderen Sicherheits- und Belastungsanforderungen wird sich dies regelmäßig anders darstellen. Aufgrund des datenschutzrechtlichen Vorteils ergibt sich eine Vielzahl von Anwendungsfeldern für Biometriekarten mit Fingerabdrucksensoren.

1178 Vgl. *Roßnagel/Hornung*, in: Reichl/Roßnagel/Müller 2005, 234 f.; *dies*., DuD 2005, 69, 72 f.

1179 S. *Konferenz der Datenschutzbeauftragten* 2002, unter 3.1 und näher unten 6.2.1.2, 6.2.1.3; dort auch zu den Problemen bei der Herstellung internationaler Interoperabilität.

1180 *Roßnagel/Hornung*, in: Reichl/Roßnagel/Müller 2005, 140. Entsprechend verbietet auch bislang § 3a Abs. 2 PersAuswG die Speicherung beim automatisierten Auslesen im Rahmen von Kontrollen.

1181 S. *ICAO* 2004a, 35; ausführlich *ICAO* 2004b.

schutzrechtlicher Sicht sind diese jedoch grundsätzlich problematisch,[1182] weil der Ausweisinhaber praktisch nicht erkennen kann, ob Daten von der Karte erhoben oder auf dieser verarbeitet werden. Wenn keine technischen Gegenmaßnahmen ergriffen werden, widerspricht dies dem Prinzip der Direkterhebung, das eine Ausprägung des Transparenzgrundsatzes ist und nicht nur eine Erhebung direkt beim Betroffenen fordert, sondern auch, dass dieser hiervon Kenntnis erlangt.[1183] Im Grundsatz sind damit kontaktorientierte Systeme kontaktlosen vorzuziehen.

Ist beim digitalen Personalausweis aus technischen Gründen – etwa der Gefahr von schnellen Abnutzungserscheinungen aufgrund einer Vielzahl von Steckzyklen in kurzer Zeit – der Einsatz kontaktorientierter Chips nicht praktikabel, sind zumindest Maßnahmen zur Herstellung von Transparenz zu ergreifen. Eine Möglichkeit zur Umsetzung dieser Anforderung ist etwa der Einsatz von Lesegeräten, die das Aussenden und Empfangen von Daten durch Licht- oder Lautzeichen anzeigen. Außerdem bietet sich die Verwendung von Chips an, die – wie „close-coupled" und „proximity" Karten entsprechend den Normen ISO/IEC 10536 und 14443 – nur von Lesegeräten ausgelesen werden können, die sich in einem sehr geringen Abstand (1 beziehungsweise 10 cm) zum Lesegerät befinden. In diesem Fall besteht nur dann noch ein Unterschied zum Einführen in das Gerät, wenn mit manipulierten Geräten (die etwa Feldstärken außerhalb des Standards verwenden) doch ein Auslesen aus größerer Entfernung möglich ist („skimming") oder die Kommunikation des Chips mit einem berechtigten Lesegerät abgehört werden kann („eaves-dropping").[1184]

Darüber hinaus kann der Zugriff auf die Daten des Chips von vornherein auf bestimmte Lesegeräte beschränkt werden, indem sich Chip und Lesegerät gegenseitig authentifizieren, bevor es zu einem Datenaustausch kommt. Hierdurch kann verhindert werden, dass Nichtberechtigte Daten aus dem Ausweis auslesen, ohne dass der Inhaber dies bemerkt. Beim Austausch sensibler Daten in geschlossenen Systemen kontaktlos betriebener Karten und Lesegeräte ist eine solche Lösung zu wählen. Sie gestaltet sich allerdings dann schwierig, wenn es – wie beim digitalen Personalausweis – um Chipkarten geht, die zumindest europaweit einsetzbar sein sollen.[1185] Als letzte Lösung verbleibt für den Bürger schließlich der Selbstschutz, etwa der Transport des Ausweises in einer Verpackung, die das vom Lesegerät ausgehende elektromagnetische Feld abschirmt. Hierzu reicht eine einfache Metallhülle oder Aluminiumfolie aus.[1186]

4.2.2.4.6 Zugriffsschutz

Um den Ausweisinhaber vor einer missbräuchlichen Verwendung seiner sensiblen biometrischen Daten zu bewahren, müssen technische Mechanismen des Zugriffsschutzes eingerichtet werden. Das ist vor allem bei den soeben beschriebenen kontaktlosen Schnitt-

1182 *BT-Enquetekommission Zukunft der Medien* 1998, 54; *Roßnagel/Pfitzmann/Garstka* 2001, 185; *Bizer* 2002, 28; *ACLU* 2004, 1 ff.; s.a. *Hornung* 2004b, 53.

1183 *Auernhammer*, § 13 Rn. 12; *Bergmann/Möhrle/Herb*, § 13 Rn. 13; Simitis-*Sokol*, § 4 Rn. 20.

1184 Diese Risiken sind durchaus real. Bei Tests im Zusammenhang mit dem US-amerikanischen „National Biometric Security Project" wurde bspw. festgestellt, dass die untersuchten Chips noch aus einer Entfernung von neun Metern auszulesen waren, vgl. OMNICARD-newsletter September 2004/2; *ACLU* 2004, 4; *Kügler*, c't 5/2005, 84, 85.

1185 S. zu den entsprechenden Möglichkeiten unten 6.2.1.2.

1186 Diese schirmen die elektromagnetische Strahlung ab, mit der kontaktlose Chips ausgelesen werden, s. *ICAO* 2004b, 14; *Kügler*, c't 5/2005, 84, 85. Zumindest beim Reisepass wäre es problemlos möglich, eine derartige Folie in die äußere Hülle des Dokuments zu integrieren. Es ist deshalb kaum verständlich, warum dies in den derzeitigen Planungen keine Rolle spielt.

stellen von großer Bedeutung, gilt aber wegen der Gefahr des Auslesens nach einem Verlust des Ausweises auch für kontaktorientierte Chips.

Bei der Frage des Zugriffsschutzes handelt es sich um eine verfassungsrechtliche Anforderung. Es wäre mit dem Grundrecht auf informationelle Selbstbestimmung nicht vereinbar, den digitalen Personalausweis so zu konstruieren, dass Nichtberechtigte mit einem handelsüblichen Kartenlesegerät und entsprechenden technischen Kenntnissen Zugriff auf die biometrischen Daten haben. Insofern ist die geltende Gesetzesformulierung in § 1 Abs. 4 Satz 2 PersAuswG, wonach die biometrischen Merkmale „auch" in verschlüsselter Form aufgebracht werden dürfen, zumindest missverständlich. Wenn die Norm so interpretiert würde, dass der Exekutive die Wahl zwischen einer verschlüsselten und einer unverschlüsselten Speicherung verbliebe, so wäre dies zumindest dann verfassungsrechtlich nicht akzeptabel, wenn auch kein alternatives Sicherungsverfahren installiert würde.[1187] Die „angekündigte" künftige Regelung des Gesetzgebers, die nach § 1 Abs. 5 Satz 1 PersAuswG auch die Art der Speicherung der biometrischen Daten bestimmen soll, muss diese Vorgabe einhalten. Für den Reisepass verlangt Art. 1 Abs. 3 der (in Deutschland unmittelbar geltenden) Verordnung (EG) Nr. 2252/2004[1188] die technische Eignung zur Sicherstellung der Vertraulichkeit der Daten.

Aus technischer Sicht kann der Zugriffsschutz mit verschiedenen Mitteln erreicht werden. Die beiden gängigsten Methoden sind die Verschlüsselung und die gegenseitige Authentisierung zwischen Karte und Lesegerät. Die Umsetzbarkeit beider Verfahren wird später behandelt.[1189]

Wenn auf dem digitalen Personalausweis neben der hoheitlichen Identifizierungsfunktion noch weitere Applikationen (insbesondere eine Signaturfunktion) ablaufen, so fordern die Prinzipien der Zweckbindung und der informationellen Gewaltenteilung, Speicher- und Verarbeitungsbereiche auf der Karte getrennt einzurichten und sauber gegeneinander abzuschotten. Zugriffsberechtigte (seien es der Karteninhaber selbst oder eine verantwortliche Stelle) sind auf technischem Wege davon abzuhalten, auf die Speicherbereiche außerhalb ihrer Berechtigung zugreifen zu können. Deshalb ist ein Zugriff staatlicher Stellen auf die Signaturfunktion auszuschließen.[1190] Umgekehrt erfordert die Identifikationsfunktion, jedweden – zumindest schreibenden – Zugriff (auch des Inhabers) auf die biometrischen und andere hoheitliche Daten zu verhindern.

4.2.2.4.7 Einrichtung effektiver Rückfallsysteme

Werden biometrische Verfahren auf große Nutzergruppen angewendet, so ist damit zu rechnen, dass Teile dieser Gruppen aus unterschiedlichen Gründen nicht oder nur schwer erkannt werden können. Das kommt mit zwei verfassungsrechtlichen Anforderungen in Konflikt, nämlich den Prinzipien der Eignung und der objektiven Zumutbarkeit der eingesetzten Maßnahme.

Unter dem Gesichtspunkt der Eignung ist es aus staatlicher Sicht unabdingbar, dass der Gesamtprozess auf eine temporäre oder dauerhafte Ungeeignetheit eines Ausweisinhabers zur Erkennung eingerichtet ist. Im Rahmen der Verhältnismäßigkeitsprüfung ist außerdem die Frage zu beantworten, ob die Belastungen, die die Verwendung biometrischer Daten für die Betroffenen mit sich bringt, im Hinblick auf das Ziel einer Erhöhung der Identifi-

1187 Im Ergebnis ist ist auch nach der derzeitigen Gesetzesfassung eine Verschlüsselung erforderlich, vgl. *Roßnagel/Hornung*, in: Reichl/Roßnagel/Müller 2005, 140; *dies*., DuD 2005, 69, 71.

1188 Vgl. dazu *Roßnagel/Hornung*, DÖV 2005, i.E. und oben 3.1.2.

1189 S.u. 6.2.1.2, 6.2.1.3.

1190 Dies ist darüber hinaus auch eine signaturrechtliche Anforderung, s.u. 5.1.2.

zierungssicherheit des digitalen Personalausweises objektiv zumutbar sind. Der Gesetzgeber hat dabei Sicherheits- und Freiheitsinteressen in ein angemessenes Verhältnis zu bringen.[1191]

Bei der Abwägung ist nicht etwa das (sehr hohe) generelle staatliche Interesse an einer sicheren Identifizierung, sondern das an der Erhöhung der Identifizierungssicherheit gerade durch die Verwendung von Biometrie anzusetzen. Letzteres kann je nach der Sicherheit oder Unsicherheit des momentanen Ausweises gegen Fälschung und Identitätstäuschung einerseits und der Zuverlässigkeit oder Unzuverlässigkeit biometrischer Systeme andererseits größer oder kleiner sein. Aus der nationalen Perspektive ist die Aufnahme biometrischer Merkmale in den Personalausweis grundsätzlich nur dann erforderlich, wenn Fälschung oder Identitätstäuschung beim bisherigen Modell tatsächlich ein Problem sind.[1192] Das Bundesministerium des Innern war jedoch beispielsweise im Rahmen einer Kleinen Anfrage der FDP-Fraktion im Januar des Jahres 2005 nicht in der Lage, konkrete Zahlen zu Passfälschungen vorzulegen.[1193] Dieser Einwand wird allerdings dadurch relativiert, dass eine Aufnahme biometrischer Daten den deutschen Staat in die Lage versetzt, gleiches auch von anderen Staaten zu fordern, so die im Ausland regelmäßig niedrigeren technischen Standards anzuheben und damit auch in Deutschland für ein höheres Sicherheitsniveau zu sorgen.

Die Belastungen der Personalausweisinhaber werden durch die beschriebenen Anforderungen an das Gesamtsystem (keine dauerhafte Speicherung außerhalb des Ausweises, Verwendung abgeschotteter Kontrollgeräte, Merkmalsauswahl unter Erforderlichkeitsgesichtspunkten, nach Möglichkeit Speicherung in Form von Templates) entscheidend vermindert. Deshalb stehen sie für den Ausweisinhaber im Regelfall nicht außer Verhältnis zum angestrebten Ziel und sind damit objektiv zumutbar. Zu fordern ist jedoch, dass tatsächlich ein signifikanter Sicherheitsgewinn zu erwarten ist.

Die objektive Zumutbarkeit ist dann anders zu beurteilen, wenn das Gesamtsystem für eine oder mehrere Gruppen von Ausweisinhabern zusätzliche Belastungen über den eigentlichen Kontrollvorgang hinaus mit sich bringt.[1194] Diese können insbesondere entstehen, wenn ein Betroffener

- temporär oder dauerhaft für das biometrische Verfahren ungeeignet ist oder
- zwar grundsätzlich geeignet ist, jedoch aus besonderen Gründen (insbesondere der Zugehörigkeit zu einer Gruppe, deren Diskriminierung in Art. 3 Abs. 2 und 3 GG untersagt wird) signifikant schlechter erkannt wird als der durchschnittliche Benutzer.

In beiden Fällen wirken die Erfordernisse der Eignung und objektiven Zumutbarkeit des Eingriffs zusammen. Ein biometrisches System ist nur dann geeignet und objektiv zumutbar, wenn der Gesamtprozess auf eine temporäre oder dauerhafte Unbenutzbarkeit durch einzelne Merkmalsträger eingerichtet ist. Für die Fälle einer einfachen Schnittverletzung

---

1191 Zum grundsätzlichen Verhältnis dieser beiden im demokratischen Verfassungsstaat s. *Koch* 2002, 3 ff., 39 ff.; *Callies*, DVBl. 2003, 1096 ff. und die Beiträge in *Roßnagel* (Hrsg.), Sicherheit für Freiheit?, 2003; speziell zum Verhältnis von biometrischen Merkmalen und innerer Sicherheit *Koch* 2002, 16 ff.

1192 *Konferenz der Datenschutzbeauftragten* 2002, unter 2.1; *Kutscha* 2001, 1. Im Rahmen der Technikfolgenabschätzung von Chipkartensystemen ist stets auch die sog. Nullvariante zu prüfen, d.h. die Beibehaltung der bisher verwendeten Verfahren, s. Roßnagel-*Weichert*, Kap. 9.5, Rn. 58; allgemeiner *Roßnagel/Wedde/Hammer/Pordesch* 1990, 284.

1193 S. BT-Drs. 15/4616, 2. Danach wurden 2002 von der Grenzschutzdirektion 35 deutsche Pässe und 30 sonstige Ausweise wegen Verdachts auf Verfälschung oder fälschliche Ausstellung untersucht. Wie viele Fälschungen dabei tatsächlich entdeckt wurden, bleibt offen.

1194 Vgl. *Roßnagel/Hornung*, in: Reichl/Roßnagel/Müller 2005, 228; 234; *dies*., DuD 2005, 69, 71.

oder eines Bruch des Fingers, einer Gesichtsverletzung oder Augenkrankheit[1195] ist die Zurückweisung des Ausweisinhabers nicht hinnehmbar.

Gleiches gilt dann, wenn der Betroffene keine oder eine zu geringe Merkmalsausprägung aufweist. Schätzungen gehen von 2 bis 5 % der Gesamtbevölkerung aus, bei denen jedes einzelne biometrische Verfahren nicht angewendet werden kann.[1196] Das trifft aber zumindest für das Gesicht nicht zu: Von schwersten Verstümmelungen abgesehen, können alle Menschen in diese Systeme enroled werden.[1197] Dies war einer der Gründe für die ICAO, den Staaten die Verwendung von Gesichtsdaten in Reisedokumenten zu empfehlen.[1198] Zu beachten ist, dass trotz der prinzipiellen Eignung zum Enrolment dieses in manchen Fällen fehlschlagen wird, weil das Merkmal mangelhaft erfasst oder verarbeitet wird. Auch bei der Gesichtserkennung verbleibt also eine gewisse FER.

Bei der Iris und dem Fingerabdruck gibt es dagegen einen Prozentsatz von Bürgern, die vollständig nicht zur Erfassung geeignet sind. Die Ergebnisse für den Fingerabdruck schwanken von 1 bis 5 %.[1199] Eigenangaben des Herstellers von Iriserkennungssystemen Iridian gehen für die Iris von 0,6 % aus.[1200] Die mangelnde Eignung kann angeboren oder verhaltensabhängig sein. So sind etwa blinde Menschen nicht zum Einsatz des Iris-Scans geeignet.[1201] Allein daraus resultiert für Deutschland eine Unanwendbarkeitsrate von ca. 0,2 %.[1202] Auch Irisveränderungen, die bei Morbus Wilson, Irisitis, Pupillenanomalien, physischen Zerstörungen und Nystaghmus die Regel sind, verhindern die Erkennung. Aus diesem Grund wurden Menschen mit diesen Erkrankungen beispielsweise von dem Feldversuch ausgeschlossen, den der Bundesgrenzschutz seit dem 13. Februar 2004 am Frankfurter Flughafen durchführt.[1203] Fehlende Gliedmaßen aufgrund von Amputationen oder Conterganschäden[1204] machen den Einsatz von Fingerabdrucksverfahren unmöglich. Bei diesen gibt es außerdem in der Gruppe körperlich arbeitender Berufstätiger einen hohen Anteil von Betroffenen, deren Fingermuster durch Abrieb nicht hinreichend ausgeprägt ist.[1205]

Auch für den Fall einer im Laufe der Zeit eintretenden Merkmalsänderung, die insbesondere bei der Gesichtserkennung ein Problem darstellen kann,[1206] muss ein Alternativverfahren vorgehalten werden. Der Fingerabdruck bleibt demgegenüber im Laufe des Lebens im Wesentlichen unverändert. Er kann sich aber durch unmittelbare mechanische Einflüsse (Abnutzung durch körperliche Arbeit oder Verletzungen des Fingers) verändern.[1207] Einige Augenkrankheiten haben eine Eintrübung der Iris zur Folge. Insgesamt fehlt es noch an Daten über die Langzeitstabilität biometrischer Merkmale.[1208] Bei einer

1195 S. *Behrens/Roth* 2001a, 14; *TAB* 2002, 15.
1196 Roßnagel-*Gundermann/Probst*, Kap. 9.6, Rn. 10 (2 %); *TAB* 2002, 23 (5 %); s.a. *Albrecht* 2003a, 36.
1197 *Booz Allen Hamilton/Bundesdruckerei/ZN Vision* 2003, 65 (zitiert nach *TAB* 2004, 31).
1198 *ICAO* 2004a, 17.
1199 *Sietmann*, c't 5/2002, 146 (2-4 %); *Woodward/Orlans/Higgins* 2003, 22 (1-4 %); *TAB* 2004, 31 (2 %); *LSE* 2005, 50 (2-5 %); s.a. *Nanavati/Thieme/Nanavati* 2002, 59.
1200 S. *Fenner* 2003; ähnlich *Bolle/Connell/Pankanti/Ratha/Senior* 2004, 114 und *LSE* 2005, 51 (0,5 %).
1201 *Woodward/Orlans/Higgins* 2003, 99; s.a. *LSE* 2005, 51 ff.
1202 Die Zahl der blinden Menschen in Deutschland wird vom Deutschen Blinden- und Sehbehindertenverband e.V. mit 155.000 angegeben, s. http://www.dbsv.org/infothek/infothek.html ##top. Allerdings fallen auch Personen mit einer Sehfähigkeit von bis zu 2 % unter die Definition der Blindheit, von denen vermutlich einige für die Iriserkennung geeignet sind.
1203 S. http://www.bundesgrenzschutz.de/Auto_Grenzkontrolle/FAQ/index.php (unter 6).
1204 *TeleTrusT* 2002, 51; *VZBV* 2002, 38.
1205 *Breitenstein* 2002, 40.
1206 S.o. 4.2.2.4.1.1.
1207 S. *Breitenstein* 2002, 35.
1208 *Woodward/Orlans/Higgins* 2003, 38.

Veränderung der Daten gibt es zwar die Möglichkeit adaptiver Systeme, bei denen der Referenzdatensatz bei jedem Matching angepasst wird. Dies setzt jedoch eine – wie auch immer gesicherte – Schreibberechtigung voraus, die stets ein Sicherheitsrisiko mit sich bringt.[1209] Diese Vorgehensweise ist deshalb für den digitalen Personalausweis ungeeignet.

Eine andere Form der Belastung besteht für bestimmte Bevölkerungsgruppen, die zwar grundsätzlich zur biometrischen Authentifikation geeignet sind, jedoch geringere Matchingscores aufweisen. Wenn diese Unterschiede hinreichend signifikant sind, kommt es zu einer Verletzung des Gleichheitssatzes (Art. 3 GG).[1210] Die absoluten Diskriminierungsverbote nach Art. 3 Abs. 2 und 3 GG können bei einigen biometrischen Merkmalen eingreifen:

- Nach den Ergebnissen des Face Recognition Vendor Test 2002 werden bei der Gesichtserkennung Männer um bis zu 9 % besser erkannt als Frauen.[1211] Je nach Algorithmus kann es auch Schwierigkeiten mit Menschen dunkler Hautfarbe geben.[1212] Weiterhin ergeben sich Unterschiede nach dem Alter: Die Erkennungsraten steigen vom 18. bis zum 63. Lebensjahr etwa um 5 % pro Dekade.[1213] Eine Diskriminierung aufgrund Alters wird zwar „nur“ vom allgemeinen Gleichheitssatz des Art. 3 Abs. 1 GG erfasst. Da hier jedoch kein rechtfertigender Umstand erkennbar ist, ist sie gleichfalls unzulässig.
- Auch der Fingerabdruck weist Unterschiede in der Ausprägung zwischen Männern und Frauen, sowie zwischen verschiedenen ethnischen Gruppen auf.[1214] So gibt es anscheinend bei asiatischen Frauen Probleme mit den bisherigen Systemen zur Fingerabdruckserkennung.[1215] Ältere Menschen können mehr Probleme mit dem Enrolment haben als jüngere.[1216]
- Beim Iris-Scan sollen nach dem gerade entstehenden Standard (ISO/IEC 19794-6) ca. 70 % der Iris im sichtbaren Bereich liegen, das heißt Verdeckungen durch spiegelnde Reflektion, Augenlieder, Augenwimpern oder andere Störungen dürfen nicht mehr als 30 % der Iris ausmachen. Dies kann sich bei bestimmten ethnischen Gruppen (etwa aus Fernost) schwierig gestalten.[1217]

Eine weitere Beeinträchtigung ergibt sich daraus, dass es stets einen Grenzbereich zwischen zum Enrolment geeigneten und ungeeigneten Personen geben wird.[1218] Werden die Merkmalsträger in diesem Grenzbereich als zur Nutzung geeignet definiert, so haben sie

---

1209 *Albrecht* 2002c, 142 f.; *Nolde* 2002, 23.

1210 Dabei sollte nicht übersehen werden, dass biometrische Verfahren hier auch Vorteile haben: Da sie automatisiert ablaufen, diskriminieren sie nicht bewusst nach äußeren Merkmalen (*Woodward* 2001, 12; *Eaton* 2003, xxxiii).

1211 *Phillips*/*Grother*/*Micheals*/*Blackburn*/*Tabassi*/*Bone* 2002, 3. Derartige Unterschiede sind bei biometrischen Verfahren nicht unüblich. So haben Frauen bei der Stimmerkennung Nachteile, vgl. *Breitenstein* 2002, 61.

1212 *Breitenstein* 2002, 46.

1213 *Phillips*/*Grother*/*Micheals*/*Blackburn*/*Tabassi*/*Bone* 2002, 3; s.a. *BSI/BKA/Secunet* 2004, 70.

1214 *Breitenstein* 2002, 40. Ethnische Unterschiede finden sich auch bei Verfahren, die in dieser Arbeit nur am Rande betrachtet werden. So wird vom US-amerikanischen INSPASS-Programm, das mit Handgeometrie arbeitet, über Probleme bei Menschen mit kleinen Händen (insbesondere japanische Flugbegleiter) berichtet, s. *Woodward/Orlans/Higgins* 2003, 289.

1215 S. http://www.silicon.de/cpo/news-itsecurity/detail.php?nr=13425. Offenbar unterscheiden sich die Fingerabdruckscharakteristika verschiedener ethnischer Gruppen, vgl. *Woodward/Orlans/Higgins* 2003, 32 m.w.N.

1216 *Nanavati/Thieme/Nanavati* 2002, 59.

1217 Zu den Problemen s. *Breitenstein* 2002, 49.

1218 *Roßnagel/Hornung*, in: Reichl/Roßnagel/Müller 2005, 234.

eine höhere „individuelle“ FRR zu erwarten.[1219] Sie sind damit im Ergebnis sogar schlechter gestellt als Ausweisinhaber, die klar ungeeignet sind.

In allen diesen Fällen kann es für die Betroffenen an Kontrollstellen zu erheblichen Nachteilen kommen. Diese können von leichten Zeitverzögerungen bis hin zum Verpassen wichtiger Termine oder zu Falschverdächtigungen reichen. Diese Nachteile sind nicht gleichmäßig über die Bevölkerung verteilt, sondern auf bestimmte Gruppen konzentriert, die ständig mit Beeinträchtigungen zu rechnen haben. Dies stellt eine Ungleichbehandlung dar, die insbesondere deswegen schwerwiegend ist, weil sie durch die Betroffenen nicht beeinflusst werden kann.[1220] Aufgrund der ständig wiederkehrenden Konstellation einer intensiveren Kontrolle könnte es auch zu Frustrationserfahrungen kommen. Eine solche Situation ist unter dem Kriterium der objektiven Zumutbarkeit nicht hinnehmbar. Deshalb sind an die notwendigen staatlichen Ausgleichsmaßnahmen hohe Anforderungen zu stellen.

Wie hoch die Gesamtzahl der Ausweisinhaber sein wird, die zum jeweiligen Zeitpunkt dauerhaft oder übergangsweise nicht biometrisch erkannt werden können oder nicht akzeptable individuelle Falschzurückweisungsraten aufweisen, kann kaum abgeschätzt werden.[1221] Es werden aber in jedem Fall so viele Bürger betroffen sein, dass schon im eigenen Interesse des Staates, insbesondere aber zur Vermeidung objektiv unzumutbarer Belastungen der Betroffenen effektive Alternativverfahren in ausreichender Zahl vorgehalten werden müssen.[1222] Dafür gibt es mehrere Möglichkeiten. Denkbar ist zunächst, anstatt der biometrischen Daten eine Angabe darüber zu speichern, dass der betroffene Ausweisinhaber für die biometrische Verifikation nicht geeignet ist. Daran dürften dann allerdings keine weiteren belastenden Folgen bei Kontrollen geknüpft werden. Eine andere Variante ist, für Personen mit schwach ausgeprägten Merkmalen individuelle Matchingscores zu definieren.[1223] Diese Ausweisinhaber würden dasselbe biometrische System verwenden, jedoch bereits bei einem geringeren Übereinstimmungsgrad zwischen den Referenzdaten und den neu erhobenen Merkmalsdaten vom System akzeptiert werden. Beide Lösungen bringen allerdings Sicherheitsdefizite mit sich.

Denkbar ist es auch, zwei oder mehr Merkmale zu kombinieren. Hierdurch kann nicht nur die Eignung des Gesamtsystems verbessert,[1224] sondern auch die Beeinträchtigung auf der Ebene der objektiven Zumutbarkeit vermindert werden. Die Schnittmenge der jeweils ungeeigneten Gruppen dürfte relativ gering sein. Allerdings bringt die Verwendung eines weiteren Merkmals auch zusätzliche Belastungen mit sich, da ein weiteres Datum verwendet wird, welches eigene datenschutzrechtliche Folgeprobleme bedingt. Bei Einhaltung der beschriebenen Anforderungen an den Umgang mit den biometrischen Daten ist jedoch auch die Verwendung zweier Merkmale objektiv zumutbar.

In jedem Fall ergibt sich als Grundanforderung aus den Erfordernissen der Eignung und der objektiven Zumutbarkeit, den digitalen Personalausweis technisch so auszugestalten,

---

1219 Im Projekt BioP I wiesen z.B. zwei (von 241) Testpersonen eine FRR von 10 % auf, während beim überwiegenden Teil der Testpopulation keine Falschabweisungen auftraten, s. *BSI/BKA/Secunet* 2004, 56.

1220 Zu diesem Kriterium vgl. BVerfGE 88, 87 (96); 91, 389 (401).

1221 Allgemein gibt es im Bereich der Biometrie bislang so gut wie keine Forschungsergebnisse zu den Anforderungen an effektive Rückfallsysteme, s. *Rejman-Greene* 2003b, 77.

1222 S.a. *Albrecht* 2002c, 137 f.; *Behrens/Roth* 2001b, 14 f.; *Art. 29 DPWP* 2004, 6 f.; *JRC/IPTS* 2005, 11, 78 f.

1223 Roßnagel-*Gundermann/Probst*, Kap. 9.6, Rn. 18; *Woodward/Orlans/Higgins* 2003, 31 (dort allerdings umgekehrt: individuell höhere Scores zur Erhöhung der Sicherheit einer bestimmten Anwendung).

1224 S. zum Einfluss der Kombination zweier Merkmale auf die Fehlerraten des Gesamtsystems oben 4.2.2.4.1.1.

dass eine herkömmliche, manuelle Ausweisprüfung jederzeit durchführbar bleibt. Aufgrund der stets gegebenen Möglichkeit einer Falschabweisung darf eine abweisende Entscheidung keinesfalls allein auf ein negatives Matching-Ergebniss gegründet werden mit der Folge, dass nunmehr der Betroffene seine Identität beweisen muss.[1225] An Kontrollstellen sind hinreichende personelle und räumliche Ressourcen vorzuhalten, um eine manuelle Nachkontrolle in einem Zeitraum zu ermöglichen, der insbesondere an den Grenzen und Flughäfen nicht zu unzumutbaren Verzögerungen für die Reisenden führt.

Umgekehrt ist – mit Blick auf die Möglichkeit einer Falschakzeptanz – auch vor einem zu großen Vertrauen der Kontrollpersonen in das technische System zu warnen. Die Einrichtung biometrischer Verfahren birgt die Gefahr des Wegfalls subjektiver Erfahrungen, die sich das staatliche Personal im Rahmen langjähriger Kontrollen erwirbt. Gegenwärtig gründen viele Beamte ihre Entscheidung über die Erforderlichkeit einer eingehenderen Kontrolle nicht – oder nicht nur – auf einen Vergleich der Daten (insbesondere des Bildes) eines Ausweises mit der Person, die vor ihnen steht. Vielmehr fällt ihnen aufgrund ihrer Berufserfahren abnormales Verhalten auf. Nach Auskünften aus der Praxis ist diese Form der Entscheidung bei den meisten Fahndungserfolgen an der Grenze zumindest beteiligt. Beim Einsatz eines biometrischen Verfahrens besteht die Gefahr, dass die Beamten sich zu sehr auf das technische Testergebnis verlassen. Dem kann zwar durch entsprechende Schulungen entgegengewirkt werden. Ob damit eine Gewöhnung an die Orientierung am Matchingergebnis verhindert werden kann, ist allerdings fraglich.

4.2.2.5 Einsatz im privaten Bereich

Nach § 4 Abs. 1 PersAuswG kann der Personalausweis auch im nichtöffentlichen Bereich als Ausweis- und Legitimationspapier benutzt werden. Es ergibt sich die Frage, ob danach zumindest der lesende Zugriff des Inhabers oder eines privaten Dritten auf die biometrischen Daten und die anschließende Identitätsprüfung mit diesen zulässig ist. Von Interesse wäre dies insbesondere für die Kontrolle von privaten Hochsicherheitsbereichen, die Prüfung durch Kreditinstitute oder allgemein beim Zusammentreffen mit bislang unbekannten Vertragspartnern. Denkbar wären daneben aber auch ein Einsatz für den Zugang zum Arbeitsplatz oder eigene Anwendungen wie ein Log-In am heimischen PC.

§ 4 Abs. 2 und 3 PersAuswG beschränken gegenwärtig den Einsatz im nichtöffentlichen Umfeld.[1226] § 4 Abs. 2 PersAuswG bezieht sich lediglich auf die Verwendung der Seriennummer und ist deshalb für biometrische Merkmale nicht einschlägig. Nach § 4 Abs. 3 PersAuswG darf der Personalausweis weder zum automatischen Abruf personenbezogener Daten noch zur automatischen Speicherung personenbezogener Daten verwendet werden.

Sofern ein Matching außerhalb des digitalen Personalausweises erfolgt, müssen hierzu die Daten aus dem Chip ausgelesen und zum Matching zumindest kurzzeitig gespeichert werden. Beides kann nur automatisiert erfolgen. Deshalb wäre ein entsprechendes Vorgehen zurzeit rechtswidrig. § 4 Abs. 3 PersAuswG lässt dagegen ein Matching-On-Card Verfahren zu, auch wenn dabei kurzzeitig eine automatische Speicherung der Vergleichsdaten auf dem Kartenchip (zum Matching) stattfindet. Von seinem Normzweck her wendet sich § 4 Abs. 3 PersAuswG nämlich nicht gegen eine Speicherung im ausschließlichen Einflussbereich des Ausweisinhabers. Aus demselben Grund ist in diesem Bereich (beispielsweise zum Zugang zum eigenen PC) bereits nach geltendem Recht ein Einsatz für private Anwendungen zulässig.

1225 *Koch* 2002, 25; vgl. zu diesem Problem noch unten 4.3.5.

1226 S. bereits oben 2.2.1.5.

Zu beachten ist, dass aus Gründen der Fälschungssicherheit im hoheitlichen Bereich voraussichtlich ein Matching in der Peripherie stattfinden wird.[1227] Ohne eine Änderung der Rechtslage könnte deshalb für private Anwendungen nur ein paralleles Matching-On-Card installiert werden, das entweder denselben oder einen zusätzlichen biometrischen Datensatz verwendet. Das führt jedoch zu Problemen hinsichtlich der Speicher- und Rechenkapazität. Überdies bestehen im privaten Bereich in vielen Anwendungen ähnlich hohe Sicherheitsbedürfnisse wie bei der Kontrolle durch staatliche Organe. Angesichts der vielfältigen Einsatzmöglichkeiten im privaten Bereich erscheint die bisherige strikte Regelung in § 4 Abs. 3 PersAuswG nicht sinnvoll und sollte deshalb modifiziert werden.

De lege ferenda könnte eine Regelung den Einsatz der biometrischen Daten unter dem Vorbehalt der Einwilligung des Ausweisinhaber auch im nichtöffentlichen Bereich unter bestimmten Bedingungen zulassen.[1228] Dies ist verfassungsrechtlich dann akzeptabel, wenn die Freiwilligkeit der Einwilligung tatsächlich gesichert ist und technische Schutzmechanismen für die Daten implementiert werden. Ersteres setzt voraus, dass der Betroffene über die Folgen der Einwilligung unterrichtet wird und ohne rechtliche oder faktische Abhängigkeiten entscheiden kann.[1229] In technischer Hinsicht besteht die Möglichkeit einer gegenseitigen Authentisierung mit einem Lesegerät, welches zuvor zertifiziert wurde. In diesem Fall kann der Ausweisinhaber sichergehen, dass seine Daten nicht über das zum Matching erforderliche Maß hinaus gespeichert oder gar weitergegeben werden. Ein strafbewehrtes Verbot könnte außerdem dem Missbrauch der Daten entgegenwirken. Aus staatlicher Sicht stellt der Zugriff Privater auf die elektronisch gespeicherten Daten kein Problem dar, wenn deren Integrität – beispielsweise durch eine elektronische Signatur – sichergestellt wird.

Die Einwilligung des Inhabers ist im Einzelfall technisch abzusichern. Hierzu könnte eine PIN eingesetzt werden.[1230] Ähnlich wie bei der elektronischen Gesundheitskarte sollte überdies ein Protokollierungsmechanismus implementiert werden, mit dem sich die Zugriffe zurückverfolgen ließen. Entsprechende Sicherungsmaßnahmen sind erforderlich, weil sich bei biometrischen Merkmalen das Problem der Profilbildung in weitaus größerem Maße stellt als bei den herkömmlichen Ausweisdaten.[1231] Außerdem besteht im Regelfall im privaten Bereich ein höheres Interesse an möglichen Zusatzinformationen, die in biometrischen Daten enthalten sein können.

1227 S.o. 4.2.2.4.4.

1228 S. bereits *Roßnagel/Gitter/Hornung*, in: Reichl/Roßnagel/Müller 2005, 150 f.; 241; *Hornung*, KJ 2004, 344, 355; *ders.* 2004b, 52.

1229 Vgl. zur Rolle der Einwilligung im Datenschutzrecht kritisch *Simitis*, JZ 1986, 188; Simitis-*Simitis*, § 4a Rn. 2 ff. m.w.N.; umfassend Roßnagel-*Holznagel/Sonntag*, Kap. 4.8, insbes. Rn. 1 ff., 44 ff. Ein Mittel zur Sicherung der Freiwilligkeit könnte die verstärkte Regelung von Kopplungsverboten zwischen der Einwilligung und der erstrebten Verwaltungs- oder Vertragsleistung sein, s. *Roßnagel/Pfitzmann/Garstka* 2001, 92 f.

1230 Hier bietet sich eine Parallelregelung zur elektronischen Gesundheitskarte an, die in § 291a Abs. 5 Satz 2 SGB V (s.o. 2.2.2.2) eine technische Absicherung der Autorisierung des Zugriffs durch den Versicherten vorsieht. Der Unterschied besteht allerdings darin, dass dort biometrische Merkmalsdaten (neben oder anstelle einer PIN) *zum* Zugang zu (Gesundheits-)Daten eingesetzt werden könnten, während es hier um den Zugang *zu* solchen Merkmalsdaten geht.

1231 Zu weitgehend deshalb *DFK* 2004, 13, wo auf eine Vergleichbarkeit mit der bisherigen visuellen Kenntnisnahme des Ausweisphotos abgestellt wird. Beide Vorgänge sind in keinster Weise miteinander vergleichbar.

4.2.2.6 Schutzpflichten für den Einsatz im Ausland?

Mit zunehmender Interoperabilität werden Chipkartenausweise mehr und mehr im Ausland Verwendung finden; bei Personalausweis und Gesundheitskarte gehört dies zur Zweckbestimmung der Karte. Aufgrund des unterschiedlichen Datenschutzniveaus in anderen Staaten kann es zu Datenverwendungen kommen, die nach deutschem Datenschutzrecht unzulässig wären. So könnte etwa ein ausländischer Staat die biometrischen Daten aus dem digitalen Personalausweis auslesen und dauerhaft speichern. Gleiches wäre auch mit den neu zum Matching erhobenen Rohdaten möglich. Der Ausweisinhaber kann nicht wissen, was mit den Daten geschieht, wer sie speichert und wie sie weiterverarbeitet werden. Außerdem besteht die Gefahr, dass es im jeweiligen Land an effektiven Rechtsschutzmöglichkeiten mangelt. Im Extremfall droht sogar das Risiko, dass Daten über Umwege wieder ins Inland kommen, etwa wenn eine private oder öffentliche Stelle des anderen Staates diese zum Verkauf (beispielsweise an einen deutschen Versicherungskonzern) anbietet. Zwar richtet sich bei Datenimporten die anschließende Datenverarbeitung und Nutzung ausschließlich nach dem deutschen Recht.[1232] Es eröffnen sich aber weitgehende Missbrauchsmöglichkeiten. Dies zeigt sowohl die aktuelle Diskussion um die Weitergabe von Flugdaten europäischer Fluggesellschaften an die US-Einwanderungsbehörden,[1233] als auch spektakuläre Datenübermittlungen wie der Ankauf des mexikanischen Wählerverzeichnisses mit den persönlichen Daten von 65 Millionen Mexikanern durch die USA über die internationale Datenfirma ChoicePoint.[1234]

Damit stellt sich die Frage, ob es eine Pflicht des deutschen Staates zum Schutz vor derartigen Gefahren gibt.[1235] Im Grundsatz treffen den Staat Schutzpflichten zugunsten seiner Angehörigen auch dann, wenn diese sich im Ausland befinden.[1236] Das folgt aus dem Grundverhältnis des Staates zu seinen Staatsangehörigen.[1237] Auf der anderen Seite wird der Betroffene sich mit dem Dokument regelmäßig freiwillig ins Ausland begeben haben. Dieses Argument gilt für das Mitführen des digitalen Personalausweises aber nur bedingt, weil deutsche Staatsbürger bei einem Auslandsaufenthalt nur deutsche Reisedokumente verwenden können und diese durch den ausländischen Staat zwangsweise zur Identitätsbestimmung verwendet werden. Insofern besteht durchaus eine Verantwortung des deutschen Staates für die Ausgestaltung dieser Dokumente.

Jeder Staat kann jedoch souverän entscheiden, welche Daten er bei der Einreise erhebt. Die Einflussmöglichkeiten der Bundesrepublik sind daher begrenzt. Mit einer datenschutzfreundlichen technischen Ausgestaltung des digitalen Personalausweises kann zwar versucht werden, die staatliche Schutzpflicht umzusetzen.[1238] Die Wirkung hängt jedoch in weitem Umfang von der Funktionsweise der Peripherie ab, die mit der Karte interagiert. Wenn der digitale Personalausweis beispielsweise mit Matching-On-Card arbeitet, sendet er zwar keine Daten an das Lesegerät des ausländischen Staates. Dieses erhebt jedoch neue

1232 Zur Zulässigkeit von Datenimporten vgl. Simitis-*Simitis*, § 4b Rn. 96 ff. m.w.N.

1233 S. *Schröder*, RDV 2003, 285 ff.; *Räther*, DuD 2004, 468; *Peeters*, MMR 2005, 11 ff., insbes 13 ff.; zum Stand Februar 2004 zusammenfassend *Privacy International* 2004.

1234 Vgl. den Bericht von *Burkeman/Tuckman* 2003; s.a. *Schröder*, RDV 2003, 285, 290 m.w.N.

1235 S. zur verfassungsrechtlichen Herleitung oben 4.2.1.2.6; vgl. zum Folgenden auch *Roßnagel/Hornung*, in: Reichl/Roßnagel/Müller 2005, 110 f.

1236 *Isensee*, HdbStR V (2000), § 111 Rn. 120 ff. Diese Pflicht wird normalerweise im Wege des diplomatischen Schutzes wahrgenommen, s. Sachs-*Kokott*, Art. 87a Rn. 18b; *Stern* 1988, 1247; v. Münch/Kunig-*Kunig*, Art. 1 Rn. 33.

1237 BVerfGE 55, 349 (364 f.); BVerwGE, 62, 11 (14) m.w.N.

1238 S. zu diesem Gedanken Roßnagel-*Trute*, Kap. 2.5, Rn. 46 ff.

Daten des Inhabers (um diese an die Karte zu senden), bei denen der Betroffene sich nicht sicher sein kann, ob eine Speicherung und Weiterverarbeitung erfolgt.

Nimmt man den beschriebenen Gestaltungsspielraum des Staates bei der Erfüllung der Schutzpflicht hinzu,[1239] so folgt aus den datenschutzrechtlichen Gefahren einer Verwendung im Ausland keine konkrete Handlungspflicht des Staates. Andererseits hat das Beispiel der Speicherung der Flugdaten der Reisenden europäischer Fluggesellschaften in die USA gezeigt, dass es durchaus möglich ist, auf der internationalen Ebene datenschutzrechtliche Verbesserungen zu erzielen. In diesem konkreten Fall willigten die USA ein, die Speicherfristen für die Daten erheblich zu verkürzen.[1240] Sofern auf der diplomatischen Ebene für biometrische Daten von Reisenden entsprechende Vereinbarungen getroffen werden könnten, läge hierin eine Möglichkeit für den Staat, die Daten seiner Bürger auch im Ausland wirksam zu schützen.

4.2.3 Die verfassungsrechtliche Zulässigkeit der elektronischen Gesundheitskarte

Anders als beim digitalen Personalausweis besteht für die elektronische Gesundheitskarte eine umfassende gesetzliche Grundlage. Diese enthält aber nur wenige Vorgaben für die technische Umsetzung. Zu prüfen ist damit einerseits die Verfassungsmäßigkeit der bestehenden Regelung, andererseits, inwieweit rechtliche Anforderungen für die technische Umsetzung der unterschiedlichen Anwendungen der Gesundheitskarte bestehen.

4.2.3.1 Grundsätzliche Verfassungsmäßigkeit

Die elektronische Gesundheitskarte wird nach der gesetzgeberischen Konzeption über verpflichtende und freiwillige Funktionen verfügen.[1241] Die drei verpflichtenden Teile (§ 291a Abs. 2 Satz 1 SGB V) sind die Speicherung der Versicherungsstammdaten, die Übermittlung des elektronischen Rezepts sowie die Ablage des Berechtigungsnachweises zur Inanspruchnahme von Leistungen in den Mitgliedstaaten der Europäischen Union. Demgegenüber werden medizinische Notfalldaten, der elektronische Arztbrief, die elektronische Patientenakte, die Daten zur Prüfung der Arzneimitteltherapiesicherheit, vom Patienten selbst zur Verfügung gestellte Daten und Daten über in Anspruch genommene Leistungen und deren vorläufige Kosten für den Versicherten (Patientenquittung) gemäß § 291a Abs. 3 Satz 3 SGB V nur nach Einwilligung des Versicherten gespeichert.

Bei der Frage der grundsätzlichen Zulässigkeit der Gesundheitskarte ist für die Daten der verpflichtenden Funktionen der Verhältnismäßigkeitsgrundsatz zu beachten. Die durch das Vorhaben verfolgten (Haupt-)Ziele der effektiveren Behandlung und Kostenreduzierung[1242] sind legitime staatliche Anliegen. Für die mit dem Telematikeinsatz erreichbaren Effizienzsteigerungen ist ein gleich geeignetes Mittel nicht ersichtlich. Insofern ist der Einsatz der Karte auch erforderlich. Für die objektive Zumutbarkeit ist vor allem entscheidend, dass es nicht um die Erhebung zusätzlicher, sondern um den spezifischen Umgang mit solchen Daten geht, die auch bisher schon im Gesundheitswesen verwendet werden. Der Umgang mit den Stammdaten entspricht dem gegenwärtigen Verfahren[1243] (in dem die

1239 S.o. 4.2.1.2.6; zum Maß des erforderlichen Schutzes für die informationelle Selbstbestimmung s. z.B. BVerfGE 65, 1 (42 ff.); *Zöllner*, RDV 1985, 3, 10 f.; *Mallmann*, CR 1988, 93, 94 f.

1240 S. http://www.heise.de/newsticker/meldung/43025; vgl. allerdings auch die Kritik in *Privacy International* 2004, 3 ff. et passim; s.a. *Peeters*, MMR 2005, 11 ff.

1241 S.o. 2.2.2.2.

1242 S.o. 2.1.2.

1243 Das gilt mit der Einschränkung, dass die Gesundheitskarte eine veränderte Krankenversichertennummer mit einem lebenslang unveränderbaren Bestandteil enthalten wird (§ 290 Abs. 1 Satz 1 SGB V, s.

Krankenversichertenkarte nach § 15 Abs. 2 SGB V ebenfalls bei jedem Arzt und Zahnarzt vorzulegen ist) und wird mit dem europäischen Berechtigungsnachweis lediglich erweitert. Das Verfahren des elektronischen Rezepts gleicht zumindest bei einer Speicherung auf der Karte selbst weitgehend dem bisherigen Ablauf. Beides bedeutet zwar keinen Freibrief für jedweden Umgang mit den Daten. Die maßgeblichen Probleme für die rechtliche Beurteilung stellen sich aber erst auf der Umsetzungsebene, insbesondere beim Ort der Datenspeicherung, dem Zugriffsschutz und der Datensicherheit. Die Einführung der Gesundheitskarte mit ihren verpflichtenden Elementen ist damit grundsätzlich zulässig.

Bei den freiwilligen Applikationen ergibt sich derzeit kein Verhältnismäßigkeitsproblem, da es sich nicht um einen zwangsweisen staatlichen Eingriff handelt. Für die weitere Entwicklung der Telematikstruktur ist aber die Frage von Interesse, ob die verpflichtende Ausgestaltung dieser Anwendungen möglich wäre.

Bei der Einführung von Telematik können durch die gleichzeitige Vorhaltung alternativer Verfahren die beabsichtigten Effizienzgewinne gemindert oder sogar aufgehoben werden. Das gilt auch für die elektronische Gesundheitskarte. Zwar lässt sich die angestrebte Verbesserung der Versorgung für die Inhaber der Gesundheitskarte realisieren, die die freiwilligen Anwendungen nutzen. Auf der Kostenebene schlägt sich jedoch nieder, dass für alle anderen Versicherten die bisherigen Verfahren weitergeführt werden müssen. Überdies kann nach der momentanen gesetzlichen Regelung die Einwilligung jederzeit widerrufen werden (§ 291a Abs. 3 Satz 4, 2. Halbsatz SGB V),[1244] und der Versicherte kann nach § 291a Abs. 6 Satz 1, 1. Halbsatz SGB V die Löschung von Daten auf der Gesundheitskarte und in der Peripherie verlangen, die im Rahmen der freiwilligen Anwendungen und für das elektronische Rezept entstanden sind. Deshalb müssen die beteiligten Leistungserbringer parallele Dokumentationen führen, weil die Daten sonst unwiederbringlich verloren gehen würden.[1245]

Unter diesen Bedingungen erscheint es sogar möglich, dass der Einsatz der Gesundheitskarte in den freiwilligen Applikationen zu einer Kostensteigerung führt. Aus diesem Grund erwartet auch die Praxis, dass das System nur bei einer verpflichtenden Verwendung durch die Versicherten wirtschaftlich betrieben werden kann.[1246] Zwar wurde die Freiwilligkeit der Verwendung im gesamten Gesetzgebungsprozess von allen Beteiligten immer wieder betont.[1247] Dies ist entscheidend auf die Intervention der Datenschutzbeauftragten zurückzuführen.[1248] Gleichzeitig rückte der Gesetzgeber jedoch von dem Plan ab, auch den Einsatz als rein administrative Karte (das heißt auch ohne die Funktion des elektronischen Rezepts) zu ermöglichen. Insofern erscheint es nicht unwahrscheinlich, dass

---

dazu *Der Bundesbeauftragte für den Datenschutz* 2005, 165 f.). Dieser ist prinzipiell als allgemeines Personenkennzeichen verwendbar und unterfällt damit den unter 4.2.1.2.4 beschriebenen Anforderungen. Da es sich jedoch nicht um eine Nummer der Gesundheitskarte handelt und Datenzusammenführungen unabhängig von dieser möglich sind, bleibt dies im Folgenden außer Betracht.

1244 Nach allgemeinen Kriterien gibt es dagegen Einschränkungen für den Widerruf der Einwilligung. Einzelheiten sind str., s. *Gola/Schomerus*, § 4a Rn. 18; Simitis-*Simitis*, § 4a Rn. 90 ff., jeweils m.w.N. Ohne die genannte Spezialregelung ergäben sich hier im Gesundheitswesen Probleme, vgl. *Hermeler* 2000, 164.

1245 Zur parallelen Dokumentation s.a. unten 4.2.3.3.

1246 *BITKOM/VDAP/VHitG/ZVEI* 2003, 4, 69; s.a. *Dierks/Nitz/Grau* 2003, 137 f.; *Hermeler* 2000, 165.

1247 S. z.B. Gemeinsame Erklärung des BMGS und der Spitzenorganisationen zum Einsatz von Telematik im Gesundheitswesen v. 3.5.2002 (abrufbar unter http://www.afgis.de/upload/pdfs/Gemeinsame%20PE%20BMG%20und%20Spitzenorg..pdf3ceba946cf919.pdf); Pressemitteilung des Staatssekretärs *Schröder* im BMGS anlässlich der Cebit am 19.3.2003 in Hannover.

1248 Diese plädierten eindringlich für die Freiwilligkeit der Karte, s. etwa *Der Bundesbeauftragte für den Datenschutz* 2002, 146 ff.; s. schon früher *Konferenz der Datenschutzbeauftragten*, DuD 1994, 308 f.

nach einer Übergangszeit zumindest einige der bisher freiwillig ausgestalteten Anwendungen zur allgemeinen Pflicht gemacht werden. Dafür spricht auch, dass mit dem elektronischen Rezept gerade die Anwendung, die kurzfristig Einsparungen verspricht, verpflichtend ausgestaltet ist: Das Einsparpotential beläuft sich auf schätzungsweise bis zu 250 Millionen Euro pro Jahr, und Experten gehen davon aus, dass das elektronische Rezept möglicherweise die einzige Telematikanwendung ist, die sich auch kurzfristig wirtschaftlich selbst trägt.[1249] Teilweise wird deutlich von der bisherigen Konzeption als „pragmatischem Ansatz" gesprochen, da ohnehin offen sei, wann die technischen Voraussetzungen für eine elektronische Patientenakte gegeben seien.[1250]

Eine ähnliche Situation könnte sich einstellen, wenn – wie in der Telematik-Expertise gefordert[1251] – ein grundsätzlicher Vorrang der elektronischen vor der papierbasierten Kommunikation implementiert und durch ein Bonus-Malus-System unterstützt würde. In Frankreich ist beispielsweise geplant, die Zuschüsse der Krankenkassen für Patienten zu kürzen, die ohne Angabe von Gründen den Zugriff auf die elektronisch gespeicherten Daten verweigern.[1252] Schließlich besteht auch die Gefahr, dass bei einer flächendeckenden Einführung und Verwendung der Gesundheitskarte de facto keine freie Entscheidungsmöglichkeit des Einzelnen mehr besteht.[1253] So kann es etwa zu Problemen in einzelnen Versorgungsbereichen kommen, wenn die standardisierten Abläufe im Gesundheitswesen auf den Einsatz einer Gesundheitskarte eingespielt sind und diejenigen Versicherten, die dies nicht wünschen, als Sonderfälle behandelt werden.

Fraglich ist damit, ob die normative oder faktische Pflicht zur Verwendung der elektronischen Gesundheitskarte in den bislang freiwilligen Anwendungen zulässig wäre.[1254] Ausgangspunkt ist die Patientenautonomie der Versicherten. Diese beinhaltet unter anderem die freie Arztwahl, die Möglichkeit, eine Untersuchung abzulehnen, die Wahl einer Behandlungsmethode und die Befugnis, selbst darüber zu entscheiden, ob und in welchem Umfang personenbezogene Daten aus der Krankengeschichte einem Leistungserbringer im Gesundheitswesen zugänglich gemacht werden.[1255]

Diese Befugnis darf auch bei der elektronischen Gesundheitskarte nicht ausgehebelt werden. Da der Versicherte als Ausfluss seiner informationellen Selbstbestimmung über das Ob, die Art und Weise und den Umfang der ärztlichen Tätigkeit selbst entscheidet, muss ihm es ihm auch offen stehen, sensible und für den aktuellen Behandlungsfall irrelevante Angaben zurückzuhalten; das Arztgeheimnis gilt auch zwischen verschiedenen Leistungserbringern.[1256] Außerdem muss dem Versicherten die Möglichkeit eröffnet bleiben, eine unabhängige ärztliche Zweitmeinung einzuholen, um eine in seinen Augen zweifelhafte Erstdiagnose überprüfen zu lassen. Letzteres würde jedoch durch die verpflichten-

1249 *Warda/Noelle* 2002, 112 m.w.N., 119. Das Einsparpotential ergibt sich aus der Zahl von jährlich ca. 700 Mio. Rezepten, s. *Weichert*, DuD 2004, 391, 396; *Grätzel v. Grätz* 2004c, 125.

1250 *Dietzel*, Bundesgesundheitsbl. 2003, 267, 269 f.

1251 *BITKOM/VDAP/VHitG/ZVEI* 2003, 3.

1252 S. http://www.heise.de/newsticker/meldung/49266.

1253 *Wellbrock*, DuD 1994, 70, 72; *Bertrand/Kuhlmann/Stark* 1995, 132; *BSI* 1995, 39; *Fuest* 1999, 74 ff.

1254 Diese Frage weist Parallelen zum Problem des abgestuften Zugriffsschutzes auch bei einer echten freiwilligen Anwendung auf; s. dazu unten 4.2.3.4.

1255 Allerdings bestehen durchaus Informations- und Hinweispflichten des Patienten, s. Laufs/Uhlenbruck-*Uhlenbruck/Kern* 2002, 597 ff. m.w.N.

1256 BGH, NJW 1991, 2955, 2957; BayObLG, NStZ 1995, 187; *Gropp*, JR 1996, 478 ff.; *Ulsenheimer/Heinemann*, MedR 1999, 197, 202; *Laufs*, NJW 1975, 1433, 1435 m.w.N.; *Roßnagel*, NJW 1989, 2303, 2306; *Tröndle/Fischer*, § 203 Rn. 30 m.w.N.

de Anwendung der elektronischen Gesundheitskarte mit Vollzugriff jedes behandelnden Arztes nahezu ausgeschlossen werden.[1257]

Andererseits besteht die Gefahr, dass der Arzt relevante Informationen über Vorerkrankungen oder ähnliche Daten nicht erhält, weil der Patient sie für unwesentlich erachtet oder aus anderen Gründen zurückhält. Ist dies für den Arzt nicht erkennbar, so hat er mangels Verschuldens nicht für Behandlungsfehler einzustehen, die aus der Unkenntnis der Daten entstehen.[1258] Wenn der Versicherte dieses Risiko nicht hinnehmen will, kann er über die Anwendung der elektronischen Patientenakte dem jeweiligen Leistungserbringer den Vollzugriff auf seine Krankengeschichte ermöglichen. Dies für alle Versicherte in allen Behandlungsfällen verbindlich vorzuschreiben, ist nicht erforderlich und damit auch nicht zulässig.

Übrig bleibt somit die Frage, ob die Implementation der freiwilligen Applikationen der elektronischen Gesundheitskarte – wie im Gesetz vorgesehen – auf der Basis einer Einwilligung des Versicherten zulässig ist. Teilweise wird eine „pauschale Einwilligung" in die Verwendung einer Karte mit medizinischen Daten, die bei jedem Arztbesuch vorzulegen sind, für unzulässig gehalten.[1259]

Diese Auffassung ist in ihrer Allgemeinheit so nicht richtig. Zwar muss dem Patienten auch bei der Einwilligung in eine umfassende Dokumentation (elektronische Patientenakte) die Eröffnung eines selektiven Informationszugangs möglich bleiben.[1260] Es können nämlich im Einzelfall berechtigte Interessen des Versicherten bestehen, einem bestimmten Leistungserbringer in einem bestimmten Behandlungsfall bestimmte Daten vorzuenthalten. Für Teilbereiche, die nicht die gesamte Krankengeschichte umfassen (Notfalldaten, Daten zur Prüfung der Arzneimitteltherapiesicherheit, Programme für chronisch Kranke) und damit datenschutzrechtlich nicht so risikobehaftet sind, stellt sich dies jedoch anders dar. Einige Anwendungen ergeben nur dann Sinn, wenn sie vollständig und aktuell sind. Das setzt voraus, dass die Karte tatsächlich bei jedem zu dokumentierenden Behandlungs- oder Medikationsfall vorgelegt wird. Am deutlichsten wird dies bei den Daten zur Prüfung der Arzneimitteltherapiesicherheit.[1261] Hier würde eine selektive Schreiberlaubnis durch den Karteninhaber zu Lücken in der Dokumentation führen, die diese unbrauchbar machen würden.[1262]

1257 S. *Konferenz der Datenschutzbeauftragten* 2001, ferner *Hermeler* 2000, 16; *Der Landesbeauftragte für den Datenschutz Bremen*, DuD 1992, 276; *BSI* 1995, XII, 52; die freie Arztwahl ist Ausdruck des Persönlichkeitsrechts des Patienten (*Menzel/Schläger*, DuD 1999, 70, 72) und auch in § 76 SGB V und § 7 Abs. 2 MBO-Ä 2004 verankert.

1258 Roßnagel-*Schirmer*, Kap. 7.12, Rn. 118.

1259 *Bultmann/Wellbrock/Biermann/Engels/Ernestus/Höhn/Wehrmann/Schurig* 2002, 7; für eine totale Wahlfreiheit hinsichtlich des Einsatzes einer Patientenkarte bei Ärzten und Apothekern auch *Fuest* 1999, 171.

1260 S.u. 4.2.3.4.

1261 *Devigne*, ZM 2003, 18; näher zur Arzneimitteldokumentation *Goetz*, DÄ 2003, A 756, 766 f.

1262 Auch bei einer Vorlagepflicht kann die Dokumentation allerdings unvollständig sein, bspw., wenn die Karte funktionsuntüchtig, abhanden gekommen oder im Notfall nicht verfügbar ist, eine Medikation jedoch erfolgen muss. Je nachdem wie zahlreich diese Fälle sind, können sie möglicherweise sogar die Funktionsfähigkeit der gesamten Anwendung beeinträchtigen, weil der behandelnde Arzt sich nicht auf die Vollständigkeit der Dokumentation verlassen kann. Zwar bleibt ein Nachtragen durch den Leistungserbringer möglich. Außerdem könnte nicht nur der Arzt, sondern auch der Apotheker einen Eintrag in die Dokumentation vornehmen; dies ist ohnehin für Selbstmedikationen geplant. Für das Nachtragen kann dann aber nicht der Karteninhaber verantwortlich sein, weil dies – gerade vor dem Hintergrund von Haftungsfällen – eine zu große Verpflichtung in einem Bereich darstellen würde, der zum Pflichtenkreis des Arztes gehört.

Wenn die Gesamtanwendung nur bei Vorlage der Gesundheitskarte bei jedem Arzt- oder Apothekenbesuch möglich ist, reduziert sich die Entscheidung auf den Einsatz oder den Verzicht auf die Anwendung. Solange diese Wahl frei und selbstbestimmt vorgenommen werden kann, bestehen unter datenschutzrechtlichen Gesichtspunkten keine Einwände dagegen, die Entscheidung auf den Versicherten zu verlagern. Das Recht auf informationelle Selbstbestimmung bleibt gewahrt, weil der Verzicht möglich ist und die Applikation nicht weniger belastend ausgestaltet werden kann. Darüber hinaus besteht nach geltendem Recht (§ 291a Abs. 3 Satz 4, 2. Halbsatz) die Möglichkeit, die Einwilligung jederzeit zu widerrufen. Der Gesetzgeber darf damit einzelne Anwendungen, über deren Einsatz der Versicherte entscheidet, auf der inhaltlichen Ebene so ausgestalten, dass eine Vorlage der Gesundheitskarte bei jedem Arztbesuch vorgeschrieben wird.

4.2.3.2 Gesetzesvorbehalt und Bestimmtheit der Ermächtigungsgrundlage

Da auf und mittels der elektronischen Gesundheitskarte eine Vielzahl sensibler Daten verwendet werden, sind an die Bestimmtheit der Rechtsgrundlage hohe Anforderungen zu stellen. Das gilt allerdings im Prinzip nur für die verpflichtenden Anwendungen. Die durch das GKV-Modernisierungsgesetz geregelten freiwilligen Funktionen hätten dagegen an sich auch auf Basis individueller Einwilligungen eingeführt werden können.[1263] Dieses Verfahren würde jedoch wegen der großen Zahl der Betroffenen und der Komplexität der technischen Infrastruktur auf unüberwindbare Schwierigkeiten stoßen. Deshalb ist auch für die freiwilligen Applikationen der elektronischen Gesundheitskarte eine genaue gesetzliche Regelung erforderlich, umso mehr, als verpflichtende und freiwillige Anwendungen in einer Karte implementiert und teilweise aufeinander bezogen sind. Das gilt beispielsweise für das (verpflichtende) elektronische Rezept und die (freiwilligen) Daten zur Prüfung der Arzneimitteltherapiesicherheit.

Die elektronische Gesundheitskarte soll durchweg Daten enthalten, die bereits bisher an verschiedenen Stellen im Gesundheitssystem verwendet wurden. Der grundrechtliche Gesetzesvorbehalt bezieht sich jedoch auch auf die Modalitäten von Speicherung und Zugriff, soweit diese wesentlich sind. Die Zusammenführung von Daten über den Versicherten auf oder mittels einer Chipkarte wird hiervon erfasst, da sie neue Zugriffsmöglichkeiten und datenschutzrechtliche Risiken von erheblichem Ausmaß mit sich bringt. Damit ist eine exakte gesetzliche Bestimmung der Funktionsweise erforderlich. Eine solche fand sich bis zum GKV-Modernisierungsgesetz nicht im geltenden Recht;[1264] allerdings war eine Einführung ohne gesetzliche Grundlage auch nie beabsichtigt.[1265]

Die Regelungen in § 291a SGB V und den diesen ergänzenden Normen sind insoweit ausreichend. Im Unterschied zum Personalausweisgesetz wird ausdrücklich bestimmt, dass auf der Gesundheitskarte Daten in elektronischer Form gespeichert werden (§ 291a Abs. 2 Satz 1 und Abs. 3 Satz 1). Bereits aus dieser Vorschrift ergibt sich mittelbar, dass es sich um eine Chipkarte handeln muss. Gleiches gilt für die Anforderung in § 291a Abs. 5 Satz 2 SGB V, dass die Karte eine technische Autorisierung durch den Versicherten zu ermögli-

1263 Dies erfolgt in Pilotprojekten wie der Gesundheitskarte Schleswig-Holstein, s. http://landesregierung.schleswig-holstein.de/coremedia/generator/Aktueller_20Bestand/MSGV/Information/Gesundheitskart e.html.

1264 *Kilian*, NJW 1992, 2313, 2316 f.; *Wellbrock*, DuD 1994, 70, 72; *Iwansky* 1999, 68 ff.; *Dierks/Nitz/Grau* 2003, 119; *BSI* 1995, 43 ff.; sehr ausführlich *Kraft* 2003, 58 ff.

1265 Das bleibt unerwähnt in den Ausführungen von *Kraft*, der lediglich auf die Möglichkeit einer individuellen Einwilligung verweist (2003, 68 f.), ohne Anforderungen an eine gesetzliche Erlaubnis zu formulieren.

chen hat. Auch die in § 291a Abs. 2 Satz 1 und Abs. 3 Satz 1 SGB V genannten Funktionalitäten und Zugriffsbefugnisse der Gesundheitskarte sind hinreichend bestimmt. Zwar werden Fragen wie die des Speicherorts der Daten (auf der Karte, auf dezentralen oder zentralen Servern) nicht geregelt. Genauere technische Ausgestaltungen können aber auch auf der untergesetzlichen Ebene normiert werden. Die den Beteiligten auf Bundesebene auferlegte technische Normierung der Telematik-Infrastruktur durch die Gesellschaft für Telematik unterliegt nach § 291b Abs. 4 Satz 1 SGB V der Rechtsaufsicht des zuständigen Ministeriums. Die technische Umsetzung wird damit kontrolliert und öffentlich gemacht. Hierdurch ist dem Bestimmtheitsgebot im Grundsatz genüge getan.

Zweifel ergeben sich hinsichtlich weiterer Funktionalitäten der Gesundheitskarte, die bislang nicht ausdrücklich normiert sind. Der Katalog des § 291a Abs. 3 Satz 1 SGB V verlangt, diese müsse „insbesondere" die aufgelisteten Funktionen ermöglichen. Die Bestimmung ist also nicht abschließend, sondern ermöglicht generalklauselartig weitere Funktionen. Eine „kleine Generalklausel" bietet darüber hinaus das zur Verfügung Stellen von Daten durch oder für den Versicherten selbst in § 291a Abs. 3 Satz 1 Nr. 5 SGB V. Auch hier können weitere Funktionen hinzugefügt werden.

Gleichzeitig begrenzt der Bestimmtheitsgrundsatz jedoch Anwendungserweiterungen; diese sind explizit gesetzlich zu regeln, wenn sie wesentlich sind. Solange der Versicherte selbst Daten zur Verfügung stellt, wird es sich regelmäßig nicht um eine wesentliche Funktionserweiterung der Gesundheitskarte handeln. Sobald es allerdings um grundsätzlich neue Einsatzmöglichkeiten der Karte geht, spricht eine Vermutung dafür, dass diese ausdrücklich normiert werden müssen.

Das Problem der Zulässigkeit von Anwendungserweiterungen kann am Beispiel der in der Telematik-Expertise angesprochenen, im Gesetz aber nicht geregelten Vertretung für Kinder, Betreute und Bettlägerige im Rahmen der freiwilligen[1266] Anwendungen der Gesundheitskarte verdeutlicht werden. Hierzu werden drei Umsetzungsmöglichkeiten vorgeschlagen:[1267]

- Der Vertreter könnte eine eigene Karte bekommen, die die Gesundheitskarte des Betroffenen freischaltet,
- der Vertreter könnte mittels einer eigenen PIN (beschränkten) Zugriff auf die Gesundheitskarte erhalten oder
- eine Vollmacht könnte vom Vertretenen elektronisch signiert und auf der eigenen Karte oder zentral gespeichert werden.

Eine signierte Vollmacht könnte einerseits auf der Karte des Vertretenen „durch" diesen selbst zur Verfügung gestellt werden. Nach der aktuellen Gesetzeslage scheitert eine derartige Umsetzung aber daran, dass gemäß § 291a Abs. 5 Satz 1 SGB V ein Zugriff auf diese Daten nur nach einer Freischaltung durch den Versicherten (selbst) erfolgen darf. Da die Vollmacht aber genau zu dieser Freischaltung dienen soll, scheidet eine Umsetzung im Rahmen von § 291a Abs. 3 Satz 1 Nr. 5 SGB V aus.[1268] Denkbar wäre auch eine Lösung mittels der Gesundheitskarte des Vertreters. Die Vollmacht wäre dann im Sinne dieser Norm „für" den Vertreter zur Verfügung gestellt.

1266 Das Problem stellt sich für das elektronische Rezept nicht, weil hier der Schutz durch den Besitz der Karte vermittelt wird und nicht wie bei den freiwilligen Anwendungen eine technische Autorisierung „des Versicherten" erforderlich ist. Durch die Weitergabe der Karte können Dritte mit der Rezepteinlösung beauftragt werden.

1267 *BITKOM/VDAP/VHitG/ZVEI* 2003, 46 f.

1268 Ein vergleichbares Problem stellt sich auch bei Daten, die vom Versicherten gerade für den Fall zur Verfügung gestellt werden, dass er zur Autorisierung nicht mehr in der Lage ist, s.u. 4.2.3.4.2.2.

Entscheidend ist, ob die Vertretungsregelung als „unbenannte Funktionalität“ im Rahmen von § 291a Abs. 3 Satz 1 SGB V eingeführt werden könnte oder so wesentlich ist, dass sie einer gesetzlichen Erwähnung bedarf. Bei allen drei Umsetzungsmöglichkeiten würde ein Zugriff auf die Gesundheitskarte des Vertretenen ohne dessen unmittelbare Autorisierung erfolgen. Zwar ließe sich eine Vollmachtslösung sprachlich noch unter die nach § 291a Abs. 5 Satz 2 SGB V für die freiwilligen Anwendungen erforderliche Autorisierung subsumieren. Vom Sinn und Zweck her ist dort jedoch eine unmittelbare Legitimation durch den Versicherten gemeint. Auch die Gesetzesbegründung nennt insoweit lediglich die PIN oder biometrische Verfahren, nicht aber eine Autorisierungskette über einen Vertreter.[1269] Aufgrund des hohen Missbrauchspotentials im Fall des Zugriffs durch andere Personen als den Versicherten sowie aufgrund der Sensibilität der auf oder mittels der Gesundheitskarte gespeicherten Daten müssen die Zugriffsbefugnisse exakt gesetzlich bestimmt werden. Jede der in der Expertise vorgeschlagenen Umsetzungsvarianten erfordert demnach eine ausdrückliche gesetzliche Regelung. Da eine Lösung für die Gruppe der Vertretenen erforderlich ist, muss der Gesetzgeber eine entsprechende Norm beschließen.

4.2.3.3 Ort der Datenspeicherung

Für die Daten, die im System der Gesundheitskarte[1270] anfallen, gibt es mehrere denkbare Aufbewahrungsorte.[1271] Soweit die Kapazität der Karte es zulässt, können Angaben in ihrem Speicher abgelegt werden. Alternativ dazu kann der Chip auch lediglich Verweise (Pointer) auf den Speicherort weiterer Informationen enthalten. Hier kommen wiederum zwei Varianten in Frage, nämlich eine verteilte Datenhaltung in einer dezentral-vernetzte Struktur (zum Beispiel aus unterschiedlichen Krankenhaus- und Praxiscomputern, die nach entsprechender Autorisierung mittels der Gesundheitskarte gegenseitig auf Daten zugreifen können) und zentral organisierte Server.

Es sollte nicht übersehen werden, dass die Wahl zwischen diesen Varianten durchaus auch von ökonomischen Interessen der Beteiligten im Gesundheitswesen bestimmt wird. Im Grundsatz streben die Apotheker eine kartenbasierte Lösung an, „um die Schnittstelle zwischen ärztlicher Verordnung und Dispensierung offline zu halten und sich die pharmakologische Beratung vorzubehalten, den Versandhandel abzufangen und durch eine Netzanbindung ab der Apotheke eine gewisse Datenhoheit zu reservieren“.[1272] Die Krankenkassen haben dagegen Probleme mit dem Investitionsbedarf bei der neuen Karte und favorisieren deshalb serverbasierte Modelle.

Das GKV-Modernisierungsgesetz bestimmt in § 291a Abs. 2 Satz 1 SGB V, dass die Versicherungsstammdaten auf der Karte selbst abgelegt werden. Hinsichtlich der weiteren Funktionalitäten enthält das Gesetz keine Regelung. Es heißt dort lediglich, die Gesundheitskarte müsse geeignet sein, Angaben für den europäischen Berechtigungsnachweis und die „Übermittlung“ des elektronischen Rezepts aufzunehmen, beziehungsweise, die frei-

1269 BT-Drs. 15/1525, 145.

1270 Nicht betrachtet werden im Folgenden Datenspeicherungssysteme ohne Verwendung der Gesundheitskarte, wie etwa eine dezentrale Speicherung mit Kommunikationsverbindungen zwischen den Leistungserbringern im Einzelfall, s. *Bultmann/Wellbrock/Biermann/Engels/Ernestus/Höhn/Wehrmann/Schurig* 2002, 14.

1271 S. z.B. *Hermeler* 2000, 9 ff.; *Rienhoff*, ZaeFQ 2001, 642 ff.; *Hornung* 2004a, 231 f.; allgemeiner *Bizer* 2002, 21 ff.

1272 *Sendatzki*, BKK 2002, 206; s.a. *Dierks/Nitz/Grau* 2003, 186 f.; s.a. die unterschiedlichen Positionen in *ATG/GVG* 2001a, 29 ff. (gesetzliche Krankenversicherungen und Kassenärztliche Bundesvereinigung) und 31 f. (ABDA); vgl. ferner *Grätzel v. Grätz* 2004c, 66 f., 119. Die Varianten wurden bereits im Gutachten von *Berger & Partner* (1997, 118 ff.) erläutert.

willigen Anwendungen nach § 291a Abs. 3 Satz 1 SGB V „zu unterstützen". Das lässt sowohl eine Speicherung auf der Karte als auch die Serverlösung zu. Insbesondere spricht § 291 a Abs. 2 Nr. 1 SGB V nicht davon, die Karte müsse das elektronische Rezept selbst aufnehmen. Die Telematik-Expertise schlägt für dieses eine Wahlmöglichkeit zwischen einer Speicherung auf der Karte und auf einem zentralen Server vor.[1273] Gleiches soll auch für weitere Gesundheitsdaten gelten.[1274] Bei der Speicherung auf der Karte hält die Expertise die zusätzliche Aufbewahrung auf einem Server zum Schutz vor dem Verlust der Karte für sinnvoll. Auch dies soll aber ins Belieben des Versicherten gestellt werden.[1275] Die internationale Entwicklung geht dahin, auf der Gesundheitskarte lediglich Verweise (Pointer) zu speichern und die Karte so als Authentisierungsinstrument zu Daten einzusetzen, die auf Servern gespeichert sind. Insofern sprechen Interoperabilitätsgesichtspunkte für diese Lösung.

Sollte es in der Telematikstruktur tatsächlich zu einer Wahlmöglichkeit kommen (was aufgrund der höheren Anforderungen an die Infrastruktur eher unwahrscheinlich ist), so ergeben sich aus dem Verhältnismäßigkeitsprinzip keine Probleme, weil es dem Betroffenen überlassen bleibt, die Lösung zu wählen, die für ihn subjektiv die geringsten Risiken bietet. Es ist jedoch sehr fraglich, ob es auf Dauer praktikabel sein wird, die Art und Weise der Datenspeicherung und -verarbeitung in das Belieben des Patienten zu stellen. Deshalb ist es erforderlich, die rechtlichen Anforderungen an die Wahl des Speicherortes zu bestimmen.

Hierbei muss man sich zunächst klarmachen, dass die Frage der Speicherung auf der Karte selbst oder – vermittelt durch sie – auf Servern keine Alternative zur bisherigen Speicherung beim Leistungserbringer ist. Diese wird vielmehr weiterhin erfolgen.[1276] Jeder behandelnde Arzt benötigt die Daten über Untersuchungen und Behandlungen zum Zweck der Leistungsabrechnung und weiteren Behandlung, aber auch zum Nachweis über den Inhalt seiner Tätigkeit, etwa in einem Haftungsprozess.[1277] Mangelhafte Dokumentationen der Leistungserbringer können zu Beweiserleichterungen für den Patienten führen,[1278] weshalb eine ordnungsgemäß erstellte und aufbewahrte Dokumentation für die Leistungserbringer von großer Wichtigkeit ist.

1273 *BITKOM/VDAP/VHitG/ZVEI* 2003, 13, 36.

1274 *BITKOM/VDAP/VHitG/ZVEI* 2003, 71.

1275 *BITKOM/VDAP/VHitG/ZVEI* 2003, 36. Dagegen plädieren *Dämmer/Männel*, BKK 2003, 279, 284 nachdrücklich für eine verpflichtende Serverlösung.

1276 *BITKOM/VDAP/VHitG/ZVEI* 2003, 49. Bereits in der Gemeinsamen Erklärung des BMGS und der Spitzenorganisationen zum Einsatz von Telematik im Gesundheitswesen v. 3.5.2002 (s.o. Fn. 1247) wird betont, dass die neue Regelung bestehende Dokumentationspflichten nicht abändern soll; s.a. *Roßnagel/Wedde/Hammer/Pordesch* 1990, 193; *Wellbrock*, DuD 1994, 70, 73; *Der Bundesbeauftragte für den Datenschutz* 2002, 148; nicht ganz so eindeutig *Bultmann/Wellbrock/Biermann/Engels/Ernestus/Höhn/Wehrmann/Schurig* 2002, 15, wonach bei einer zentralen Speicherung die dezentrale Vorhaltung der Daten auch entfallen könnte; viel zu eng *Fuest* 1999, 109 ff. (das Verfügungsrecht stehe ausschließlich dem Patienten zu) und 172 (es müsse in der freien Entscheidung des Versicherten liegen, wo eine Sicherungskopie der auf der Karte gespeicherten Daten abgelegt werde).

1277 *Bizer* 2002, 37 (s.a. für die Verwaltung ebd., 23). Das wird übersehen von *Iwansky* 1999, 87, die eine Speicherung beim jeweiligen Leistungserbringer als „unpraktisch" bezeichnet; zur ärztlichen Dokumentation im Prozess s. *Wendt* 2001 und *Hermeler* 2000, 29 f.

1278 Vgl. BGHZ 72, 132 ff.; 85, 212 (216 f.); 159, 48 ff.; *Wendt* 2001, insbes. 211 ff., 277 ff., 315 ff.; *Laskaridis* 2003, 66 ff.; *Ortner/Geis*, MedR 1997, 337 m.w.N. Die Dokumentationspflicht dient damit der prozessualen Beweissicherung (BGH, NJW 1987, 1482 f.; *Inhester*, NJW 1995, 685, 688; *Hermeler* 2000, 112 ff.; *Laskaridis* 2003, 41 ff.), daneben allerdings mehr und mehr auch anderen Zwecken außerhalb der Behandlung (Qualitätsmanagement, verfeinerte Abrechnung, s. *Bäumler*, MedR 1998, 400, 402).

Wenn insoweit die Berufsordnungen der Ärzte[1279] und einzelne spezialgesetzliche Regelungen[1280] Dokumentationspflichten vorsehen, so kommt damit zum Ausdruck, dass Gesundheitsdaten immer Ausdruck von Sozialbeziehungen sind. Sie enthalten nicht nur objektive Beschreibungen des Patienten, sondern ebenso subjektive Einschätzungen des behandelnden Arztes und geben über dessen Tätigkeit Aufschluss. Wegen der grundsätzlichen Verfügungsbefugnis des Patienten über die Daten[1281] ist das Interesse des Leistungserbringers an einer Speicherung und Nutzung zwar begründungspflichtig, jedoch zu bejahen. An Daten, die sich nur oder auch auf den Arzt beziehen, kann es keine alleinige Verfügungsbefugnis des Patienten geben.[1282] Es ist weder praktikabel noch dem Arzt zuzumuten, dass diese Daten nicht mehr bei ihm, sondern auf Servern gespeichert werden. Erst recht ist eine ausschließliche Ablage auf der Gesundheitskarte nicht möglich. Für den Fall des Verlusts der Karte wären die Daten unwiederbringlich verloren; der Zugang zu ihnen würde außerdem in das Belieben des Versicherten gestellt – dieser ist jedoch der wahrscheinlichste Prozessgegner des Arztes im Haftungsfall. Eine totale Datenhoheit des Versicherten mittels der Chipkarte wird also den unterschiedlichen Interessen nicht gerecht.

Der behandelnde Arzt muss damit aus sachlichen Gründen wie bisher über ein paralleles Dokumentationssystem verfügen. Die Gesetzeslage trägt dem Rechnung. § 291a Abs. 5 Satz 2 SGB V regelt, dass ein Zugriff auf die auf oder mittels der Gesundheitskarte gespeicherten Daten der freiwilligen Anwendungen (mit Ausnahme der Notfalldaten) ohne Autorisierung des Versicherten technisch auszuschließen ist. Bei einer andauernden Behandlung ist dies für den Arzt unproblematisch: Er kann nach der erfolgten Autorisierung auf die durch ihn selbst gespeicherten Daten zugreifen. Für eigene Zwecke (zum Beispiel im Rechtsstreit) ist ihm das jedoch ohne Mitwirkung des Versicherten technisch unmöglich. Die Leistungserbringer sind deshalb gezwungen, die erhobenen Daten ohne Einsatz der jeweiligen Gesundheitskarte für sich selbst zu speichern und erst im zweiten Schritt diese auf oder durch die Karte für andere Beteiligte bereitzustellen.

Unter Verhältnismäßigkeitsgesichtspunkten ist damit (nur) die weitere Frage zu beantworten, wo die Gesundheitsdaten im System der elektronischen Gesundheitskarte zusätzlich zu speichern sind. Auch im Gesundheitswesen gilt, dass eine Speicherung auf der Karte weniger eingriffsintensiv ist als eine solche auf Servern und bei den Serverlösungen eine verteilte Datenhaltung weniger in das Recht auf informationelle Selbstbestimmung eingreift als ein zentrales System. Zentrale Datenspeicherungen sind insbesondere deshalb gefährlich, weil eine große Menge sensibler Daten an einem Punkt zusammengeführt wird. Ein Angreifer könnte umfassende Informationen über die vollständige Krankengeschichte einer Vielzahl von Versicherten erhalten. Werden derart zusammengeführte Daten publik, sind sie außerdem kaum noch aus der Welt zu schaffen. Eine dezentrale Telematikstruktur hat demgegenüber zwar den Nachteil, dass ein Netzwerk zwischen den jeweiligen Leistungserbringern geschaffen werden muss, das in hohem Maße resistent gegen Störungen ist. Diese Anforderungen sind aber in technischer Hinsicht erfüllbar. Um dem verfassungs-

1279 Entsprechend § 10 MBO-Ä 2004. Die Aufbewahrungsdauer beträgt nach § 10 Abs. 3 MBO-Ä 2004 mindestens zehn Jahre. Schon aus beweistechnischen Gründen bewahren viele Leistungserbringer die Dokumente aber 30 Jahre auf, s. *Bäumler*, MedR 1998, 400, 4001; *GDD* 2002, 38; *Hermeler* 2000, 28; *Inhester*, NJW 1995, 685, 688. Dies führt zum Problem der Langzeitaufbewahrung elektronischer Dokumente, s.u. 6.3.1; zur Dokumentationspflicht bereits oben 2.2.2.1.

1280 S. die Bsp. bei *Hermeler* 2000, 24; *Wendt* 2001, 43 ff.; *Laskaridis* 2003, 28.

1281 BGH, NJW 1992, 763, 765.

1282 *Kilian*, NJW 1992, 2313, 2315. Deshalb gibt es auch keinen Anspruch des Patienten auf Widerruf einer Diagnose, s. BGH, NJW 1989, 774 f.

rechtlichen Verhältnismäßigkeitsprinzip zu genügen, muss daher auf die zentrale Datensammlung verzichtet werden.[1283]

Vergleicht man die Möglichkeiten einer Speicherung auf der Karte und einer verteilten Datenhaltung miteinander, so hat eine Speicherung auf der Karte selbst den Vorteil, dass die Daten in der physischen Obhut des Versicherten sind und dieser nicht auf die Sicherheit von Serversystemen angewiesen ist. Ausschließlich er selbst entscheidet über den Zugang zu seinen Gesundheitsangaben. Die Ablage auf der Karte stellt sich damit als eingriffsschwächer dar. In einem System verteilter Datenhaltung kann allerdings zum Beispiel durch ein dreistufiges Directory-Sicherheitskonzept (wie in der Telematik-Expertise vorgeschlagen)[1284] verhindert werden, dass aus einzelnen Geschäftsvorgängen auf den Versicherten zurückgeschlossen werden kann. Hierin liegt ein grundlegender Unterschied zum digitalen Personalausweis. Dort müssen Daten auch ohne freiwillige Mitwirkung des Betroffenen verfügbar sein, während im Gesundheitswesen eine Absicherung des Zugangs über eine PIN des Versicherten möglich ist. Wenn die Verfahren hinreichend sicher sind, insbesondere im verteilten System die Daten mit dem öffentlichen Schlüssel der Gesundheitskarte verschlüsselt gespeichert und übertragen werden (Ende-zu-Ende-Verschlüsselung), so ist diese Lösung nur noch unwesentlich eingriffsintensiver als eine Speicherung auf der Karte.[1285] Nichtsdestotrotz verbleibt bei letzterer ein gewisser datenschutzrechtlicher Vorteil für den Versicherten.

In der Analyse der einzelnen Funktionalitäten der elektronischen Gesundheitskarte ist nunmehr zu klären, welche Speichervarianten für sie geeignet sind. Der begrenzende Faktor für eine Ablage auf der Karte selbst ist die Speicherkapazität des Chips. Gerade bei Patienten mit Mehrfach- oder Dauererkrankungen, bei denen die elektronische Bereitstellung der Krankengeschichte für den (neu) behandelnden Arzt besonders sinnvoll erscheint, dürfte die erforderliche Datenmenge schnell die Speichermöglichkeiten der Karte überfordern.[1286] Ob dies der Fall ist, kann aber nur im Einzelfall entschieden werden:

- Einige Daten müssen aus funktionalen Gründen auf der elektronischen Gesundheitskarte selbst gespeichert werden. Das ist bei den Versicherungsstammdaten, dem europäischen Berechtigungsnachweis und den Notfalldaten der Fall.[1287] Mit den Stammdaten identifiziert sich der Versicherte gegenüber dem Leistungserbringer; dieser Prozess ist dem Zugriff auf Server mittels der Karte vorgelagert. Der europäische Nachweis kann – sollte er von Beginn an oder in Zukunft nicht in visueller, sondern in elektronischer Form gespeichert werden – erst dann serverbasiert funktionieren, wenn ein europaweiter Onlinezugriff auf die Daten gesichert wird, der momentan unrealistisch ist. Bei den Notfalldaten (und denjenigen vom Versicherten selbst zur Verfügung gestellten Daten, die genau wie diese im Notfall vor Ort verfügbar sein sollen) ist eine Auslesbarkeit durch mobile Geräte zu gewährleisten. Dies ist im Servermodell kaum durchführbar. Überdies sollten die Daten

1283 Ablehnend gegenüber einer zentralen Datenbank im Gesundheitswesen auch *Konferenz der Datenschutzbeauftragten* 2001 und 1995b, unter 6; *Bultmann/Wellbrock/Biermann/Engels/Ernestus/Höhn/Wehrmann/Schurig* 2002, 16; *Goetz* 2001, 119 ff.; *ATG/GVG* 2005, 27 ff.; s.a. *Hornung* 2004a, 231 f.

1284 *BITKOM/VDAP/VHitG/ZVEI* 2003, 30 ff.; s. näher unten 6.3.2.

1285 Ebenso *Der Bundesbeauftragte für den Datenschutz* 2002, 147.

1286 Das gilt insbes. für speicherintensive Untersuchungsergebnisse, bspw. nach einer Computertomographie oder Magnet-Resonanz-Untersuchung. Kommen mehrere solcher Behandlungen zusammen, entstehen Datenmengen, die auch mittel- und langfristig nicht auf Chipkarten Platz finden werden.

1287 Ebenso *Weichert*, DuD 2004, 391, 396. Für die Notfalldaten wird dies nunmehr ausdrücklich gesetzlich angeordnet (§ 291a Abs. 3 Satz 1 n.F. a.E.), war aber – da das Gesetz im Übrigen keine Aussage zum Ort der Datenspeicherung trifft – auch zuvor nicht ausgeschlossen.

auch im Ausland zur Verfügung stehen. Hierzu ist eine Ablage auf der Karte erforderlich.

- Andere Daten könnten in funktionaler Hinsicht auf der Karte oder auf Servern gespeichert werden, benötigen jedoch nur einen so geringen Speicherplatz, dass sie für eine Speicherung auf der Karte geeignet sind. Das gilt insbesondere für die Patientenquittung nach § 305 Abs. 2 SGB V. Auch das elektronische Rezept hat keinen erheblichen Datenumfang und kann überdies nach dem Einlösen in der Apotheke auf der Karte gelöscht werden. Der Transport des Rezepts durch den Versicherten entspricht auch dem bisherigen Ablauf. Das Verlustrisiko ist gering; außerdem besteht wie bisher die Möglichkeit der Ausstellung eines Ersatzrezepts. Allerdings gibt es Fälle, in denen eine Übertragung nur mittels Servern möglich ist. Wenn beispielsweise der Arzt den Patienten (und den öffentlichen Schlüssel seiner Karte) kennt, kann er so nach einer telephonischen Bestellung das Rezept verschlüsselt übersenden. Dieser Vorgang entspricht dem bisherigen Postversand.[1288]
- Elektronische Arztbriefe können je nach Umfang der Daten auf der Karte oder auf (verteilten) Servern gespeichert werden. Bei einer Speicherung auf der Karte besteht allerdings die Gefahr des Verlusts oder der Unbenutzbarkeit. In diesem Fall müssen die Daten von der erhebenden Stelle erneut bereitgestellt werden. Das bereitet aber keine wesentlichen Probleme, weil weiterhin eine Speicherung beim Leistungserbringer erfolgt. Es tritt also kein vollständiger Datenverlust ein.
- Für die elektronische Patientenakte ist eine Speicherung auf der Gesundheitskarte zum gegenwärtigen Zeitpunkt aus Kapazitätsgründen nicht realistisch. Schon deshalb ist der Serverlösung der Vorzug zu geben. Gleiches gilt auch bei sehr umfangreichen Daten zur Prüfung der Arzneimitteltherapiesicherheit, insbesondere, wenn mehrere verschreibende Ärzte beteiligt sind. Eine Speicherung auf der Karte erscheint darüber hinaus auch unter praktischen Gesichtspunkten nicht geeignet. Denn im Unterschied zum elektronischen Rezept und dem elektronischen Arztbrief, bei denen der vollständige Datensatz bei der speichernden Stelle verfügbar und der Aufwand bei einem Verlust der Karte deshalb gering ist, bestehen die elektronische Patientenakte und die Daten zur Prüfung der Arzneimitteltherapiesicherheit aus einer Vielzahl von Informationen, die in dieser Zusammensetzung möglicherweise nicht oder nur schwer wieder zu rekonstruieren wären.[1289] Hier ergibt sich im Fall der Servervariante eine Rekonstruktionsmöglichkeit: Der Karteninhaber könnte die auf der Gesundheitskarte gespeicherten Pointer und Schlüssel bei einem vertrauenswürdigen Dritten hinterlegen und im Verlustfall auf diese zurückgreifen. Wenn eine sichere Ende-zu-Ende-Verschlüsselung unter Verwendung des geheimen Schlüssels der Karte eingerichtet wird, muss sogar nur dieser Schlüssel hinterlegt werden (Key Recovery). Zur Absicherung des Versicherten ist der Schlüssel dabei in mindestens zwei Teile zu trennen, die bei unterschiedlichen Treuhändern zu verwahren sind. Da diese Möglichkeit nicht im Gesetz vorgesehen ist, wäre hierzu allerdings eine individuelle Einwilligung erforderlich.

1288 S. zu diesen und anderen Fragen der technischen Umsetzung des elektronischen Rezepts die Spezifikation vom 11.3.2005, *Struif* (Ed.) 2005, Teil 3.

1289 Dies ist allerdings dann möglich, wenn der Hausarzt des Versicherten ebenfalls eine derartige Dokumentation führt, wie dies bereits heute nach § 73 Abs. 1b SGB V möglich ist. Diese Dokumentation ist jedoch freiwillig, und der Hausarzt hat keine Möglichkeit, die Vollständigkeit dieser Datensammlung zu kontrollieren.

Echte Alternativen zwischen verschiedenen Speicherorten bestehen damit nur für das elektronische Rezept,[1290] sowie dann, wenn ein elektronischer Arztbrief lediglich Speicherkapazitäten benötigt, die eine Ablage auf der Gesundheitskarte zulassen. In diesen Fällen ist unter Verhältnismäßigkeitsgesichtspunkten die Speicherung auf der Karte zu wählen. Wenn demgegenüber größerer Datenmengen transportiert oder aufbewahrt werden müssen, ist auf die – dezentrale – Serverlösung zurückzugreifen.

Zu beachten bleibt, dass diese Doppellösung die parallele Bereitstellung zweier grundsätzlich unterschiedlicher Speicher- und Zugriffslösungen innerhalb einer Telematikstruktur voraussetzt. Dies könnte mit nicht unwesentlichen Kosten verbunden sein. Auch in einer reinen Serverlösung fallen jedoch Kosten für die lokale Infrastruktur an, da auch bei dieser Informationen (Pointer, Session-Keys, etc.) aus der Gesundheitskarte ausgelesen werden müssen und deshalb Kartenleser und anderes Zubehör bereitgestellt werden muss. Ist diese Infrastruktur vorhanden, kann sie auch zum Auslesen von Gesundheitsinformationen verwendet werden, die auf der Karte selbst gespeichert sind. Solange außerdem einige Anwendungen der Gesundheitskarte diese Art der Speicherung aus funktionalen Gründen erfordern, müssen ohnehin beide Varianten implementiert werden.

4.2.3.4 Zugriffsbefugnisse

Zur Absicherung der datenschutzrechtlichen Zweckbindung und zur Sicherstellung informationeller Gewaltenteilung (Verhinderung unkontrolliert zusammengeführter Datenbestände) müssen die einzelnen Anwendungen der elektronischen Gesundheitskarte in getrennt eingerichteten Speicher- und Verarbeitungsbereichen ablaufen.[1291] Die Anforderungen an die Definition und technische Sicherung der unterschiedlichen Zugriffsbefugnisse für die auf oder mittels der elektronischen Gesundheitskarte gespeicherten Daten sind wegen der Vielzahl der Applikationen der Karte und der Beteiligten im Gesundheitswesen sehr kompliziert. Zum Verständnis der Problemstellung ist es zunächst erforderlich, sich die grundsätzlichen Rechte des Versicherten in Bezug auf seine medizinischen Daten zu verdeutlichen.

4.2.3.4.1 Die grundsätzliche Informationshoheit des Versicherten

Die Offenbarung von Krankheiten, Leiden oder Beschwerden kann dem Einzelnen unangenehm und peinlich oder seiner sozialen Geltung abträglich sein.[1292] Patienten befinden sich deshalb unter Datenschutzgesichtspunkten in einer widersprüchlichen Situation. Einerseits bringt die Preisgabe von Gesundheitsinformationen die Speicherung, Verarbeitung und Nutzung sensibler Daten in Bereichen mit sich, über die der Patient keine Kontrolle hat. Andererseits ist dem behandelnden Arzt eine optimale Versorgung nur möglich, wenn er über alle relevanten Informationen verfügt.

Das geltende Recht löst diesen Widerspruch so, dass der Versicherte frei darüber bestimmen kann, welche Daten er offenbart, ihm im Fall der Preisgabe aber Schutzmechanismen gegen eine nicht autorisierte Verwendung zur Seite stehen. In den Worten des Bundesverfassungsgerichts darf und muss jeder Patient erwarten, „dass alles, was der Arzt im Rahmen seiner Berufsausübung über seine gesundheitliche Verfassung erfährt, geheim

1290 Das gilt vorbehaltlich funktionaler Besonderheiten, s.o.

1291 S. bereits oben 4.2.2.4.6 für den digitalen Personalausweis.

1292 Allerdings kommt es für den Schutzbereich des Allgemeinen Persönlichkeitsrechts nicht darauf an, ob dies konkret der Fall ist. Vielmehr wird ganz allgemein die „Beurteilung des Gesundheitszustands durch einen Arzt vor fremden Einblicken“ bewahrt, s. BVerfGE 32, 373 (380).

bleibt und nicht zur Kenntnis Unberufener gelangt. Nur so kann zwischen Patient und Arzt jenes Vertrauen entstehen, das zu den Grundvoraussetzungen ärztlichen Wirkens zählt, weil es die Chancen der Heilung vergrößert".[1293] Auch der Europäische Gerichtshof für Menschenrechte hat betont, dass eine Beschädigung des Vertrauensverhältnisses zwischen Patient und Arzt zu Gefahren für die Gesundheit führen kann.[1294] Dieses Verhältnis wird durch die Rechtsordnung dreifach geschützt, nämlich durch

- die Schweigepflicht der Informationsempfänger (diese ergibt sich aus § 203 StGB, der standesrechtlichen Norm des § 9 MBO-Ä 2004 und dem Behandlungsvertrag),[1295]
- das Zeugnisverweigerungsrecht des Arztes, anderer Beteiligter im Gesundheitswesen und deren Hilfspersonen in einem Prozess gegen den Versicherten (§§ 53 Abs. 1 Nr. 3, 53a StPO)[1296] und
- den Beschlagnahmeschutz für Mitteilungen, Aufzeichnungen und Befunde gegenüber Strafverfolgungsbehörden (§ 97 Abs. 1 StPO).[1297]

Das Zusammenspiel aus der (auch für Teilbereiche möglichen) Einwilligung des Patienten in die Datenerhebung und dem Schutz der erhobenen Daten, der nur durch den Patienten selbst aufgehoben werden kann, muss auch bei der elektronischen Gesundheitskarte erhalten bleiben. Es findet seine Rechtfertigung in der besonderen Sensibilität der verwendeten Daten, deren Bekanntwerden und Weitergabe an Versicherungen, Arbeitgeber, staatliche Organe oder andere soziale Interaktionspartner zu massiven Nachteilen für den Betroffenen führen können.

Die Befugnis des Versicherten, darüber zu entscheiden, wem gegenüber er welche Informationen offenbart, gilt aber auch innerhalb des Gesundheitswesens. Abgesehen von spezifischen ärztlichen Mitteilungspflichten und -rechten[1298] (bei denen die Daten empfangende Stelle an die besondere Zweckbindungsregel des § 39 Abs. 1 BDSG gebunden ist) findet auch hier die ärztliche Schweigepflicht sowohl in ihrer gesetzlichen[1299] als auch ihrer standesrechtlichen[1300] Ausprägung Anwendung. Dies ist Ausfluss des Prinzips der informationellen Gewaltenteilung. Danach darf jede Daten verarbeitende Stelle nur diejenigen Daten erheben und übermittelt bekommen, die sie zur Erfüllung ihrer Aufgaben benötigt. Das gilt auch im Gesundheitswesen: Ebenso wie die Verwaltung sind auch Krankenhäuser keine informationellen Einheiten. Ärzte dürfen sich nicht gegenseitig Einsicht in Unterlagen gewähren.[1301] Für Krankenhäuser wie für Praxisgemeinschaften sind voneinan-

1293 BVerfGE 32, 370 (380); s.a. *Beier* 1979, 55.

1294 Z ./. Finnland, Urteil v. 25.2.1997 (abrufbar unter http://www.echr.coe.int/Eng/Judgments.htm), Abs. 95; s. zu den Gefahren für das Vertrauensverhältnis auch *Lilie* 1980, 49; *GDD* 2002, 12.

1295 Dazu Laufs/Uhlenbruck-*Schlund/Ulsenheimer* 2002, 540 ff.; Hoeren/Sieber-*Sieber*, Kap. 19, Rn. 464 ff.; *Bäumler*, MedR 1998, 400; *Klöcker/Meister* 2001, 27 ff.; ausführlich zu § 203 StGB unten 4.2.3.5.1.

1296 S. *Meyer-Goßner*, § 53 Rn. 17 ff.; KK-*Senge*, § 53 Rn. 17 ff.; KMR-*Neubeck*, § 53 Rn. 14 f.

1297 Vgl. Laufs/Uhlenbruck-*Schlund* 2002, 583 ff.; *Meyer-Goßner*, § 97 Rn. 41 m.w.N.; SK StPO-*Rudolphi*, § 97 Rn. 56 und unten 4.2.3.5.2.

1298 Gesetzliche Pflichten zur Offenbarung bestehen etwa nach § 301 SGB V, §§ 6, 7 IfSG, §§ 138, 139 Abs. 3 StGB, § 39 JarbSchG; näher Laufs/Uhlenbruck-*Ulsenheimer* 2002, 554 ff.; Laufs/Uhlenbruck-*Schlund* 2002, 570 ff.; *GDD* 2002, 26 ff.; *LAK Baden-Württemberg* 2004, 17 ff.; *Kersten*, CR 1989, 1020, 1022; *Lilie* 1980, 96 ff., 111 ff.; *Meier* 2003, 159 ff.

1299 S. die Nachweise in Fn. 1256 (oben S. 209).

1300 Das ergibt sich mittelbar aus § 9 Abs. 4 MBO-Ä 2004, wonach mehrere Ärzte, die gleichzeitig oder nacheinander denselben Patienten untersuchen oder behandeln, untereinander von der Schweigepflicht insoweit befreit sind, als das Einverständnis des Patienten vorliegt oder anzunehmen ist.

1301 *GDD* 2002, 16, 25; *Meier* 2003, 47 m.w.N.

der abgeschottete Dokumentationssysteme erforderlich. Etwas anderes kann in Gemeinschaftspraxen gelten, in denen Patienten von einer Gruppe von Ärzten behandelt werden.[1302]

Für das System der Gesundheitskarte bedeutet dies insbesondere, dass es in der Verarbeitungsstruktur keinen „roten Knopf", also keinen Mechanismus geben darf, der unabhängig vom Willen des Patienten alle Daten über diesen zusammenführt.[1303] Die Missbrauchsgefahren einer solchen Zugriffsmöglichkeit wären zu groß. Datenverarbeitungen zu unterschiedlichen Zwecken sind außerdem organisatorisch zu trennen. In einigen Fällen lässt sich objektiv feststellen, welche Daten für die verantwortliche Stelle erforderlich sind. Weitaus häufiger allerdings wird eine Entscheidung darüber erfolgen müssen, wer zum Zugriff berechtigt ist. Diese Entscheidung kann aufgrund des informationellen Selbstbestimmungsrechts nur der Versicherte selbst treffen. Bei der Verwendung der Gesundheitskarte ist es möglich, diese Befugnis über eine Kombination von Besitz (der Gesundheitskarte) und Wissen (einer PIN) zu realisieren.[1304] Eine solche Absicherung durch eine zusätzliche Autorisierung ist in jedem Fall geboten. Aus der bloßen Vorlage der Karte beim Arzt kann nämlich nicht auf eine Einwilligung in die Anforderung oder den Abruf von Informationen bei anderen Leistungserbringern geschlossen werden, weil die Gesundheitskarte zum Zweck des Nachweises der Leistungsberechtigung (entsprechend der jetzigen Regelung zur Krankenversichertenkarte in § 15 Abs. 2 SGB V) vor dem Beginn jeder Behandlung vorgelegt werden muss.[1305] Keinesfalls kann der Auffassung gefolgt werden, bei einer Speicherung von Gesundheitsdaten auf der Karte seien weder Verschlüsselung noch Authentisierung des Zugreifenden erforderlich, weil davon auszugehen sei, der Patient habe den Lesezugriff autorisiert.[1306]

4.2.3.4.2 Zugriffsbefugnisse auf einzelne Anwendungen und technische Absicherung

§ 291a Abs. 4 und 5 SGB V enthalten Regelungen über Zugriffsbefugnisse für die auf oder mittels der elektronischen Gesundheitskarte gespeicherten Daten. Davon werden sowohl der lesende wie der schreibende Zugriff erfasst. Die Bestimmungen sind abschließend, sodass beispielsweise Krankenkassen kein Recht haben, auf die Daten des elektronischen Rezepts und der freiwilligen Anwendungen zuzugreifen. Legt man das Kriterium der Entscheidungshoheit des Versicherten über den Informationsfluss zugrunde, so ist fraglich, ob die Regelungen über den Zugriffsschutz hinreichend sind. Hierbei ist nach den einzelnen Anwendungen der elektronischen Gesundheitskarte zu differenzieren.

4.2.3.4.2.1 Verpflichtende Anwendungen

Der erste Gesetzesentwurf zum GKV-Modernisierungsgesetz sah noch eine technische Absicherung der Autorisierung des Versicherten beim „Zugriff auf und...Erheben, Verar-

1302 *GDD* 2002, 22 f.
1303 *BITKOM/VDAP/VHitG/ZVEI* 2003, 7, 52.
1304 Der Einsatz von Biometrie ist in Anbetracht des engen Zeitrahmens der Einführung der Gesundheitskarte unrealistisch, da es bislang kein Verfahren gibt, das eine der PIN vergleichbare Sicherheit garantiert und für den Einsatz bei allen Krankenversicherten in Deutschland geeignet wäre. Aus diesem Grund kommt der Einsatz von Biometrie lediglich für eine spätere Kartengeneration in Betracht; s.a. unten 6.3.3.2.
1305 Für die aktuell Krankenversichertenkarte: *Bultmann/Wellbrock/Biermann/Engels/Ernestus/Höhn/Wehrmann/Schurig* 2002, 6; *Der Landesbeauftragte für den Datenschutz Brandenburg* 2002, 98.
1306 So aber *Warda/Noelle* 2002, 136 f.

beiten und Nutzen von Daten unter Einsatz der elektronischen Gesundheitskarte“[1307] vor. Eine Ausnahme sollte nur für die Notfalldaten bestehen. Diese allgemeine Klausel hätte auch die verpflichtenden Anwendungen nach § 291a Abs. 2 Satz 1 SGB V erfasst, wobei für das elektronische Rezept eine weitere Ausnahme für Abrechnungszwecke vorgesehen war. In der nunmehr Gesetz gewordenen Fassung folgt dagegen im Umkehrschluss aus § 291a Abs. 5 Satz 2 SGB V, dass keine PIN-Eingabe oder vergleichbare technische Freigabe durch den Versicherten nötig ist.

Die Regelung wäre verfassungsrechtlich bedenklich, wenn für die verpflichtenden Anwendungen kein Einverständnis durch den Versicherten erforderlich wäre. In diese Richtung könnte § 291a Abs. 5 Satz 1 SGB V interpretiert werden, der das Erheben, Verarbeiten und Nutzen von Daten mittels der Gesundheitskarte für die freiwilligen Anwendung des § 291a Abs. 3 Satz 1 SGB V an das Einverständnis der Versicherten koppelt. Hieraus ließe sich im Umkehrschluss folgern, für die übrigen Anwendungen (insbesondere das elektronische Rezept) sei eine derartige Willensbekundung nicht erforderlich. Allerdings ergibt sich systematisch aus den folgenden Sätzen des § 291a Abs. 5 SGB V, dass dieser sich allein mit der technischen Umsetzung und Sicherstellung des Einverständnisses befasst, welches nur bei den freiwilligen Funktionen nach § 291a Abs. 3 Satz 1 SGB V zum Tragen kommt. Die Regelung trifft damit keine Aussage über die verpflichtenden Anwendungen nach § 291a Abs. 2 Satz 1 SGB V. Überdies verstieße eine Erhebung, Verarbeitung und Nutzung von Daten des elektronischen Rezepts ohne jedes Einverständnis des Patienten gegen sein Selbstbestimmungsrecht. In verfassungskonformer Auslegung ist § 291a Abs. 5 Satz 1 SGB V damit auf die technische Realisierung der Fälle des § 291a Abs. 3 Satz 1 SGB V zu beschränken. Ein Einverständnis des Versicherten bleibt auch für den Zugriff auf die Daten der verpflichtenden Anwendungen erforderlich.

Für die weitere Absicherung ist zu differenzieren. Das elektronische Rezept wird – wie die Daten der freiwilligen Anwendungen – zusätzlich dadurch geschützt, dass zum Zugriff gemäß § 291a Abs. 5 Satz 3 SGB V der Einsatz eines elektronischen Heilberufsausweises oder anderen Berufsausweises erforderlich ist. Bei Stammdaten und europäischem Berechtigungsnachweis (wenn dieser elektronisch gespeichert wird) erschöpft sich der Schutz dagegen in dem Erfordernis einer Einwilligung des Versicherten, die sich in der Übergabe der Karte manifestiert. Beide Datensätze werden damit nach dem Gesetz ohne technischen Zugriffsschutz gespeichert und können grundsätzlich mit jedem Chipkartenlesegerät ausgelesen werden. Dies entspricht der Situation bei der bisherigen Krankenversichertenkarte.[1308] Auch die Telematik-Expertise der Wirtschaft geht davon aus, dass der lesende Zugriff auf die Stammdaten wie bisher ohne Authentifizierung des Leistungserbringers möglich sein wird.[1309]

Fraglich ist jedoch, ob dies unter Berücksichtigung des informationellen Selbstbestimmungsrechts des Karteninhabers verfassungsrechtlich zulässig ist. Zwar ist die Information über das Bestehen eines Versicherungsverhältnisses im Grundsatz kein sensibles Datum. Deshalb ist der momentane Zustand des Auslesens ohne Autorisierung durch den Versicherten akzeptabel. Der Status Quo wird jedoch dadurch entscheidend verändert, dass mit der Einführung der elektronischen Gesundheitskarte nach § 291 Abs. 2 Satz 1 Nr. 8 SGB V in den Stammdatensatz eine Information über den Zuzahlungsstatus aufgenommen werden wird.[1310] Ist eine Zuzahlungsbefreiung eingetragen, so kann auf eine Erkrankung von er-

1307 BT-Drs. 15/1170, 39 (§ 291a Abs. 5 Satz 1 des Entwurfs).
1308 Vgl. *Fox*, DuD 1997, 600.
1309 *BITKOM/VDAP/VHitG/ZVEI* 2003, 57.
1310 Das bleibt unerwähnt im Kartenreport von *TeleTrusT* 2004, 9.

heblichem Umfang beziehungsweise auf eine chronische Krankheit geschlossen werden, insbesondere dann, wenn die Eintragung zu einem frühen Zeitpunkt im Kalenderjahr erfolgt. Deshalb stellt die Information über den Zuzahlungsstatus eine Angabe über die Gesundheit dar,[1311] die im Unterschied zu den sonstigen Stammdaten sensibel ist und nicht frei auf der Gesundheitskarte auslesbar sein darf.

Ein Zugriffsschutz ist insbesondere wegen der Gefahren des Verlusts und des Missbrauchs der Karte erforderlich. Da auf dieser ohnehin ein PIN-Mechanismus implementiert wird, wäre eine Sicherung technisch möglich. Diese könnte entweder über eine Ablage des kompletten Stammdatensatzes in einem geschützten Bereich oder durch einen Schutz nur des Datenfeldes „Zuzahlungsstatus" erreicht werden. Es müsste lediglich gewährleistet werden, dass die Krankenkassen zum Zweck der Änderung des Zuzahlungsstatus (die relativ häufig erfolgt) ebenfalls einen Zugriff erhalten.[1312] Problematisch ist allerdings, dass dann der Zugriff auf die Stammdaten insgesamt oder den Zuzahlungsstatus davon abhängig wäre, dass der Karteninhaber sich an die PIN erinnert. Dies könnte zu Komplikationen führen, da der Leistungserbringer in jedem Behandlungsfall auf die Stammdaten zugreifen und aufgrund der (teilweise erweiterten) Zuzahlungsregelungen[1313] in der überwiegenden Zahl der Fälle auch den Zuzahlungsstatus abfragen muss. Als Alternative zu der Verwendung einer PIN kommt eine Freischaltung der Stammdaten mittels eines elektronischen Heilberufsausweises in Betracht. Diese Form der Absicherung entspräche der Regelung für das elektronische Rezept und wäre insoweit datenschutzrechtlich akzeptabel. Die freie Auslesbarkeit der um den Zuzahlungsstatus erweiterten Stammdaten ist aber auf jeden Fall zu vermeiden. Deshalb genügt die derzeitige Gesetzeslage den verfassungsrechtlichen Anforderungen nicht.

Ähnlich wie die Stammdaten bleibt auch ein europäischer Berechtigungsnachweis in künftig elektronischer Form nach § 291a Abs. 2 Satz 1 Nr. 2 SGB V ohne jede technische Absicherung. Im Unterschied zu dem um den Zuzahlungsstatus erweiterten Stammdatensatz enthält er aber keine Informationen über die Gesundheit. Deshalb bestehen die obigen datenschutzrechtlichen Probleme nicht. Der durch den Besitz der Karte vermittelte Schutz für den Versicherten ist deshalb ausreichend.

Anders als bei den bisher betrachteten, mehr administrativen Daten regelt § 291a Abs. 4 Satz 1 Nr. 1 SGB V für das elektronische Rezept genau die Gruppe der Zugriffsberechtigten, nämlich Ärzte, Zahnärzte, Apotheker, Apothekerassistenten, Pharmazieingenieure, Apothekenassistenten, berufsmäßige Gehilfen sowie sonstige Erbringer ärztlich verordneter Leistungen. Diese Regelung ist im Prinzip sachgerecht, weil die genannten Leistungserbringer auf das elektronische Rezept zugreifen können müssen. Problematisch könnte allerdings sein, dass – im Unterschied zu den freiwilligen Anwendungen nach § 291a Abs. 3 Satz 1 SGB V – eine technische Autorisierung durch den Versicherten nicht erforderlich ist.[1314] Zwar besteht nach § 291a Abs. 5 Satz 5 SGB V für ihn die Möglichkeit, das Rezept durch ein „geeignetes technisches Verfahren" freizugeben. Diese Variante ist jedoch nur

1311 Daraus folgt auch die Anwendbarkeit der Regeln über besondere Arten personenbezogener Daten (§ 3 Abs. 9 BDSG); s. ausführlich unten 4.3.4.2.2.

1312 Nach den Planungen wird der gesamte Stammdatensatz für den Versicherungsträger updatefähig sein, s. *TeleTrusT* 2004, Anhang A, 5; s.a. die Begründung zum Gesetz zur Vereinfachung der Verwaltungsverfahren im Sozialrecht, BT-Drs. 15/4428, 28.

1313 § 61 SGB V und die auf diesen verweisenden Normen, z.B. §§ 23 Abs. 6 Satz 1, 24 Abs. 3 Satz 1, 31 Abs. 3 Satz 1, 32 Abs. 2 Satz 1, 33 Abs. 2 Satz 4, 37 Abs. 5, 37a Abs. 3, 38 Abs. 5, 39 Abs. 4, 40 Abs. 5 Satz 1, Abs. 6 Satz 1, 41 Abs. 3 SGB V.

1314 Unzutreffend *TeleTrusT* 2004, 9 f., wonach alle Bereiche außer dem Stammdatensatz einer Freischaltung durch den Versicherten bedürfen sollen.

als Alternative zur Freischaltung durch einen beliebigen elektronischen Heil- oder sonstigen entsprechenden Berufsausweis konzipiert. Letzteres wird innerhalb Deutschlands die Regel sein, während die selbständige Freigabe durch den Karteninhaber für den Einsatz im Ausland vorgesehen wurde.[1315] Dies schränkt die Datensicherheit für den Versicherten ein, insbesondere auch im Fall des Verlusts der Karte.

Auf der anderen Seite erscheint dieses Risiko hinnehmbar, weil das vorgesehene Verfahren hinsichtlich Datenschutz und Datensicherheit weitgehend dem jetzigen Ablauf entspricht. Wie bisher kann der Versicherte durch Vorlage (des Papierrezepts oder der Gesundheitskarte) darüber entscheiden, wer Zugriff auf das Rezept hat. Außerdem bleibt es möglich, unter Übergabe der Karte einen Dritten (etwa ein Familienmitglied) damit zu beauftragen, das Rezept einzulösen, ohne dass hierfür eine technische Zugriffsmöglichkeit eingerichtet werden muss. Beim Einlösen des Rezepts in der Apotheke kann – anders als beim Arztbesuch[1316] in der Aushändigung der Gesundheitskarte auch eine Autorisierung des Auslesens der Rezeptdaten durch den Versicherten gesehen werden, da die Karte zu genau diesem Zweck übergeben wird. Im Verlustfall wird sich die Stellung des Versicherten sogar verbessern: Im Unterschied zur Papierversion können nur Personen mit entsprechenden Heilberufsausweisen auf das elektronische Rezept zugreifen. Da die elektronische Gesundheitskarte als kontaktorientierte Chipkarte ausgestaltet werden wird, ist auch kein unbemerktes Auslesen möglich.

Obwohl sich kritisch anmerken lässt, dass bereits bei der ersten echten Massenanwendung der geplanten Telematikstruktur im Gesundheitswesen auf eine technische Sicherung zugunsten des Versicherten verzichtet wird (auffällig ist insoweit, dass dies auf alle verpflichtenden Anwendungen der Gesundheitskarte zutrifft), ist die Regelung damit im Ergebnis nicht zu beanstanden.

4.2.3.4.2.2 Freiwillige Anwendungen

Gemäß § 291a Abs. 5 Satz 1 SGB V steht die Erhebung, Verarbeitung und Nutzung der Daten aller freiwilligen Applikationen der elektronischen Gesundheitskarte unter dem Vorbehalt des Einverständnisses des Versicherten. Anders als beim elektronischen Rezept ist überdies nach § 291a Abs. 5 Satz 2 SGB V (neben dem Einsatz eines elektronischen Heilberufsausweises) mit Ausnahme der Notfalldaten eine technische Autorisierung durch den Versicherten erforderlich. Dies ist sachgerecht, weil die Daten der freiwilligen Anwendungen grundsätzlich wesentlich sensibler sind als die des elektronischen Rezepts.

Der Zugriff auf die Notfalldaten ohne technische Autorisierung ist sinnvoll und begegnet keinen Bedenken, da diese gerade bei Bewusstlosigkeit oder Bewegungsunfähigkeit des Karteninhabers verfügbar sein müssen.[1317] Auch für die Notfalldaten besteht das Erfordernis des Einverständnisses nach § 291a Abs. 5 Satz 1 SGB V. Man wird allerdings davon ausgehen können, dass mit dem Einverständnis in eine Speicherung von Notfalldaten auf der Karte gleichzeitig ein Einverständnis in das Auslesen im Notfall verbunden ist. In jedem Fall liegt etwa bei Bewusstlosigkeit nach einem Unfall ein mutmaßliches Einverständnis zur Nutzung der Daten vor, sofern nicht im Einzelfall gegenteilige Indizien bestehen.

1315 S. die Gesetzesbegründung, BT-Drs. 15/1525, 145.

1316 S.o. 4.2.3.4.1 a.E.

1317 S.a. *Iwansky* 1999, 111. Nach *BSI* 1995, XIV und 55 soll es nicht erforderlich sein, Notfalldaten zu speichern, da im Notfall kein Lesegerät verwendet werden könne. Dies wird jedoch nicht begründet und ist auch nicht zutreffend. Die Auffassung von *Fuest* (1999, 192 f.), wonach auch Notfalldaten durch PIN oder Biometrie gesichert werden müssen, verkennt den Verwendungszweck dieser Daten.

Die Regelung der Zugriffsbefugnisse bei den freiwilligen Anwendungen ist jedoch unter einem anderen Gesichtspunkt problematisch. Wie oben erläutert, gelten auch innerhalb des Gesundheitswesens die ärztliche Schweigepflicht und die Befugnis des Versicherten, selbst darüber zu entscheiden, welche Informationen er an wen weitergibt.[1318] § 291a Abs. 5 SGB sieht jedoch keine abgestuften Zugriffsrechte auf technischer Ebene vor. Nach dem Wortlaut kann der Versicherte durch seine technische Autorisierung den Zugriff auf den geschützten Speicherbereich nur vollständig freischalten.

Als Sicherung gegen einen nachfolgenden Vollzugriff des Leistungserbringers darf nach § 291a Abs. 4 Satz 1 SGB V auf die Daten nur zugegriffen werden, „soweit es zur Versorgung der Versicherten erforderlich ist". Hierin liegt ein grundsätzlicher Systemwechsel des Informationsflusses im Gesundheitswesen.[1319] Bislang entscheidet der Versicherte – und nur er[1320] – darüber, welche Leistungserbringer welche Daten erhalten. Das im Gesetz aufgestellte Kriterium der Erforderlichkeit bestimmt sich dagegen objektiv, zum Beispiel nach dem aktuellen Krankheitsbild und eventuellen Vorerkrankungen, aber auch nach der Funktion des zugreifenden Leistungserbringers. Sinnvoll ist, zwischen diesen zu differenzieren.

In manchen Fällen lässt sich nämlich objektiv ausschließen, dass bestimmte Daten für bestimmte Berufsgruppen zur Versorgung des Versicherten zur Verfügung stehen müssen. Das betrifft etwa Apotheker: Zur Erfüllung ihrer Funktion ist es nicht notwendig, Informationen über Krankheitsdiagnosen und gar die gesamte Krankengeschichte zu erhalten. Apotheker dürfen deshalb allein auf diejenigen Daten der Gesundheitskarte zugreifen, die die ärztliche Verordnung betreffen.[1321] § 291a Abs. 4 Satz 1 Nr. 2 c) SGB V gestattet also letztlich Apothekern und ihrem Personal – obwohl alle freiwilligen Anwendungen mit Ausnahme der Patientenquittung genannt sind – auf bestimmte Anwendungen gerade keinen Zugriff, weil dieser objektiv nicht erforderlich ist. Soweit dies, wie bei Behandlungsinformationen, für alle denkbaren Fälle gilt, ist der Zugriff auch technisch auszuschließen. Das kann über die die Einteilung der Gesundheitskarte in verschiedene Speicherbereiche geschehen, auf die nur mit entsprechenden Attribut-Zertifikaten zugegriffen werden kann.[1322]

Die Daten zur Prüfung der Arzneimitteltherapiesicherheit müssen den Apothekern demgegenüber zugänglich sein.[1323] Diese müssen gemäß § 20 Abs. 1 Satz 1 ApoBetrO ihre Kunden informieren und beraten, soweit dies aus Gründen der Arzneimittelsicherheit erforderlich ist.[1324] Grundsätzlich besteht zwar keine Pflicht, Neben- und Wechselwirkungen der Medikamente nochmals zu prüfen, die der Arzt verschrieben hat.[1325] Einnamemodalitäten und Wechselwirkungen können sich aber anders darstellen, wenn etwa ein Patient von zwei unterschiedlichen Ärzten zwei Medikamente erhält. Außerdem ergeben sich bei nicht rezeptierten Medikamenten aus § 20 Abs. 1 Satz 3 ApoBetrO besondere Hinweis-, Aufklärungs- und Beratungspflichten hinsichtlich der Kontraindikationen, Neben- und Wechselwirkungen.[1326] Es ist sinnvoll, auch nicht verschreibungspflichtige Mittel zu dokumentieren, weil diese unter Umständen ebenfalls zu gefährlichen Wechselwirkungen

1318 S.o. 4.2.3.4.1.
1319 Vgl. schon *Hornung* 2004a, 232.
1320 Vorbehaltlich der Ausnahmen der ärztlichen Mitteilungsbefugnisse, s.o. in Fn. 1298 (S. 219).
1321 S.a. *Dierks/Nitz/Grau* 2003, 202.
1322 S. zur Umsetzung unten 6.3.3.1.
1323 Dies ist nach der Gesetzesbegründung auch geplant, s. BT-Drs. 15/1525, 144.
1324 Vgl. *Deutsch/Spickhoff* 2003, Rn. 1186; *Quaas/Zuck* 2004, 688.
1325 *Deutsch/Spickhoff* 2003, Rn. 1193.
1326 *Deutsch/Spickhoff* 2003, Rn. 1186, 1193.

führen können,[1327] die vom Arzt sonst nicht erkannt werden würden. Hierzu sind eine Schreibberechtigung des Apothekers und sein Zugriff auf Grundinformationen wie Allergien und Ähnliches erforderlich. Falls die Sachkunde des Apothekers nicht zu einer Entscheidung ausreicht, könnte in einem Telephonat der verschreibende Arzt konsultiert werden.[1328]

Für behandelnde Ärzte kann demgegenüber nicht kategorial entschieden werden, auf welche Datenfelder sie zugreifen können müssen, weil prinzipiell alle Daten der freiwilligen Anwendungen für den Behandlungsfall von Bedeutung sein können. Die Regelung in § 291a Abs. 4 Satz 1 SGB V, die auf die Erforderlichkeit zur Versorgung des Versicherten abstellt, ist aus zwei Gründen kein wirksamer Schutz:

- Zum einen kann die objektive Erforderlichkeit einer Verwendung der Daten nur durch den jeweiligen Leistungserbringer bestimmt werden. Allenfalls ließe sich die Erforderlichkeit des Zugriffs verneinen, wenn der Versicherte nicht in den Zugriff auf ein bestimmtes Datum eingewilligt hat. Dagegen spricht aber, dass das Einverständnis des Versicherten (also die subjektive Komponente des Vorgangs) in § 291a Abs. 5 SGB V geregelt ist. Eine Begrenzung auf einzelne Informationen sieht das Gesetz dort nicht vor.
- Zum anderen wird im Regelfall die Erforderlichkeit eines Datenzugriffs ohne eben diesen Zugriff für den Leistungserbringer nicht zu erkennen sein. Ob sich in der Krankengeschichte des Versicherten Hinweise finden, die für die gegenwärtige Behandlung relevant sind, lässt sich nur bei Durchsicht der gesamten Krankengeschichte feststellen. Für die Beurteilung der Frage, ob sich aus anderen Medikationen Kontraindikationen für eine vom Arzt geplante Therapie ergeben, ist ein Zugriff auf die Daten zur Prüfung der Arzneimitteltherapiesicherheit erforderlich.

Beide Faktoren zusammen führen dazu, dass zumindest für den behandelnden Arzt das Kriterium der Erforderlichkeit nahezu immer erfüllt sein wird und dieser – nach der globalen Autorisierung durch den Patienten – auf den gesamten geschützten Speicherbereich der Karte zugreifen darf.

Unter dem Gesichtspunkt einer objektiv (das heißt allerdings vom Arzt – insoweit subjektiv – beurteilten) optimalen Gesundheitsversorgung mag ein derartiges System gerechtfertigt sein. Es widerspricht aber grundsätzlich der Konzeption des Arzt-Patient-Verhältnisses, das eben nicht paternalistisch von einseitigen Entscheidungsbefugnissen des Arztes, sondern von der Mitwirkung des Patienten bestimmt wird: Gemäß § 7 Abs. 1 MBO-Ä 2004 hat jede medizinische Behandlung unter Wahrung der Menschenwürde und unter Achtung der Persönlichkeit, des Willens und der Rechte des Patienten, insbesondere des Selbstbestimmungsrechts, zu erfolgen. Mit diesem Selbstbestimmungsrecht kollidiert die Einschränkung der Entscheidung des Versicherten auf die Alternativen der vollständigen Freigabe und der Totalverweigerung des Zugriffs auf die Daten.

Es obliegt dem Patienten zu entscheiden, ob er sich überhaupt in Behandlung begibt, eine (auch sinnvolle) Therapie verweigert oder vornimmt,[1329] welchen Risiken er sich aussetzt – und eben auch, welche Informationen er dem Arzt gegenüber offenbaren will. Dies gilt umso mehr, als bestimmte Gesundheitsinformationen die Intimsphäre in einem Maße berühren können, welches es unbedingt erforderlich macht, die Entscheidung über eine

1327 Etwa die gleichzeitige Einnahme von Aspirin mit anderen gerinnungshemmenden Mitteln (wie Trombosemedikamenten); s.a. *Grätzel v. Grätz* 2004c, 127 f.

1328 *TeleTrusT* 2004, 3.

1329 S. *Zuck* 1983, 33 ff. Man kann das plastisch als "Recht auf Krankheit" bezeichnen, s. ebd.; *Hammer/Roßnagel* 1989, 140.

Offenbarung dem Versicherten vorzubehalten.[1330] Ein System, in dem ein Orthopäde, der den Patienten möglicherweise zum ersten Mal behandelt, die Krankengeschichte auf mögliche Kontraindikationen gegen ein Schmerzmittel analysiert und dabei Kenntnis von einer schweren, länger zurückliegenden und mittlerweile ausgeheilten Geschlechtskrankheit des Patienten nimmt, wäre mit dieser Entscheidungsbefugnis nicht zu vereinbaren.

Macht der Arzt, oder ein anderer Leistungserbringer, demgegenüber deutlich, dass ein Zugriff auf sämtliche gespeicherten Daten im Einzelfall für die Behandlung nötig oder sinnvoll ist, so wird der Versicherte dies vernünftigerweise gestatten. Es muss ihm aber weiterhin möglich sein, bestimmte Informationen in vollem Bewusstsein darüber zurückzuhalten, dass daraus möglicherweise Nachteile für ihn selbst entstehen. Dies ist nur die logische Konsequenz des Selbstbestimmungsrechts, das eben auch die eigenverantwortliche Entscheidung darüber beinhaltet, bestimmte Risiken einzugehen.

Im Ergebnis ist damit die Erhebung, Speicherung und Nutzung von Gesundheitsdaten auf und mittels der Gesundheitskarte nur mit dem Selbstbestimmungsrecht des Patienten und dem Verhältnismäßigkeitsprinzip zu vereinbaren, wenn ein gestufter Zugriffsschutz im Einzelfall ermöglicht wird.[1331] Hierfür gibt es mehrere technische Umsetzungsmöglichkeiten.[1332]

Das Erfordernis der Einwilligung im Einzelfall gilt auch für den schreibenden Zugriff auf die Daten der freiwilligen Anwendungen.[1333] Gemäß § 291a Abs. 5 Satz 1 SGB V kann der Versicherte im Einzelfall in die Dokumentation auf oder mittels der Gesundheitskarte einwilligen oder diese verweigern. Eine andere Vorgehensweise erscheint auch angesichts des unbeschränkten Löschungsrechts des Karteninhabers in § 291a Abs. 6 Satz 1, 1. Halbsatz SGB V wenig sinnvoll. Es wäre eine überflüssige Belastung des Leistungserbringers und des Patienten, wenn letzterer zunächst die Dokumentation ohne seine Einwilligung hinnehmen müsste, um unmittelbar danach seinen Löschungsanspruch geltend zu machen. Liegt die Einwilligung vor, so können Behandlungs- und Medikationsinformationen durch den jeweiligen Leistungserbringer auf oder mittels der Gesundheitskarte dokumentiert werden. Dabei ist sicherzustellen, dass bereits vorhandene Einträge nicht unberechtigterweise verändert werden können und berechtigte Änderungen nachvollziehbar sind. Hierzu können elektronische Signaturen und Zeitstempel verwendet werden.

Mit dem Erfordernis einer Zugriffsautorisierung für alle Fälle der vom Versicherten selbst zur Verfügung gestellten Daten nach § 291a Abs. 3 Satz 1 Nr. 5 SGB V ist dem Gesetzgeber ein Fehler unterlaufen. Im Regelfall ist der PIN-Schutz hier natürlich sinnvoll: Entscheidet sich der Versicherte, Daten auf der Karte speichern zu lassen, so muss er auch über deren Freigabe bestimmen können. Dies ist jedoch nicht möglich, wenn der Versicherte Daten gerade für solche Konstellationen zur Verfügung stellt, in denen er keine Autorisierung vornehmen kann. Die Gesetzesbegründung selbst nennt die Patientenverfügung[1334] und den Organspendeausweis[1335] als Beispiele. In der Folge wurde ganz offen-

1330 S. insoweit bereits *Beier* 1979, 38 f.

1331 Ebenso *Wellbrock*, DuD 1994, 70, 72 f.; Roßnagel-*v. Zezschwitz*, Kap. 3.1, Rn. 99; *Fuest* 1999, 173; *Dierks/Nitz/Grau* 2003, 240; *BSI* 1995, XV; *Konferenz der Datenschutzbeauftragten* 2005; s. schon *Hornung* 2004a, 232.

1332 S. ausführlich unten 6.3.3.1.

1333 S.a. *Weichert*, DuD 2004, 391, 400.

1334 BT-Drs. 15/1525, 145; BT-Drs. 15/1170, 123 (1. Entwurf).

1335 BT-Drs. 15/1170, 123 (1. Entwurf). Diese Einordnung als Anwendung der selbst zur Verfügung gestellten Daten ist korrekt. Zwar handelt es sich bei der Situation, in der der Organspendeausweis benötigt wird, um einen Notfall. Der Einsatz des Ausweises erfolgt jedoch nicht zur Notfall*versorgung*, sodass eine Speicherung im Datenfeld nach § 291a Abs. 3 Satz 1 Nr. 1 SGB V (die wegen des Entfallens der technischen Autorisierung das im Folgenden beschriebene Problem lösen würde) nicht

sichtlich übersehen, dass nach dem Gesetz der – im Regelfall hirntote – Karteninhaber natürlich nicht in der Lage ist, mittels einer PIN den Zugriff auf seinen Organspendeausweis freizuschalten. Für diese Fälle ist die Zugriffsautorisierung im Wege der Gesetzesänderung neu zu regeln. Denkbar wäre eine Absicherung, die einen Zugriff nur mit Hilfe eines elektronischen Heilberufsausweises zuließe. Dies entspräche der Speicherung von Notfallinformationen nach § 291a Abs. 3 Satz 1 Nr. 1 SGB V. Für andere Daten, die der Versicherte selbst zur Verfügung stellt, ist der PIN-Schutz dagegen sinnvoll. Deshalb bietet sich eine (physische oder logische) Teilung des Datenfeldes entsprechend den jeweiligen Verwendungszwecken an.

Ebenfalls nicht überzeugend ist die Regelung zur Patientenquittung (§ 291a Abs. 3 Satz 1 Nr. 6 SGB V). Diese wird in § 291a Abs. 4 Satz 1 SGB V nicht erwähnt. Deshalb haben nur die Karteninhaber, nicht jedoch die Leistungserbringer Zugriff. § 291a Abs. 5 Satz 3 SGB V bestimmt jedoch, dass der Zugriff auf die Patientenquittung nur in Verbindung mit einem elektronischen Heilberufsausweis oder sonstigem Berufsausweis erfolgen darf, mit anderen Worten die Mitwirkung eines Leistungserbringers erforderlich ist, obwohl diesem der Zugriff auf die Daten verwehrt ist. Sinn und Zweck der Patientenquittung ist jedoch, dem Versicherten den transparenten und ausführlichen Nachvollzug der Behandlung in einer selbstgewählten Umgebung zu ermöglichen. Es ist unrealistisch anzunehmen, dass der Karteninhaber sich erneut zu einem Arzt begeben wird, um die Daten über in Anspruch genommene Leistungen und deren vorläufige Kosten einzusehen. Damit würde der Sinn und Zweck des Anspruchs auf eine Patientenquittung nach § 305 Abs. 2 SGB V verfehlt. Deshalb sollte ein selbständiger Zugriff auf diese Daten ermöglicht werden. Dies könnte in Anlehnung an die Zugriffsregelung für die selbst zur Verfügung gestellten Daten erfolgen, also unter Verwendung einer eigenen Signaturkarte des Inhabers, die über die Möglichkeit zur Herstellung qualifizierter elektronischer Signaturen verfügt.

4.2.3.4.2.3 Protokolldaten

Gemäß § 291a Abs. 6 Satz 2 BDSG ist durch technische Vorkehrungen zu gewährleisten, dass mindestens die letzten 50 Zugriffe auf die Daten „nach Absatz 2 oder Absatz 3“ für Zwecke der Datenschutzkontrolle protokolliert werden. Darunter fällt jeder Zugriff, insbesondere auch der auf die Versicherungsstammdaten. Diese sind in § 291a Abs. 2 Satz 1 SGB V zwar nicht gesondert aufgeführt, dennoch aber von der Verweisung umfasst. Es ließe sich zwar auch vertreten, dass § 291a Abs. 2 SGB V nur deklaratorisch auf § 291 Abs. 2 SGB V verweise und seinem Regelungsgehalt nach nur die verpflichtenden Zusatzfunktionen hinzufüge. Für eine umfassende Protokollierung spricht neben dem Wortlaut aber auch die Sensibilität der um den Zuzahlungsstatus erweiterten Stammdaten.[1336]

Die Regelung ist sinnvoll, um die Zugriffe auf die Gesundheitskarte zu kontrollieren. Die Sammlung von Protokolldaten birgt jedoch in erheblichem Maße das Risiko der Bildung von Bewegungs- und Behandlungsprofilen.[1337] Aus den Daten kann auf sämtliche Behandlungen eines Versicherten in einem unter Umständen sehr langen Zeitraum zurück-

---

in Betracht kommt. In der politischen Diskussion wird im Übrigen erwogen, jeden Versicherten bei der Ausgabe der Gesundheitskarte zu fragen, ob er sich als Organspender zur Verfügung stellen möchte, s. http://www.heise.de/newsticker/meldung/58304.

1336 S.u. 4.3.4.2.2.

1337 Dies stellt ein allgemeines Problem von Protokolldaten dar, vgl. Simitis-*Simitis*, § 14 Rn. 106 ff. m.w.N.; s. bereits *Der Bundesbeauftragte für den Datenschutz* 1993, 194.

geschlossen werden.[1338] Deshalb enthalten sie Informationen über die Gesundheit und sind damit besondere Arten personenbezogener Daten nach § 3 Abs. 9 BDSG,[1339] die keinesfalls in einem ungeschützten Speicherbereich der Karte abgelegt werden dürfen.

Zum Schutz der Protokolldaten ist in § 291a Abs. 6 Satz 3 SGB V eine Zweckbindung vorgesehen: danach dürfen diese ausschließlich zum Zweck der Datenschutzkontrolle verwendet werden. Die allgemeinen Regeln der §§ 14 Abs. 4, 31 BDSG werden von dieser Vorschrift verdrängt. Allerdings sind die Protokolldaten wie die Daten der freiwilligen Anwendungen der Gesundheitskarte (§ 291a Abs. 2 Satz 1 SGB V) nicht vom Erfordernis einer technisch abgesicherten Autorisierung durch den Versicherten in § 291a Abs. 5 Satz 2 SGB V erfasst. In § 291a Abs. 6 Satz 4 SGB V wurden aber „geeignete Vorkehrungen gegen zweckfremde Verwendung und sonstigen Missbrauch" normiert.

Diese Vorkehrungen können in der ausschließlichen Entscheidungsbefugnis des Karteninhabers stehen, weil sämtliche Leistungserbringer im Gesundheitswesen kein legitimes Interesse an der Kenntnis dieser Daten haben. Sie dienen nach dem ausdrücklichen Gesetzeswortlaut vielmehr der Datenschutzkontrolle. Damit darf der Zugriff nur dem Versicherten und nicht den Leistungserbringern (mit oder ohne Einsatz eines elektronischen Heilberufsausweises) offen stehen. Die Daten sollten auch den zuständigen Datenschutzbehörden zugänglich gemacht werden.[1340] Dies kann jedoch nicht ohne eine Mitwirkung des Karteninhabers erfolgen, weil die Daten Informationen über seine Gesundheit enthalten. Denkbar wäre der Schutz der Protokolldaten durch eine gesonderte PIN. Hiervon geht auch die Gesetzesbegründung aus.[1341]

Weggefallen ist gegenüber dem ersten Entwurf das ausdrückliche Erfordernis, die Zugriffe auf der Karte selbst zu protokollieren.[1342] In der Sache ändert dies aber nichts. Da zumindest einige Angaben (wie die Versicherungsstammdaten) ausschließlich auf der Gesundheitskarte gespeichert sind, ist eine Ablage der Protokolldaten auf der Karte selbst für eine vollständige Dokumentation unumgänglich. Für ein Dokumentationssystem in der Peripherie bestünde keine Möglichkeit, Zugriffe auf die elektronische Gesundheitskarte zu erkennen und zu protokollieren. Umgekehrt kann es im Einzelfall erforderlich sein, die Protokolldaten in der Peripherie – oder zumindest unter ihrer Mithilfe – zu erstellen. Nur so können beispielsweise Datum und Uhrzeit eines Datenzugriffs bestimmt und protokolliert werden, da die Gesundheitskarte keine Möglichkeit hat, diese Angaben autonom festzustellen.

Der Umfang der Protokollierung richtet sich nach ihrem Zweck zur Datenschutzkontrolle. Erforderlich ist damit zumindest die Angabe des Datensegments, auf das zugegriffen wurde, der Identität der zugreifenden Person und des Zeitpunkts des Zugriffs.

4.2.3.5 Normativer Schutz von Zweckbindung und Zugriffsbefugnissen

Die erläuterten abgestuften Zugriffsbefugnisse dienen dem Schutz der Zweckbindung der auf oder mittels der elektronischen Gesundheitskarte gespeicherten Daten. In vielen Situationen ist es möglich und notwendig, die Zweckbindung durch technische Absiche-

1338 Theoretisch wäre auch eine Erstellung von Tätigkeitsprofilen der Leistungserbringer möglich. Da jedoch die Protokollierung nach Zugriffen auf die Gesundheitskarte (nicht nach Leistungserbringern) erfolgt, müssten dazu sämtliche Protokolldaten aller Versicherten zusammengeführt werden. Dies erscheint nicht realistisch.

1339 S.u. 4.3.4.2.2.

1340 *Weichert*, DuD 2004, 391, 402.

1341 S. BT-Drs. 15/1525, 145.

1342 Vgl. § 291a Abs. 4 Satz 3 SGB V des ersten Entwurfs, BT-Drs. 15/1170, 39.

rungen zu schützen. Diese allein sind jedoch nicht ausreichend, weil trotz einer solchen Absicherung drei Risiken verbleiben, nämlich

- Indiskretionen durch Personen, denen bei den verantwortlichen Stellen der Zugriff technisch möglich ist,
- zweckerweiternde Zugriffe von Seiten der Strafverfolgungsorgane, die die verantwortliche Stelle zur Preisgabe von Daten zwingen können und
- die Ausübung sozialen Drucks auf den Versicherten, um diesen zur Preisgabe der gespeicherten Daten zu drängen.

Um dem vorzubeugen, ist ein normativer Schutz der Zweckbindung unumgänglich. Hierzu stehen für die genannten Risiken jeweils eigene rechtliche Schutzinstrumente zur Verfügung, nämlich die gesetzliche Schweigepflicht der Leistungserbringer, Zeugnisverweigerungsrechte und Beschlagnahmeschutz sowie abschreckende Normen des Straf- und Ordnungswidrigkeitsrechts.

4.2.3.5.1 Gesetzliche Schweigepflicht

Die Schweigepflicht der Leistungserbringer wird durch das gesetzliche Verbot des § 203 Abs. 1 Nr. 1 StGB gesichert, anvertraute Geheimnisse des Patienten zu offenbaren.[1343] Parallele Pflichten ergeben sich auch aus der standesrechtlichen Norm des § 9 MBO-Ä 2004 und dem Behandlungsvertrag.[1344] Die Schweigepflicht ist nicht nur Teil der ärztlichen Berufsethik,[1345] sondern auch Grundlage für eine vom Vertrauen des Patienten getragene wirkungsvolle ärztliche Behandlung.[1346] Das ist auch im Interesse der Allgemeinheit, weil – in den Worten des Bundesverfassungsgerichts – das Vertrauensverhältnis zwischen Versichertem und Leistungserbringer „Grundvoraussetzung ärztlichen Wirkens [ist], das die Chancen der Heilung vergrößert und insgesamt der Aufrechterhaltung einer leistungsfähigen Gesundheitsfürsorge dient".[1347] Ebenso hat der Europäische Gerichtshof für Menschenrechte darauf hingewiesen, dass ein beschädigtes Vertrauen in die Verschwiegenheit der Leistungserbringer Gefahren für die gesamte Bevölkerung hervorrufen kann.[1348]

§ 203 StGB ist ein Sonderdelikt, das nur durch die genannten Leistungserbringer (§ 203 Abs. 1 StGB), ihre berufsmäßig tätigen Gehilfen und Personen, die bei ihnen zur Vorberei-

1343 Der Bruch der ärztlichen Schweigepflicht wurde erstmals im Preußischen Allgemeinen Landrecht von 1794 unter Strafe gestellt, s. *LAK Baden-Württemberg* 2004, 5; *Meier* 2003, 130; ausführlich zur Schweigepflicht Laufs/Uhlenbruck-*Schlund/Ulsenheimer* 2002, 545 ff. und *Hermeler* 2000, 38 ff.; zum historischen Hintergrund *Lilie* 1980, 52 f.; *Kersten*, CR 1989, 1020; *Lin* 1996, 40 f.; *Goerke*, ZaeFQ 1999, 716 ff.

1344 *Bäumler*, MedR 1998, 400; *Klöcker/Meister* 2001, 29 ff.; *Ulsenheimer/Heinemann*, MedR 1999, 197, 202.

1345 *Laufs*, NJW 1975, 1433 m.w.N.

1346 *Kersten*, CR 1989, 1020; *Vahle*, DuD 1991, 614.

1347 BVerfGE 32, 373 (380). Ebenso wie das Grundrecht auf informationelle Selbstbestimmung (s.o. 4.1.1.2) hat damit auch die ärztliche Schweigepflicht eine „überindividuelle" Komponente; s.a. *Ulsenheimer/Heinemann*, MedR 1999, 197, 202; *Lilie* 1980, 78 f.; *Beier* 1979, 55; Roßnagel-*Schirmer*, Kap. 7.12, Rn. 23; zu diesem Gedanken bereits *Schmidt*, NJW 1962, 1745, 1747; *Laufs*, NJW 1975, 1433, 1434; s.a. *Roßnagel*, NJW 1989, 2303, 2306. Die Gewichtung zwischen dem individuellen Schutz des Einzelnen und dem Interesse der Allgemeinheit ist im Einzelnen umstritten, s. näher *Meier* 2003, 131 ff. m.w.N.

1348 Z ./. Finnland, Urteil v. 25.2.1997 (abrufbar unter http://www.echr.coe.int/Eng/Judgments.htm), Abs. 95.

tung auf den Beruf tätig sind (§ 203 Abs. 3 Satz 2 StGB) begangen werden kann.[1349] Die Norm verbietet die Offenbarung von Geheimnissen. Dies sind Tatsachen, die nur einem begrenzten Personenkreis bekannt sind, und an deren Geheimhaltung eine Privatperson ein schutzwürdiges Interesse hat.[1350] Letzteres wird bezüglich gesundheitlicher, familiärer und finanzieller Verhältnisse regelmäßig zu bejahen sein.[1351] Das Geheimnis muss dem Geheimnisträger anvertraut sein. Dies setzt voraus, dass er es – auf welche Weise auch immer – in Ausübung seines Berufes erfährt.[1352]

Die Tathandlung des Offenbarens ist verwirklicht, wenn das Geheimnis einem anderen, der davon keine oder keine gesicherte Kenntnis hat, bekannt gegeben wird.[1353] Das gilt auch dann, wenn es sich hierbei um eine Person handelt, die ihrerseits schweigepflichtig ist.[1354] Erforderlich ist schließlich, dass die Offenbarung unbefugt erfolgt. Dabei handelt es sich nach überwiegender Auffassung nicht um ein Tatbestandsmerkmal, sondern um einen Verweis auf die allgemeinen Rechtsfertigungsgründe.[1355]

Medizinische Daten, die dem Leistungserbringer anvertraut werden, unterfallen voll dem Geheimnisbegriff des § 203 StGB. Geschützt sind bereits die Tatsache eines Arztbesuchs und der Name des Patienten.[1356] Im System der Gesundheitskarte ist die ärztliche Schweigepflicht vor allem deshalb von besonderer Wichtigkeit, weil zumindest mittelfristig in weiten Bereichen mit einer Serverarchitektur gearbeitet werden wird, an der aller Voraussicht nach externe Dienstleister beteiligt sein werden.

Dies weist Parallelen zum Einsatz externen technischen Fachpersonals auf, der bereits bisher zur Wartung von Datenverarbeitungsanlagen beim Leistungserbringer oder über Online-Verbindungen (Fernwartung) erfolgt. Inwieweit hierbei ein Offenbaren im Sinne von § 203 vorliegt, ist umstritten.[1357] Vertreten wird, es sei eine mutmaßliche Einwilligung anzunehmen, da die Wartung im ureigensten Interesse des Patienten liege.[1358] Nach anderer Ansicht handelt es sich im Regelfall um eine Offenbarung, da mangels Sach- und Fachkenntnis des Arztes keine Überwachung möglich sei.[1359] Eine vermittelnde Auffassung geht davon aus, dass dann keine Offenbarung vorliegt, wenn der Arzt die Wartungsarbeiten überwacht und darauf achtet, dass kein Zugriff auf Patientendaten erfolgt.[1360]

1349 Den Leistungserbringern drohen daneben standesrechtliche Konsequenzen bis hin zum Widerruf der Approbation, s. Laufs/Uhlenbruck-*Ulsenheimer* 2002, 562; zu den Tätergruppen vgl. *Meier* 2003, 136 ff. m.w.N.

1350 BGHSt 41, 140 (142); LK-*Jähnke*, § 203 Rn. 19 ff.; Schönke/Schröder-*Lenckner*, § 203 Rn. 5 ff.; *Wessels/Hettinger* 2003, Rn. 563.

1351 *Kersten*, CR 1989, 1020, 1021.

1352 Schönke/Schröder-*Lenckner*, § 203 Rn. 13; *Hermeler* 2000, 45.

1353 RGSt 26, 5 ff.; 38, 62 ff.; BGH, NJW 1995, 2915, 2916; LK-*Jähnke*, § 203 Rn. 39; Schönke/Schröder-*Lenckner*, § 203 Rn. 19 m.w.N.

1354 S. die Nachweise in Fn. 1256 (oben S. 209).

1355 *Tröndle/Fischer*, § 203 Rn. 31 m.w.N.; differenzierend Schönke/Schröder-*Lenckner*, § 203 Rn. 21 (s. jedoch die dortigen Hinweise auf die h.M.).

1356 LG Köln, NJW 1959, 1598, 1599; OLG Oldenburg, NJW 1982, 2615, 2616; *Beier* 1979, 69; *Vahle*, DuD 1991, 614, 615; *Taupitz*, MDR 1992, 421, 424; *Lin* 1996, 49. Die Tatsache des Arztbesuchs unterfällt als Information über die Gesundheit insoweit auch § 3 Abs. 9 BDSG, s.u. 4.3.4.2.2.

1357 Davon losgelöst ist die datenschutzrechtliche Einordnung. Hier dürft im Regelfall eine Prüfung oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen nach § 11 Abs. 5 BDSG vorliegen; s.a. unten 4.3.6.

1358 *Ulsenheimer/Heinemann*, MedR 1999, 197, 202.

1359 *Bäumler*, MedR 1998, 400; *Wienke/Sauerborn*, MedR 2000, 517, 518 f.; s.a. *Otto*, wistra 1999, 201, 203.

1360 *ULD* 2002, unter 3; ähnlich *Ehmann*, CR 1991, 293, 294 f.

Die Speicherung auf externen Servern ist jedoch rechtlich nicht identisch mit dem Einsatz von Wartungspersonal, weil bei der Speicherung aktiv medizinische Daten an Dritte weitergegeben werden, die zuvor keine Kenntnis von diesen haben. Deshalb liegt in der Einspeisung dieser Daten in das Serversystem grundsätzlich ein Offenbaren von Geheimnissen, das der Rechtfertigung bedarf.

Eine andere Beurteilung ergibt sich dann, wenn der Leistungserbringer die Kontrolle über die externe speichernde Stelle hat und diese damit lediglich eine Gehilfenstellung einnimmt.[1361] Dies dürfte allerdings schon auf Dienstleister, die nur für einen einzelnen Leistungserbringer tätig werden, selten zutreffen. Eine Gehilfenstellung ist aber praktisch ausgeschlossen, wenn die Dienstleister für eine Vielzahl von Leistungserbringern Daten erheben, speichern und verarbeiten.[1362] Letzteres wird bei der Gesundheitskarte der Fall sein, sodass ein Offenbaren im Grundsatz vorliegen kann.

Aufgrund der Besonderheiten der modernen Datenverarbeitung ist es jedoch möglich, dass ein Offenbaren aus anderen Gründen ausscheidet. Bereits in der Vergangenheit wurde dieses Tatbestandsmerkmal verneint, wenn Patientendaten zur Verwahrung in anonymisierten und verschlossenen, beziehungsweise versiegelten Umschlägen an Archivunternehmen übergeben wurden.[1363] Das erscheint zwar diskussionswürdig. Durch moderne kryptographische Verschlüsselungsmechanismen ist es jedoch möglich, ein erheblich höheres Schutzniveau herzustellen. Wird durch eine sichere (Ende-zu-Ende-)Verschlüsselung die Kenntnisnahme durch den Empfänger ausgeschlossen und übernimmt dieser lediglich die Speicherung oder den Transport der Daten, so ist § 203 Abs. 1 StGB nicht verwirklicht.[1364] Gleiches gilt bei einer anonymisierten Weitergabe und für pseudonymisierte Daten, wenn bei diesen für den Dienstleister der Personenbezug nicht herstellbar ist.[1365]

Soweit bei der elektronischen Gesundheitskarte entsprechende Sicherungsmechanismen für den Einsatz externer Dienstleister ergriffen werden (was regelmäßig datenschutzrechtlich erforderlich ist), ist der Tatbestand von § 203 Abs. 1 Nr. 1 StGB damit nicht einschlägig. Wird im Einzelfall keine Sicherung vorgenommen, so ist eine Rechtfertigung erforderlich, die sich aus gesetzlichen Regelungen, ausdrücklicher, konkludenter und mutmaßlicher Einwilligung, den Grundsätzen der Güter- und Pflichtenabwägung und anderen Rechtfertigungsgründen ergeben kann.[1366] Für die regelmäßige Weitergabe von Daten an externe Dritte im System der Gesundheitskarte kämen nur die ersten beiden Alternativen in Betracht. Entweder müsste die Offenbarung gesetzlich geregelt werden, was bislang aufgrund

---

1361 *Kilian*, NJW 1987, 695, 697; *Inhester*, NJW 1995, 685, 688; *Geis*, DuD 1997, 582, 586 f.

1362 Zu weitgehend deshalb *Kilian*, NJW 1987, 695, 697, wonach auch Mitarbeiter in Rechenzentren, die Patientendaten dokumentieren, als Gehilfen des Arztes und nicht als außenstehende Dritte anzusehen sind. Das ist mit dem selbst aufgestellten Kriterium der „effektiven Kontrolle“ unvereinbar. Für eine erweiterte Auslegung des Gehilfenbegriffs plädieren *Hoenike/Hülsdunk*, MMR 2004, 788 ff. Die dort vorgeschlagene Abgrenzung hätte allerdings zur Folge, dass praktisch jede Outsourcing-Lösung im Gesundheitswesen ohne Einwilligung der Patienten zulässig wäre; das wäre mit der Grundkonzeption des Patientengeheimnisses unvereinbar.

1363 *Langkeit*, NStZ 1994, 6, 9; *Taupitz*, MDR 1992, 421, 424; s.a. Hoeren/Sieber-*Sieber*, Kap. 19, Rn. 476 ff.

1364 *Geis*, DuD 1997, 582, 587; *Hermeler* 2000, 141 ff.; *Bultmann/Wellbrock/Biermann/Engels/Ernestus/Höhn/Wehrmann/Schurig* 2002, 8.

1365 OLG Düsseldorf, CR 1997, 536 f.; *Klöcker/Meister* 2001, 74 f.; *ULD* 2002, unter 3.

1366 *BÄK*, DÄ 1996, A-2809, 2810 f.; *Hermeler* 2000, 47 ff.; *Tröndle/Fischer*, § 203 Rn. 32 ff.; *Wessels/Hettinger* 2003, Rn. 568; zu den gesetzlichen Pflichten einer Datenweitergabe s. die Nachweise in Fn. 1298 (S. 219).

der für Karten- und Serverlösung offenen Gesetzeslage nicht der Fall ist.[1367] Oder der Versicherte müsste im Behandlungsvertrag oder durch ausdrückliche oder konkludente[1368] Erklärung einer Offenbarung gegenüber Dienstleistern zustimmen. Eine mutmaßliche Einwilligung scheitert bei der elektronischen Gesundheitskarte dagegen im Regelfall bereits daran, dass ein ausdrückliches Befragen möglich ist.[1369]

Ist die verschlüsselte Weitergabe an externe Dritte damit möglich, so stellt sich das Problem, ob hierdurch das Schutzniveau für den Versicherten abgesenkt wird. Denn im Unterschied zum Beschlagnahmeschutz[1370] hat das GKV-Modernisierungsgesetz den personellen Anwendungsbereich der gesetzlichen Schweigepflicht und des Zeugnisverweigerungsrechts nicht auf die externen, Daten empfangenden Stellen erstreckt. Zwar wird der Datenweitergabe im Regelfall ein Vertrag zugrunde liegen, der auch entsprechende Verschwiegenheitspflichten enthalten wird. Diese werden allerdings im Unterschied zu der gesetzlichen Schweigepflicht der Leistungserbringer nicht strafbewehrt sein.

Einschlägig sind jedoch zwei andere Strafnormen. Externe Dienstleister haben kein Zugriffsrecht für die auf oder mittels der Gesundheitskarte gespeicherten Daten, da sie in der abschließenden Aufzählung in § 291a Abs. 4 Satz 1 SGB V nicht genannt werden. Ein Zugriff unter Verstoß gegen diese Bestimmung wird gemäß § 307a Abs. 1 SGB V mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.[1371] Da überdies die Daten auf dem Server verschlüsselt gespeichert werden und ein Zugriff nur unter Verwendung der elektronischen Gesundheitskarte des Versicherten möglich ist, greift bei einer Weitergabe der Daten durch den Dienstleister § 202a StGB ein.[1372] Danach wird bestraft, wer sich oder einem anderen unbefugt Daten verschafft, die nicht für ihn bestimmt und gegen unberechtigten Zugang besonders gesichert sind. Ein Beispiel für eine besondere Sicherung ist die Datenverschlüsselung.[1373] Im Ergebnis ergänzen sich – jedenfalls im Fall der verschlüsselten Speicherung – die Schutznormen der § 203 StGB einerseits sowie § 202a StGB und § 307a SGB V andererseits. Damit besteht ein hinreichender Schutz des Karteninhabers gegen missbräuchliche Zugriffe durch Angehörige dieser Gruppen.

1367 Eine Befugnis zur Auftragsdatenverarbeitung besteht zum Teil nach den Landeskrankenhausgesetzen, s. *Bultmann/Wellbrock/Biermann/Engels/Ernestus/Höhn/Wehrmann/Schurig* 2002, 8. Diese ist jedoch nicht auf ein bundesweites System anwendbar. Überdies liegt bei einer einrichtungsübergreifenden Serverarchitektur keine Auftragsdatenverarbeitung vor, s.u. 4.3.6.2.2.1.

1368 Eine konkludente Einwilligung widerspricht datenschutzrechtlich dem Regelfall des § 4a Abs. 1 Satz 3 BDSG. Dennoch ist sie strafrechtlich beachtlich, wobei allerdings hohe Anforderungen zu stellen sind. So ist die Weitergabe von Patientendaten an privatärztliche Verrechnungsstellen, externe Rechenzentren oder an Praxisübernehmer nur mit ausdrücklicher Einwilligung des Patienten zulässig, s. BGHZ 115, 123; 116, 268; OLG Düsseldorf, CR 1997, 536, 538; *Taupitz*, MDR 1992, 421 ff.; *Tröndle/Fischer*, § 203 Rn. 33; s. bereits *Roßnagel*, NJW 1989, 2303 ff. Eine Befugnis zur Übermittlung von Daten kann auch nicht allein aus dem Zweck des Behandlungsvertrages abgeleitet werden, s. Richtlinien der *BÄK*, DÄ 1996, A-2809, 2810; s.a. *Meier* 2003, 176 ff.

1369 *ULD* 2002, unter 2; allgemein für organisierte telemedizinische Anwendungen *Dierks/Nitz/Grau* 2003, 47. Das gilt jedenfalls im Bereich der Weitergabe an externe Stellen. In anderen Zusammenhängen kann die mutmaßliche Einwilligung weiterhin relevant sein, etwa beim Zugriff auf die Notfalldaten, wenn der Verletzte nicht zu einer ausdrücklichen Erklärung in der Lage ist.

1370 S.u. 4.2.3.5.2.

1371 S. näher unten 4.2.3.5.3, dort auch zur problematischen Reichweite der Norm.

1372 S.a. *Fuest* 1999, 113 f.

1373 *Lenckner/Winkelbauer*, CR 1986, 483, 487; Schönke/Schröder-*Lenckner*, § 202a Rn. 8; *Meyer-Goßner*, § 202a Rn. 8.

4.2.3.5.2 Zeugnisverweigerungsrecht, Beschlagnahmeschutz und Überwachung der Telekommunikation

§ 203 StGB wird durch die Zeugnisverweigerungsrechte in § 53 StPO und § 383 Abs. 1 ZPO in das Prozessrecht hinein „verlängert".[1374] Auch hierdurch wird das Vertrauensverhältnis zwischen Leistungserbringer und Patient geschützt.[1375] Ebenso wie § 203 StGB erfassen auch die Zeugnisverweigerungsrechte externe Dienstleister nicht. Im Unterschied zum materiellen Strafrecht wird dies jedoch nicht durch andere Normen kompensiert. Ein Zugriff auf die Daten eines Karteninhabers durch Dritte wäre also verboten, dieser könnte jedoch (falls die Daten nicht für ihn unzugänglich verschlüsselt sind) in einem Prozess gegen den Inhaber als Zeuge über den Dateninhalt vernommen werden. Es fragt sich deshalb, ob § 53 StPO entsprechend erweitert werden sollte. Dagegen spricht allerdings, dass auch bislang nicht allen Personen, die berufsmäßig Kenntnis von Gesundheitsdaten haben, ein Zeugnisverweigerungsrecht zugebilligt wird. Das gilt sogar für einige der in § 203 StGB genannten Geheimnisträger, beispielsweise für Angehörige eines Unternehmens der privaten Kranken-, Unfall- oder Lebensversicherung oder einer privatärztlichen Verrechnungsstelle (§ 203 Abs. 1 Nr. 6 StGB).[1376] Nach der Rechtsprechung des Bundesverfassungsgerichts darf der Kreis der Zeugnisverweigerungsberechtigten im Interesse einer funktionsfähigen Rechtspflege nicht beliebig ausgeweitet werden, sondern muss auf das unbedingt erforderliche Maß begrenzt werden.[1377] Für die Zulässigkeit eines Zeugnisverweigerungsrechts kann beispielsweise eine funktionierende Standesaufsicht durch Berufskammern sprechen, die gewährleistet, dass von dem Recht nicht unangemessen Gebrauch gemacht wird.[1378] Dieses Kriterium wäre bei externen Dienstleistern im Gesundheitswesen nicht erfüllt. Sie sind eher dem aufgeführten Personenkreis vergleichbar, der trotz Zugangs zu Gesundheitsdaten kein Zeugnisverweigerungsrecht hat. Eine Erweiterung von § 53 StPO ist deshalb im Ergebnis nicht geboten. Wenn eine sichere Ende-zu-Ende-Verschlüsselung eingerichtet wird, besteht das Problem überdies weitgehend nicht.

Nach § 94 Abs. 2 StPO bedarf es der Beschlagnahme, wenn eine Person Gegenstände, die als Beweismittel im Strafprozess in Frage kommen, in Gewahrsam hat und nicht freiwillig herausgibt. Da in elektronischer Form vorliegende Daten nicht verkörpert sind, können sie auf zwei Arten beschlagnahmt werden: durch eine Beschlagnahme des Datenträgers und durch das Kopieren der Daten auf einen anderen Datenträger ohne Beschlagnahme des ursprünglichen Trägers.[1379]

Das Beschlagnahmeverbot in § 97 StPO setzt dieser Form der Beweiserhebung allerdings Grenzen. Es dient im Gesundheitswesen – ebenso wie die gesetzliche Schweigepflicht und das Zeugnisverweigerungsrecht – dem Schutz des Vertrauensverhältnisses

---

1374 Wobei allerdings keine vollständige Übereinstimmung besteht, s. *Meyer-Goßner*, § 53 Rn. 4 m.w.N.; zum Zeugnisverweigerungsrecht der Leistungserbringer nach § 383 Abs. 1 Nr. 6 ZPO vgl. Baumbach-*Hartmann*, § 383 Rn. 13 m.w.N.

1375 BVerfGE 38, 312 (323); OLG Oldenburg, NJW 1982, 2615, 2616; *Meyer-Goßner*, § 53 Rn. 1 m.w.N.

1376 Umgekehrt verfügen einige Personengruppen (etwa Geistliche) über ein Zeugnisverweigerungsrecht, das unabhängig von einer strafrechtlichen Verschwiegenheitspflicht besteht.

1377 BVerfGE 33, 367 (383); 38, 312 (321).

1378 BVerfGE 33, 367 (383 f.).

1379 Ausführlich *Bär* 1992, 266 ff. § 94 StPO bietet hierfür eine hinreichende Grundlage, vgl. auch *Schäfer*, wistra 1989, 8, 12; *Möhrenschlager*, wistra 1991, 321, 329; s.a. *Meyer-Goßner*, § 94 Rn. 16a; KK-*Nack*, § 94 Rn. 4 m.w.N. Das weitere Problem, inwieweit nach der Beschlagnahme ein Anspruch der Strafverfolgungsbehörden auf Entschlüsselung (bzw. eine Möglichkeit zur Beschlagnahme der Entschlüsselungsschlüssel) besteht, bleibt im Folgenden ausgeklammert. Im Regelfall besteht diese Möglichkeit, s. *Hermeler* 2000, 129 ff.; KK-*Nack*, § 94 Rn. 4.

zwischen Leistungserbringer und Versichertem, nicht jedoch dem Schutz des Leistungserbringers in einem gegen ihn geführten Strafprozess.[1380] Die Regelung bezweckt, eine Umgehung der Zeugnisverweigerungsrechte der in §§ 52, 53, 53a StPO genannten Personen zu verhindern.[1381] Dies ist notwendig, weil die Tätigkeit zum Beispiel von Ärzten oder Anwälten in aller Regel nicht ohne das Anfertigen von Aufzeichnungen und den Schriftverkehr mit dem jeweiligen Klienten denkbar ist. Ließe man eine Beschlagnahme und nachfolgende strafrechtliche Verwertung dieser Gegenstände zu, so würde das Zeugnisverweigerungsrecht ad absurdum geführt und das diesem zugrundeliegende Vertrauensverhältnis insgesamt beschädigt.

§ 97 Abs. 1 StPO nimmt deshalb bezogen auf das Gesundheitswesen drei Gruppen von Gegenständen von der Beschlagnahme aus:

- schriftliche Mitteilungen zwischen dem Versicherten und den in § 53 Abs. 1 Nr. 3 StPO genannten Leistungserbringern (Ärzten, Zahnärzten, psychologischen Psychotherapeuten, Kinder- und Jugendlichenpsychotherapeuten, Apothekern und Hebammen),
- Aufzeichnungen, die diese über ihnen anvertraute Mitteilungen und Umstände machen, sowie
- andere Gegenstände, auf die sich das Zeugnisverweigerungsrecht erstreckt. Das Gesetz nennt als Beispiel hierfür ausdrücklich ärztliche Untersuchungsbefunde.[1382]

Der Beschlagnahmeschutz gilt nach § 97 Abs. 3 StPO entsprechend auch für die Berufshelfer der Leistungserbringer nach § 53a StPO.

Da der Schutzzweck des Beschlagnahmeverbots die Absicherung des Vertrauensverhältnisses zwischen Patient und Leistungserbringer ist, findet das Verbot nach § 97 Abs. 2 Satz 1 StPO nur Anwendung, sofern sich der Gegenstand im Gewahrsam der zur Zeugnisverweigerung berechtigten Person befindet. Sind die Informationen dagegen aus anderer Quelle verfügbar, so ist dieses Verhältnis nach der gesetzgeberischen Vorstellung nicht tangiert. Speziell für das Gesundheitswesen regelt allerdings § 97 Abs. 2 Satz 2 StPO, dass auch der Gewahrsam einer Krankenanstalt ausreicht, wenn es um einen Gegenstand geht, auf den sich das Zeugnisverweigerungsrecht eines der genannten Leistungserbringer erstreckt.

Der geplante Einsatz der elektronischen Gesundheitskarte hätte unter diesen Bedingungen dazu geführt, dass eine Reihe von gespeicherten Daten nicht mehr von der Beschlagnahme ausgenommen gewesen wäre, weil kein Gewahrsam eines Leistungserbringers vorliegt: Die Gesundheitskarte mitsamt ihres Dateninhalts befindet sich im Gewahrsam des Versicherten,[1383] und in der Telematikstruktur werden externe Dienstleister die Speicherung oder Verarbeitung von Daten übernehmen. Sofern diese Dienstleister nicht selbst

1380 BGHSt 38, 144 (146) m.w.N.; *Meyer-Goßner*, § 97 Rn. 4 f.; KK-*Nack*, § 97 Rn. 8, jeweils m.w.N.

1381 BVerfGE 20, 162 (188); 32, 373 (385); BGHSt 38, 144 (145); *Beulke* 2002, Rn 248; *Meyer-Goßner*, § 97 Rn. 1; *Michalowski*, ZStW 109, 519, 642 f. Auch ansonsten gibt es Normen, die zur diesem Zweck eingeführt wurden (zuletzt § 100h Abs. 2 StPO, dazu *Wollweber*, NJW 2002, 1554, 1555).

1382 Zur Anwendung auf das Gesundheitswesen *Hermeler* 2000, 36 ff.

1383 Die Gewahrsamsverhältnisse wären sehr kompliziert, wenn es auf die jeweiligen Zugriffsmöglichkeiten ankäme: Da der Versicherte auf die meisten Daten nur mit Hilfe eines Leistungserbringers und dessen elektronischem Heilberufsausweises zugreifen kann, läge insoweit wohl Mitgewahrsam vor. Gewahrsam besteht jedoch nur an körperlichen Sachen. Deshalb kommt es nicht auf die Zugriffsmöglichkeit, sondern auf den Gewahrsam am Datenträger an, s. *Hermeler* 2000, 127 f.

zeugnisverweigerungsberechtigt sind,[1384] hätte nach alter Rechtslage kein Beschlagnahmeschutz eingegriffen.

Der Gesetzgeber hat diese neuen Gefahren und die Unklarheit über den Anwendungsbereich von § 97 StPO zur Kenntnis genommen und den Beschlagnahmeschutz angepasst.[1385] Die Gesundheitskarte unterliegt nach dem neuen § 97 Abs. 2 Satz 1 StPO auch dann nicht der Beschlagnahme, wenn sie sich – wie regelmäßig – nicht im Gewahrsam des Leistungserbringers befindet. Der Wortlaut der Norm ist allerdings missverständlich, da die Gesundheitskarte selbst an sich gar nicht von § 97 Abs. 1 StPO erfasst wird und § 97 Abs. 2 Satz 1 StPO sich auf diesen bezieht. Die Bestimmung ist deshalb so auszulegen, dass sie selbständig die Beschlagnahme der Gesundheitskarte und der Daten untersagt, die auf ihr oder unter ihrer Verwendung gespeichert werden.

Die neue Fassung von § 97 Abs. 2 Satz 2 StPO ordnet darüber hinaus an, dass der Gewahrsam eines Dienstleisters, der für die genannten Leistungserbringer Daten erhebt, verarbeitet oder nutzt, genauso behandelt wird wie der einer Krankenanstalt.

Im Prinzip besteht damit ein hinreichender Schutz der Informationen auch unter den neuen Bedingungen der Datenverarbeitung. Allerdings muss der Schutz der Gesundheitskarte vor Beschlagnahme so verstanden werden, dass er sich auch auf die oben erwähnte Variante des Kopierens von Daten ohne Beschlagnahme der Karte selbst bezieht. Andernfalls wäre die Regelung wirkungslos. Des Weiteren ist der Begriff des „Dienstleisters“ in § 97 Abs. 2 Satz 2 StPO umfassend zu verstehen. Hierunter fallen nicht nur unabhängige Betreiber, die ein komplettes Speicher- und Nutzungsmanagement anbieten, sondern auch deren Unterauftragnehmer, Anbieter, die kleine Verarbeitungen lediglich im Rahmen ihrer sonstigen Tätigkeit miterledigen, sowie die Betreiber der zugrundeliegenden technischen Infrastruktur.

Nach der Rechtsprechung des Bundesgerichtshofes und der herrschenden Meinung in der Literatur endet der Beschlagnahmeschutz auch bei einer unfreiwilligen Besitzaufgabe. Der Gegenstand kann bei einem Dieb oder Finder beschlagnahmt werden.[1386] Dies wird damit begründet, dass sich die Stoßrichtung der staatlichen Maßnahme dann nicht mehr gegen das Vertrauensverhältnis zwischen Patient und Leistungserbringer richte. Obwohl dies im Grundsatz zutrifft, ist diese Auffassung unter den Bedingungen einer massenhaften Speicherung von Gesundheitsdaten auf mobilen Medien und bei externen Dritten in Frage zu stellen. Für die Gesundheitskarte besteht das Problem nicht, da sie nie, das heißt auch nicht bei einem unfreiwilligen Abhandenkommen, der Beschlagnahme unterliegt. Die Verarbeitung und Nutzung durch externe Dritte birgt jedoch auf zwei Ebenen zusätzliche Gefahren. Zum einen werden hier Daten täglich zwischen verschiedenen Stellen hin- und herübermittelt. Auch bei der gebotenen Verwendung sicherer Verschlüsselungsverfahren

1384 In diesem Fall wäre eine Anwendung des § 97 Abs. 2 Satz 1 StPO a.F. durchaus diskutabel gewesen, s. *Bultmann/Wellbrock/Biermann/Engels/Ernestus/Höhn/Wehrmann/Schurig* 2002, 8.

1385 Dies wurde auch von *BITKOM/VDAP/VHitG/ZVEI* (2003, 73) gefordert; s.a. *Der Landesbeauftragte für den Datenschutz Baden-Württemberg* 1998, 30; *Reichow/Hartlep/Schmidt*, MedR 1998, 162, 166; *Warda/Noelle* 2002, 172; *Hermeler* 2000, 133 ff. (keine verfassungsrechtliche Notwendigkeit, Gesetzesänderung aber politisch wünschenswert); *Klöcker/Meister* 2001, 75 f.; *Wehrmann/Wellbrock*, CR 1997, 754, 757; *Fuest* 1999, 113, 115 f., 180; differenzierend *Dierks/Nitz/Grau* 2003, 165 ff. (Erweiterung auf externe Dienstleister empfehlenswert, nicht aber auf die Gesundheitskarte); grundlegend a.A. *Iwansky* 1999, 143, wonach sich ein Beschlagnahmeverbot für die Gesundheitskarte „aus verfassungsrechtlichen Gründen nicht realisieren lassen“ soll. Dabei werden jedoch staatliche Strafverfolgungsinteressen zu hoch gewichtet und die strafprozessuale Gefährdungslage verkannt, die durch die Gesundheitskarte hervorgerufen wird.

1386 BGH, 3 StR 432/76 v. 15.12.1976; AK StPO-*Amelung*, § 97 Rn. 12; *Meyer-Goßner*, § 97 Rn. 13; Löwe/Rosenberg-*Schäfer*, § 97 Rn. 22; SK StPO-*Rudolphi*, § 97 Rn. 17; a.A. *Beulke* 1980, 210.

kann dabei kaum garantiert werden, dass Daten niemals ausspioniert werden. Zum anderen besteht die Gefahr, dass bei einem speichernden Dienstleister interne oder externe Angriffe auf die Daten verübt werden, die beim Leistungserbringer nicht oder nur erschwert möglich wären. In beiden Fällen könnten die Informationen nach der genannten Rechtsprechung zu einem späteren Zeitpunkt beschlagnahmt und verwertet werden.

Zwar wird das Vertrauensverhältnis zwischen Leistungserbringer und Versichertem durch einen einzelnen Fall der Beschlagnahme nach einem Abhandenkommen von Daten in der Regel nicht beschädigt werden. Aber auch ein solcher Einzelfall kann dazu führen, dass der Patient aufgrund wirklicher oder angenommener Datensicherheitsrisiken in der Telematikstruktur seine Offenheit dem Arzt gegenüber einschränkt. Unter diesen Umständen sollte die genannte Rechtsprechung zumindest für das System der Gesundheitskarte modifiziert werden.

Im Rahmen des strafprozessualen Verfahrens unterfällt der direkte Zugriff der Strafverfolgungsbehörden auf die Übertragungswege der medizinischen Daten § 100a StPO.[1387] Es handelt sich nicht um eine Beschlagnahme, weil die Daten während des Übertragungsvorgangs nicht verkörpert sind.[1388] Nach § 100a StPO kann bei einem auf Tatsachen gestützten Verdacht auf eine der dort aufgeführten Katalogtaten die Überwachung und Aufzeichnung der Telekommunikation angeordnet werden, wenn die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise aussichtslos oder wesentlich erschwert wäre. Die Norm enthält keine Privilegierung für Daten, die zwischen Leistungserbringern im Gesundheitssystem oder von einem Leistungserbringer zu einem externen Dienstleister und umgekehrt übermittelt werden. Eine Analogie zu § 53 StPO oder § 97 StPO ist nach der Rechtsprechung des Bundesgerichtshofes[1389] und der herrschenden Meinung in der Literatur[1390] abzulehnen.

Nach geltendem Recht ist damit eine Überwachung der Datenströme der Serverarchitektur im Gesundheitswesen zur Beweisgewinnung über einen Versicherten nach § 100a StPO zulässig, wenn die sonstigen Voraussetzungen der Norm erfüllt sind. Das Problem wird zwar dadurch entschärft, dass auf den Übertragungswegen ohnehin starke Verschlüsselungsverfahren anzuwenden sind. Diese bieten jedoch keinen absoluten Schutz. Deshalb stellt sich die Frage, ob eine Ausnahmeregelung in § 100a StPO entsprechend der Neufassung von § 97 StPO erforderlich ist. Hiergegen spricht zwar, dass auch heute schon eine Beschlagnahme ärztlicher Unterlagen auf dem Postweg nach § 99 StPO und eine Überwachung von Telefongesprächen mit dem Arzt nach § 100a StPO möglich ist.[1391] Im Unterschied zum System der elektronischen Gesundheitskarte sind diese Kommunikationswege jedoch vom Versicherten kontrollierbar; dieser kann etwa dadurch ausweichen, dass er persönlich die Arztpraxis aufsucht. Außerdem ist bislang keinesfalls das Abhören und Ausforschen einer kompletten Krankengeschichte möglich. Dies wäre jedoch bei der Übertragung einer elektronischen Patientenakte der Fall. Schließlich wäre es auch ein eindeutiger Wertungswiderspruch, die Daten bei beiden Teilnehmern der Übertragung (sowohl beim Leistungserbringer als auch beim externen Dienstleister) vor einer Beschlagnahme zu

1387 S. *Hermeler* 2000, 119.

1388 *Hermeler* 2000, 120; allgemeiner *Meyer-Goßner*, § 100a Rn. 2 m.w.N.

1389 BGHSt 29, 23 (25). Eine Ausnahme gilt aufgrund § 148 StPO für den Verkehr mit dem Verteidiger, s. BGHSt 33, 347 (348 ff.).

1390 *Werle*, JZ 1991, 482, 484 ff.; *Hermeler* 2000, 123 ff.; Löwe/Rosenberg-*Schäfer*, § 100a Rn. 25; *Meyer-Goßner*, § 100a Rn. 10 m.w.N.; a.A. SK StPO-*Rudolphi*, § 100a Rn. 17 ff.; AK StPO-*Maiwald*, § 100a Rn. 12 ff.

1391 *Hermeler* 2000, 135; Ausnahmen bestehen in beiden Fällen lediglich für die Kommunikation mit dem Verteidiger, s. *Meyer-Goßner*, § 99 Rn. 13, § 100a Rn. 21, jeweils m.w.N.

schützen, einen Zugriff auf dem Übertragungsweg jedoch zulassen. Im Ergebnis ist § 100a StPO deshalb entsprechend anzupassen.

4.2.3.5.3 Schutznormen im SGB V

Der Gesetzgeber hat im Rahmen des GKV-Modernisierungsgesetzes im Sozialrecht besondere Vorschriften zum Schutz der Zweckbindung der auf oder mittels der elektronischen Gesundheitskarte gespeicherten Daten eingerichtet. Nach § 307a SGB V wird der Zugriff unter Verstoß gegen die Zugriffsbefugnisse der Leistungserbringer zur Versorgung des Karteninhabers (§ 291a Abs. 4 Satz 1 SGB V) unter Strafe gestellt, während §§ 291a Abs. 8, 307 Abs. 1 SGB V dem Schutz des Versicherten vor der Ausübung sozialen Drucks dienen.

Bei diesen Normen ist problematisch, dass sich ihr Anwendungsbereich nicht auf alle Daten der elektronischen Gesundheitskarte erstreckt. Sie beziehen sich nicht auf die Stammdaten und den (zumindest mittelfristig) elektronisch gespeicherten europäischen Berechtigungsnachweis. Dies ist in Anbetracht der Erweiterung des Stammdatensatzes um den Zuzahlungsstatus und dessen Sensibilität[1392] nicht akzeptabel. Je nach Sachlage kann die Information einer Zuzahlungsbefreiung wesentlich sensibler sein als die einer Standardmedikation. Auch der missbräuchliche Zugriff auf den Stammdatensatz ist damit normativ abzusichern. Noch gravierender ist, dass § 307a SGB V durch die Verweisung auf § 291a Abs. 4 Satz 1 SGB V keinen Schutz für die Daten der so genannten Patientenquittung gemäß § 291a Abs. 3 Satz 1 Nr. 6 SGB V bietet.[1393] Diese enthalten Informationen über in Anspruch genommene Leistungen des Versicherten, die ebenso schutzbedürftig sind wie die zugehörigen Behandlungsergebnisse. § 307a SGB ist dementsprechend zu erweitern.

Tathandlung der Strafnorm des § 307a Abs. 1 SGB V ist der Verstoß gegen § 291a Abs. 4 Satz 1 SGB V. Deshalb gliedert sich der personelle Anwendungsbereich in zwei Gruppen, nämlich die dort genannten Leistungserbringer (vor allem Ärzte, Zahnärzte, Apotheker und das sie unterstützende Hilfspersonal) und andere. Für die zweite Tätergruppe ist der Zugriff auf die Daten stets strafbar. Für die in § 291a Abs. 4 Satz 1 SGB V genannten Personen kommt dagegen eine Straftat nur dann in Betracht, wenn auf Daten zugegriffen wird, soweit es nicht „zur Versorgung des Versicherten erforderlich ist“. Hier stellt sich insbesondere die oben beschriebene Neuordnung des Informationsflusses bei der Gesundheitskarte[1394] als Problem dar. Die Erforderlichkeit eines Zugriffs wird der Leistungserbringer – wenn kein klarer Sachverhalten vorliegt – in vielen Fällen erst nach eben diesem Zugriff beurteilen können. Dabei wird ihm aber bewusst sein, dass die abgerufenen Daten möglicherweise gerade nicht zur Versorgung erforderlich sind, und er wird dies auch zumindest billigend in Kauf nehmen. Der objektive und subjektive strafrechtliche Tatbestand wäre damit erfüllt.

Allerdings wird der Karteninhaber in diesen Fällen regelmäßig in den Zugriff des behandelnden Arztes eingewilligt haben. Da der Versicherte über die Daten verfügungsbefugt ist,[1395] kann er eine solche strafrechtlich rechtfertigende Einwilligung auch wirksam erteilen. Zu beachten ist, dass der Karteninhaber in einen Zugriff einwilligt, der den daten-

1392 S. bereits oben bei der Frage der technischen Absicherung des Zugriffs (4.2.3.4.2.1).

1393 Dagegen bezieht sich § 291a Abs. 8 Satz 1 SGB V nur hinsichtlich des berechtigten Personenkreises auf § 291a Abs. 4 Satz 1 SGB V, verweist aber ausdrücklich auf alle Anwendungen nach § 291a Abs. 3 Satz 1 SGB V.

1394 S.o. 4.2.3.4.2.2.

1395 S.o. 4.2.3.4.1, dort auch zu den bestehenden Einschränkungen.

schutzrechtlich normierten Regelfällen widerspricht. An die Freiwilligkeit und Eindeutigkeit der Einwilligung sind deshalb hohe Anforderungen zu stellen.[1396]

Eine Einwilligung kommt auch dann in Betracht, wenn ein Zugriff durch Personen erfolgt, die keine Leistungserbringer sind. Allerdings schränkt § 291a Abs. 8 Satz 1 SGB V die Einwilligungsmöglichkeit des Versicherten ein. Dort wird die Vereinbarung über eine Gestattung des Zugriffs auf die Daten durch Personen, die nicht in § 291a Abs. 4 Satz 1 SGB V genannt sind, ausdrücklich untersagt. Gleiches gilt, wenn der Zweck des Zugriffs nicht die Versorgung des Versicherten (einschließlich der Abrechnung von Leistungen) ist. Gestattet in diesen Fällen der Versicherte vertraglich, also freiwillig, den Zugriff, so bleibt der Vertragsschluss für seinen Vertragspartner verboten. Hieraus könnte gefolgert werden, § 291a Abs. 8 Satz 1 SGB V schließe eine rechtfertigende Einwilligung im Rahmen von § 307a SGB V aus. § 307 Abs. 1 SGB V bestimmt jedoch, dass bei einem Verstoß gegen § 291a Abs. 8 Satz 1 SGB V eine Ordnungswidrigkeit vorliegt. Damit liegt kein gesetzlicher Ausschluss der Einwilligungsmöglichkeit vor, und diese wirkt rechtfertigend hinsichtlich einer möglichen Straftat nach § 307a SGB V. Dies gilt also unabhängig davon, ob es sich bei dem Täter um einen Leistungserbringer handelt oder nicht.

§ 307a Abs. 2 SGB V enthält Qualifikationstatbestände. Während ein Verstoß gegen § 307a Abs. 1 SGB mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft wird, erhöht sich die Strafdrohung auf Freiheitsstrafe bis zu drei Jahren oder Geldstrafe, wenn der Täter gegen Entgelt oder in der Absicht handelt, sich oder einen Anderen zu bereichern oder einen Anderen zu schädigen. Grundtatbestand und Qualifikation sind gemäß § 307a Abs. 3 SGB V Antragsdelikte. Antragsberechtigt sind der Betroffene und der Bundesbeauftragte für den Datenschutz oder die zuständige Aufsichtsbehörde.

§ 291a Abs. 8 und § 307 Abs. 1 SGB V sollen vor Einflussnahmen auf den Versicherten schützen. Eines der Hauptziele des Projekts der elektronischen Gesundheitskarte ist der erweiterte, erleichterte und schnellere Zugang zu Gesundheitsdaten. Dies ist nützlich und sinnvoll, solange diese Daten zum Zwecke der Gesundheitsvorsorge verwendet werden. Gleichzeitig steigt aber die Gefahr von Begehrlichkeiten durch Personen oder Institutionen, zu denen der Versicherte in sozialen Abhängigkeitsverhältnissen steht. Als Beispiele werden hier häufig Arbeitgeber und Versicherungen genannt.

Der Patient ist insoweit in einer zwiespältigen Position.[1397] Je stärker seine Rolle im Gesamtgefüge des Informationsflusses ist, desto mehr wird seine Stellung als eigentliches Subjekt der Datenverarbeitung im Gesundheitswesen betont und seine informationelle Selbstbestimmung gestärkt. Eine weitgehende Entscheidungsbefugnis des Einzelnen hat jedoch zur Folge, dass seine Entscheidung über eine Datenfreigabe von seinem sozialen Umfeld beeinflusst werden kann.

In gewisser Weise bestehen diese Risiken bereits gegenwärtig.[1398] Auch ohne die geplante Telematikstruktur im Gesundheitswesen kann auf Versicherte Druck ausgeübt werden, Behandlungsergebnisse zu offenbaren, sich untersuchen zu lassen oder Leistungserbringer von ihrer Schweigepflicht zu entbinden. Die Probleme werden aber durch die leichtere Verfügbarkeit der Daten verschärft. So bietet die elektronische Gesundheitskarte,

1396 Vgl. zum Verhältnis zwischen datenschutzrechtlicher und strafrechtlich rechtfertigender Einwilligung oben Fn. 1368 (S. 232); zur Sicherung der Freiwilligkeit der Einwilligung oben Fn. 1229 (S. 205).

1397 S. hierzu schon *Hornung* 2004a, 233.

1398 Deshalb gibt es auch schon seit der Verwendung von EDV im Gesundheitswesen Warnungen vor Datensammlungen, die mehr oder weniger freiwillig anderen Institutionen zur Verfügung gestellt werden, vgl. z.B. *Schaefer* 1979, 22. Die Auswirkungen des Einsatzes von Telematik auf das Problem des sozialen Drucks werden seit einigen Jahren diskutiert, s. etwa den Bericht von *Klinkhammer*, DÄ 1998, A 1437, 1438.

konsequent angewendet, den Zugang zu einer elektronischen Patientenakte mit allen oder allen wesentlichen Informationen über die gesamte Krankengeschichte des Versicherten, wenn er es wünscht. Im heutigen System gibt es eine derartige Datensammlung nicht.[1399] Die Zusammenführung kann dem Versicherten auch unter sozialem Druck kaum abgenötigt werden. Besteht dagegen eine elektronische Patientenakte, so kann er bei einem beliebigen Arzt eine Art „Gesundheitsauszug" über seine Krankengeschichte und den aktuellen Gesundheitszustand erhalten. Diese Vereinfachung erhöht das Risiko, dass der Versicherte psychischem oder materiellem sozialen Druck ausgesetzt wird und diesem nachgibt.

Um dem vorzubeugen, regelt § 291a Abs. 8 Satz 1 SGB V, dass vom Inhaber der Gesundheitskarte nicht verlangt werden darf, den Zugriff auf das elektronische Rezept und alle Informationen nach § 291a Abs. 3 Satz 1 SGB V anderen als berechtigten Personen oder zu anderen Zwecken als denen der Versorgung zu gestatten. Es darf auch keine Vereinbarung über eine solche Gestattung getroffen werden. Gemäß § 291a Abs. 8 Satz 2 SGB V dürfen aus der Bewirkung oder Verweigerung des Zugriffs weder Vor- noch Nachteile erwachsen. Die Vorschrift des § 291a Abs. 8 Satz 1 SGB V (nicht jedoch § 291a Abs. 8 Satz 2 SGB V) ist in § 307 Abs. 1 SGB V bußgeldbewehrt. Je nach der Art und den Umständen der Druckausübung können daneben auch allgemeine Straftatbestände, insbesondere Nötigung (§ 240 StGB), in Betracht kommen.

Im Ergebnis ist der Zugriff von Nicht-Leistungserbringern ohne Gestattung des Versicherten eine Straftat; mit einer abgenötigten oder vertraglich vereinbarten Gestattung handelt es sich um eine Ordnungswidrigkeit, wobei darüber hinaus Vorfeldhandlungen (Vereinbarung über die Gestattung) mit einbezogen sind. Die nachgelagerten Vorgänge der Bevorzugung oder Benachteiligung aufgrund der Gestattung oder deren Verweigerung sind dagegen zwar gemäß § 291a Abs. 8 Satz 2 SGB V unzulässig, ein Verstoß gegen dieses Verbot wird jedoch nicht sanktioniert.[1400] Leistungserbringer machen sich strafbar, wenn sie nicht zu Zwecken der Versorgung oder in größerem Umfang, als es zur Versorgung erforderlich ist, auf die Daten zugreifen. Auch hier wirkt eine Einwilligung rechtfertigend. Verlangt der Leistungserbringer die Einwilligung oder vereinbart er sie mit dem Karteninhaber, so verbleibt eine Ordnungswidrigkeit.

Zu einer Strafbarkeitslücke kann es allerdings kommen, wenn ein Leistungserbringer im Auftrag eines Dritten auf die Daten zugreift. So könnte etwa ein Arbeitgeber von einem Bewerber verlangen, dem mit einem elektronischen Heilberufsausweis ausgestatteten Betriebsarzt den Zugriff zu gestatten. In diesem Fall beginge der Arzt aufgrund der Einwilligung keine Straftat nach § 307a SGB V. Gleichzeitig läge in seiner Person jedoch auch keine Ordnungswidrigkeit vor, weil er als ausführendes Organ weder vom Versicherten dessen Gestattung verlangt, noch mit ihm einen Vertrag über die Gestattung geschlossen hätte. Allerdings verbliebe für den Arbeitgeber eine Ordnungswidrigkeit, weil dieser vom Bewerber die Gestattung zu einem anderen Zweck als dem der Versorgung gefordert hätte. Dennoch sollte die genannte Lücke geschlossen werden, weil der Betriebsarzt sich sonst kaum gegen das Ansinnen des Arbeitgebers zur Wehr setzen wird. De lege lata verbleiben in gravierenden Fällen die Möglichkeiten standesrechtlicher Konsequenzen und einer Bestrafung wegen Teilnahme an einer eventuellen Nötigung durch den Arbeitgeber.

1399 Es besteht zwar die Möglichkeit einer umfassenden Dokumentation durch den Hausarzt nach § 73 Abs. 1b SGB V. Diese ist jedoch freiwillig. Außerdem können die beteiligten Personen die Vollständigkeit der Dokumentation nicht überprüfen. Wenn der Versicherte keinen Hausarzt angibt oder eine Übermittlung ablehnt, verbleiben insoweit Lücken.

1400 Das gilt jedenfalls im Bereich des Straf- und Ordnungswidrigkeitenrechts. Wenn die Bevorzugung oder Benachteiligung in einer Vertragsklausel enthalten ist, kommt je nach Sachverhalt eine Nichtigkeit gemäß § 134 BGB in Betracht.

4.2.3.6 Eigene technische Zugriffsmöglichkeit des Karteninhabers?

Fragen des sozialen Drucks spielen auch eine Rolle bei der Abwägung, ob dem Versicherten ein eigenes Einsichtsrecht in die auf oder mittels der elektronischen Gesundheitskarte gespeicherten Daten eingeräumt werden sollte. Dieses könnte etwa vom heimischen PC ausgeübt werden, dem Patienten so erstmals einen direkten Zugang zu den über ihn gespeicherten Informationen verschaffen und ihn damit mehr als bisher zum „mündigen" Subjekt im Gesundheitswesen werden lassen. § 291a Abs. 5 Satz 3, 2. Halbsatz SGB V sieht bisher ein eigenes technisches Zugriffsrecht nur für selbst zur Verfügung gestellte Daten vor.[1401] Zur Ausübung ist außerdem eine Signaturkarte des Versicherten erforderlich, die qualifizierte Signaturen erstellen kann. Daneben ist dem Karteninhaber die Einsicht der Daten des elektronischen Rezepts möglich, weil er dieses nach § 291a Abs. 5 Satz 5 SGB V auch ohne Mitwirkung eines Leistungserbringers freischalten kann.

Ein allgemeines individuelles Einsichtsrecht würde hohe Anforderungen an die technische Infrastruktur stellen. Es wäre vermutlich nur in einem offenen Netz zu realisieren, in dem die Sicherheit der transportierten Daten schwierig zu garantieren wäre. Darüber hinaus sollten möglichst alle Versicherten über Chipkarten mit qualifizierten Signaturverfahren verfügen, weil andernfalls ein Ungleichgewicht hinsichtlich des individuellen Informationszugangs die Folge wäre. Zwar soll die elektronische Gesundheitskarte technisch zur Erstellung qualifizierter Signaturen in der Lage sein.[1402] Eine allgemeine Ausstattung der Karte mit dieser Funktion ist jedoch bislang nicht vorgesehen. Dieser Einwand würde sich allerdings dann erledigen, wenn es aufgrund der Einführung des JobCard-Verfahrens zu einer weiten Verbreitung von Signaturkarten kommen sollte.[1403]

Für ein eigenes individuelles Einsichtsrecht spricht, dass damit der Transparenzgedanke im Gesundheitswesen wesentlich gestärkt würde. Erstmals erhielte der Versicherte die Möglichkeit, in einer selbst gewählten Umgebung ohne Zeitdruck Auskunft über seinen Gesundheitszustand, vorgenommene Behandlungen und abgerechnete Leistungen zu erhalten. Dies könnte zu einem bewussteren Umgang mit Ressourcen beitragen, weil dem Versicherten erweiterte Kontrollmöglichkeiten über das Verhalten der Akteure an die Hand gegeben würden. Aus der Perspektive des aufgeklärten Patienten ist ein eigenes Informationszugangsrecht anzustreben.

Problematisch erscheint dieses dagegen bei Einbeziehung der genannten sozialen Abhängigkeiten. Der eigene Zugriff auf Gesundheitsdaten ohne Mitwirkung eines Leistungserbringers würde ein Szenario ermöglichen, in dem bei einem Vorstellungsgespräch der Bewerber – etwa mit dem verklausulierten Hinweis, es diene der Verbesserung seiner Chancen – dazu aufgefordert werden könnte, über einen bereitstehenden PC seine aktuellen Gesundheitsdaten zur Einsichtnahme bereitzustellen. Insoweit stellt die aktuell vorgesehene Lösung durchaus eine Art Mittelweg dar, indem sie dem Versicherten zwar einen Zugriff auf die auf oder mittels der Gesundheitskarte gespeicherten Daten einräumt, diesen aber in weitem Umfang technisch an die Mitwirkung eines Leistungserbringers knüpft. Hierdurch werden insbesondere Überrumpelungsfälle wie in dem genannten Beispiel verhindert. Es ist damit nicht zutreffend, dass für den Gesetzgeber nur die Wahl zwischen

1401 § 291a Abs. 4 Satz 2 SGB V beinhaltet kein technisches Zugriffsrecht, s.u. 4.3.7.3.

1402 Es soll sich um eine Mikroprozessorkarte mit einem zertifizierten Betriebssystem handeln, s. die Gesetzesbegründung, BT-Drs. 15/1525, 144; s.a. die eCard-Strategie der Bundesregierung, http://www.bundesregierung.de/-,413.799497/artikel/eCard-Strategie-der-Bundesregi.htm.

1403 S. dazu bereits oben 2.1.3 und unten 4.2.4.2.

dem uneingeschränkten Informationsrecht des Patienten und der vollständigen Verhinderung des Zugriffs und damit dem Verlust seiner Datenhoheit besteht.[1404]

Auf der anderen Seite kann der Gefahr sozialen Drucks durch geeignete Strafbestimmungen vorgebeugt und begegnet werden. Überdies wäre es zu weitgehend, mit dem Argument einer Erpressbarkeit des Versicherten diesem den selbstbestimmten Zugriff auf seine Daten zu verwehren. Da dieses Verfahren wesentlich einfacher ist als ein Gang zum Arzt (der eventuell ausschließlich zu dem Zweck erfolgen würde, das Auskunftsrecht geltend zu machen), ist auch zu erwarten, dass deutlich mehr Versicherte ihre Daten einsehen würden. Dies dient sowohl der informationellen Selbstbestimmung des Einzelnen als auch der Effektivität des Gesundheitswesens.

Sofern die genannten technischen Probleme lösbar sind, sollte deshalb ein eigener Zugriff durch den Inhaber der Gesundheitskarte ermöglicht werden. Für die nahe Zukunft wäre zumindest eine Umsetzungsvariante denkbar, bei der der Versicherte die Informationen an Terminals, zum Beispiel in Arztpraxen oder örtlichen Filialen von Krankenkassen, einsehen könnte. Hierdurch wäre eine Lösung ohne offenes Netz denkbar. Gleichzeitig würde auch das Risiko einer vorschnellen Freigabe von Informationen minimiert. Für die verbleibenden Gefahren würde die Verbotsnorm des § 291a Abs. 8 SGB V eingreifen. Auch wenn Missbrauchsfälle hierdurch nicht völlig verhindert werden können, wäre dieser Schutz zumindest dann hinreichend, wenn der Anwendungsbereich der Norm auf alle Daten der Karte erweitert würde.[1405]

4.2.4 Die verfassungsrechtliche Zulässigkeit des JobCard-Verfahrens

Für das geplante JobCard-Verfahren besteht bislang keine gesetzliche Regelung. Allerdings gibt es konkrete Überlegungen für die technische Umsetzung. Diese bauen auf dem bisherigen Datenfluss in der Arbeitslosenversicherung auf.

Ist ein Arbeitnehmer arbeitslos, hat er gemäß § 117 Abs. 1 SGB III Anspruch auf Arbeitslosengeld, wenn er sich bei der Arbeitsagentur arbeitslos gemeldet und die Anwartschaft erfüllt hat, die nach § 123 in Verbindung mit § 124 Abs. 1 SGB III im Regelfall erreicht wird, wenn der Arbeitnehmer in den letzten zwei Jahren vor Beginn der Arbeitslosigkeit mindestens zwölf Monate versicherungspflichtig beschäftigt war.[1406] Die Höhe des Arbeitslosengelds richtet sich gemäß § 130 Abs. 1 SGB III im Grundsatz nach dem durchschnittlichen Verdienst der letzten 52 Wochen vor dem Eintritt des Leistungsfalls (Bemessungszeitraum). Der Arbeitslose muss beim Antrag die erheblichen Tatsachen angeben und auf Verlangen des Leistungsträgers Beweisurkunden vorlegen (§ 60 Abs. 1 Satz 1 Nr. 1 und 3 SGB I). Das betrifft beim Arbeitslosengeld die Arbeitsbescheinigung. In dieser hat der Arbeitgeber nach § 312 Abs. 1 Satz 1 SGB III bei Beendigung eines Beschäftigungsverhältnisses alle Tatsachen zu bescheinigen, die für die Entscheidung über den Anspruch auf Arbeitslosengeld, Arbeitslosenhilfe, Unterhalts- oder Übergangsgeld erheblich sein können.[1407] Diese Pflicht trifft den Arbeitgeber, obwohl er jeden Monat nach § 28d SGB IV den Sozialversicherungsbeitrag an die Einzugsstelle (regelmäßig die gesetzliche Kran-

1404 So aber *BITKOM/VDAP/VHitG/ZVEI* 2003, 52. Das Argument, dem Informationsrecht des Patienten sei „uneingeschränkt Vorzug zu geben", geht an der Sache vorbei, weil auch im dort vorgeschlagenen Konzept kein selbständiges technisches Zugriffsrecht des Versicherten vorgesehen ist.

1405 S. zum Problem des Anwendungsbereiches oben 4.2.3.5.3.

1406 Vgl. näher Hauck/Noftz-*Valgolio*, § 117 Rn. 5 ff.; zur Anwartschaft ebd., § 123 Rn. 6 ff.; § 124 Rn. 6 ff.

1407 Zum Inhalt der Bescheinigungspflicht s. Hauck/Noftz-*Voelzke*, § 312 Rn. 38 ff.

kenkasse des Arbeitnehmers) überweist[1408] und sich daraus die für den Anspruch wesentlichen Daten ergeben.

4.2.4.1 Der geplante Ablauf des Verfahrens

Im künftigen JobCard-Verfahren sollen sowohl Arbeitgeber wie Arbeitnehmer hinsichtlich der Arbeitsbescheinigungen entlastet werden.[1409] Die Arbeitgeber übermitteln monatlich im Online-Verfahren die Arbeits- und Verdienstbescheinigungen sowie Angaben zur Auflösung von Beschäftigungsverhältnissen an eine Zentrale Speicherstelle.[1410] Sie werden gleichzeitig von der Pflicht entlastet, die Bescheinigungen aufzubewahren und im Leistungsfall bereitzustellen. Das System setzt an der bereits gesetzlich festgeschriebenen Pflicht für Arbeitgeber an, ab dem 1. Januar 2006 Bescheinigungen an die Sozialversicherungsbehörden nur noch in elektronischer Form zu übermitteln.[1411] Die Speicherstelle bestätigt den Eingang der Daten, überprüft ihre Vollständigkeit und speichert sie (unter Verwendung von Session-Keys) in verschlüsselter Form. Dabei wird zunächst intern die Sozialversicherungsnummer als Ordnungskriterium verwendet. Nach der allgemeinen Verbreitung von Signaturkarten soll dies auf die Zertifikatsnummer umgestellt werden.

Die Speicherung der Daten erfolgt somit ohne Mitwirkung der Arbeitnehmer. Der Abruf hat dagegen zur Voraussetzung, dass sich diese eine Signaturkarte besorgen und mit den zugehörenden Zertifikaten bei der „Registratur Fachverfahren“ anmelden, wo eine Verknüpfung zwischen Zertifikats- und Sozialversicherungsnummern erfolgt. Wird der Arbeitnehmer arbeitslos, so begibt er sich zur Arbeitsagentur und füllt dort ein elektronisches Formular, die Einverständniserklärung zum Datenabruf, aus. Diese wird sowohl von ihm als auch vom Mitarbeiter der Arbeitsagentur qualifiziert signiert und dann zur Zentralen Speicherstelle gesendet. Die Speicherstelle prüft – automatisiert – die beiden Signaturen und die Gültigkeit der Zertifikate. Anhand der Zertifikatsnummer des Arbeitnehmers kann sie im Anschluss daran die zugehörige Sozialversicherungsnummer bestimmen und die gespeicherten Daten identifizieren. Im Ergebnis verwendet das JobCard-Verfahren den Signaturschlüssel der Karte des Arbeitnehmers für zwei Zwecke, nämlich zur formgerechten Datenschutzeinwilligung nach §§ 4a BDSG, 128 Abs. 3, 126a BGB sowie zur Authentisierung.[1412]

Der Datenabruf kann während der Gültigkeit der Einverständniserklärung durch einen von mehreren berechtigten Mitarbeitern der Arbeitsagentur erfolgen. Sie authentisieren sich gegenüber der Zentralen Speicherstelle, die die individuelle Berechtigung und – erneut – die bei ihr gespeicherte Einverständniserklärung überprüft. Im Erfolgsfall werden die Daten des Antragstellers an die Arbeitsagentur übermittelt, wo sie zur Überprüfung der Leistungsberechtigung und der Höhe der Ansprüche weiterverarbeitet werden.

1408 Diese leitet die Beiträge an die Rentenversicherer und die Bundesagentur für Arbeit weiter.

1409 S. etwa *ITSG* 2003; *Hornung/Roßnagel*, K&R 2004, 263, 264 f.; *Schulzki-Haddouti*, c't 13/2004, 46 f.; *Der Bundesbeauftragte für den Datenschutz* 2005, 41 f.; 153 ff. Herr *Schlottke* (Applied Security GmbH) war auf der CeBIT 2004 so freundlich, Fragen zum Thema zu beantworten.

1410 Die folgende Darstellung orientiert sich am geplanten Ablauf im Vollbetrieb. Dieser wird in der Praxis als sog. „JobCard II“ bezeichnet. In einer Übergangsphase („JobCard I“) soll es nur zu einer Übermittlung von Daten durch die Arbeitgeber kommen, wenn ein Arbeitsverhältnis beendet wird.

1411 S. §§ 28a Abs. 1, 28b Abs. 2 SGB IV in der ab dem 1.1.2006 geltenden Fassung, wonach Meldungen nur noch per maschinell verwertbarem Datenträger oder Datenfernübertragung erfolgen dürfen.

1412 Vgl. *Hornung/Roßnagel*, K&R 2004, 263, 265.

4.2.4.2 Zulässigkeit einer verpflichtenden Implementierung von Verfahren der elektronischen Signatur, Verschlüsselung und Authentisierung

Wird dieses Verfahren eingeführt, so benötigt jeder Antragsteller in der gesetzlichen Arbeitslosenversicherung ab dem Jahre 2007 eine qualifizierte Signaturkarte. Denkbar wäre zunächst, eine Chipkarte mit hohem Verbreitungsgrad (wie den digitalen Personalausweis oder die elektronische Gesundheitskarte) verpflichtend mit einer Signaturfunktion auszustatten. Ein solches Vorgehen ist nicht geplant, wäre aber – zumindest bei den derzeitigen Gebühren der Zertifizierungsdiensteanbieter[1413] – auch unverhältnismäßig. Zwar werden Millionen Bundesbürger für das JobCard-Verfahren eine Signaturkarte benötigen.[1414] Diese Gruppe wird jedoch immer noch die Minderheit in der Bevölkerung sein. Da eine Beschränkung der Verpflichtung zum Besitz von Signaturkarten auf die vom JobCard-Verfahren Betroffenen möglich ist, ist dies der weniger belastende Eingriff. Die verpflichtende Ausgabe von Zertifikaten ist damit unzulässig, solange sie mit erheblichen finanziellen Belastungen verbunden ist.

Eine andere Frage ist, ob die Einrichtung eines staatlichen Verfahrens möglich ist, das eine Vielzahl von Bürgern zum Besitz einer Signaturkarte verpflichtet, ohne dass Ausweichmöglichkeiten – wie beispielsweise ein alternatives Verfahren in Papierform – bereitgestellt werden. Im Konzept der Hartz-Kommission wurde noch von einer Einwilligungslösung ausgegangen: Der Arbeitgeber sollte „mit Einverständnis des Arbeitnehmers" die Bescheinigungen bei einem Dritten hinterlegen.[1415] Von einem derartigen Freiwilligkeitselement ist in den Plänen der Bundesregierung nicht mehr die Rede. Dahinter dürfte der richtige Gedanke stehen, dass sich der aufwendige Aufbau der benötigten Infrastruktur finanziell nur dann auszahlt, wenn sowohl Arbeitgeber wie Arbeitnehmer gesetzlich zur Teilnahme verpflichtet werden. Dieser Ansatz verfolgt ein legitimes staatliches Anliegen. Wenn der Zweck des JobCard-Verfahrens nur mit einer solchen Pflicht erreicht werden kann, so muss der Staat keine Alternativverfahren bereitstellen. Allerdings trifft ihn die Verpflichtung zu einer datenschutzgerechten und nutzerfreundlichen Ausgestaltung des Gesamtprozesses. Das beschriebene Verfahren wird die Antragsteller nicht über Gebühr belasten, zumal bei Bedienungsproblemen die Mitarbeiter der Arbeitsagenturen Unterstützung leisten können.

Verfassungsrechtlich bedenklich wäre es allerdings, die Kosten für die Signaturkarte ausschließlich den Arbeitslosen aufzuerlegen.[1416] Das JobCard-Verfahren bewirkt Effizienzgewinne in der Arbeitslosenverwaltung und bei den Arbeitgebern. Während erstere aufgrund der paritätischen Beitragsfinanzierung zumindest hälftig den Arbeitnehmern zugute kommen, ist dies bei letzteren nicht der Fall. Der Vorteil der Arbeitnehmer beschränkt sich jenseits einer möglichen Beitragssenkung im Wesentlichen auf eine erleichterte und beschleunigte Leistungsauszahlung. Dies stellt indes einen weitgehend immateriellen Vorteil dar.

1413 Das Starterpaket der Signtrust (Signaturkarte, Kartenleser und Software in der Minimalversion) kostete bspw. im Mai 2005 103,24 Euro; in den Folgejahren betrug die Gebühr jeweils 45,24 Euro.

1414 Die genaue Verbreitungszahl ist für die erste Phase der Einführung des JobCard-Verfahrens schwer abzuschätzen. Die Zahl der Versicherten beträgt ca. 35 Mio. Von diesen benötigen aber nur diejenigen eine Signaturkarte, die auch tatsächlich Anträge auf Leistung stellen.

1415 *Kommission zum Abbau der Arbeitslosigkeit und zur Umstrukturierung der Bundesanstalt für Arbeit* 2002, 27, 130.

1416 *Hornung/Roßnagel*, K&R 2004, 263, 265; s.a. *Tschoepe*, c't 13/2004, 49.

Es sind deshalb Finanzierungsmodelle zu entwickeln, die die Kosten nicht einseitig den Antragstellern in der Arbeitslosenversicherung auferlegen.[1417] Wirtschaftliche Vorteile haben zunächst nur die Arbeitgeber und die Arbeitsverwaltung. Zumindest für die erste Kartengeneration würden viele Beschäftigte zu einer Investition in eine Signaturkarte verpflichtet werden, mangels Internetanschluss oder Interesse an Electronic Commerce und Electronic Government jedoch keine unmittelbaren wirtschaftlichen Vorteile erlangen. Daher sollten die Arbeitgeber verpflichtet werden, den Erwerb der Signaturkarten durch ihre Arbeitnehmer (etwa zur Hälfte) mitzufinanzieren.

4.2.4.3 Fragen der Datenspeicherung und der Zugriffsbefugnisse

Das JobCard-Verfahren ist zunächst unter dem Gesichtpunkt der grundsätzlich unzulässigen Vorratsdatenspeicherung[1418] als problematisch zu bewerten. Gespeichert werden die Beschäftigungs- und Verdienstdaten aller Versicherten. Ein großer Anteil der Betroffenen wird jedoch nie arbeitslos. Ihre Daten werden im Datenspeicher an sich nicht benötigt. Andere Betroffene werden vielleicht erst in zehn oder zwanzig Jahren arbeitslos. Hier werden in der Anfangszeit Daten gespeichert, die zum Zeitpunkt der Anspruchsberechnung nicht benötigt werden. Allein von der Notwendigkeit der Datenverarbeitung für die Leistungserbringung her betrachtet, stellt sich das geplante System in weiten Teilen als eine nicht erforderliche Vorratsdatenspeicherung dar. Akzeptiert man jedoch das gesetzgeberische Ziel, alle Beteiligte zu entlasten und die Datenerhebung und -verarbeitung zu effektivieren, ist die geplante Verarbeitung der Daten notwendig und deshalb – bei Einrichtung entsprechender Schutzmaßnahmen – zulässig.

Die Speicherung der Daten soll an einer zentralen Stelle, nicht etwa dezentral bei den Trägern der Rentenversicherung erfolgen. Wie bereits erläutert, stellt die zentrale Form der Datenhaltung einen stärkeren Grundrechtseingriff dar, auf den nach Möglichkeit zu verzichten ist.[1419] Eine dezentrale, nicht vernetzte Datenhaltung würde jedoch die Zielsetzungen des geplanten Systems nicht erfüllen können. War der Antragsteller im Bemessungszeitraum in mehreren Arbeitsverhältnissen in den Zuständigkeitsbereichen mehrerer Arbeitsagenturen beschäftigt, muss die zuständige Agentur auf alle erforderlichen Daten zugreifen können. Auch ist es erforderlich, die Daten kurzfristig der zentralen Datenhaltung zur Verfügung zu stellen, da andernfalls – insbesondere bei kurzen Beschäftigungsverhältnissen und kurzfristigen Kündigungen – der Beschleunigungseffekt nicht eintreten kann. Eine dezentrale Variante mit zentralem Directory-System wäre erwägenswert, würde die Risiken aber nur geringfügig verringern.

Nimmt der Gesetzgeber zur Effektivitätssteigerung eine Erhöhung der datenschutzrechtlichen Risiken in Kauf, muss er allerdings zusätzliche Schutzvorkehrungen treffen und dabei die Grundsätze der informationellen Gewaltenteilung und der Erforderlichkeit des Zugriffs durch verlässliche Mechanismen umsetzen.[1420] Die sicherste Form der Speicherung wäre eine Ende-zu-Ende-Verschlüsselung unter Verwendung des öffentlichen Schlüssels der Signaturkarten der Beschäftigten. In diesem Fall würde jeder Zugriff bei der Übermittlung und in der zentralen Speicherstelle unterbunden. Die technische Realisierbarkeit eines solchen Systems ist allerdings derzeit unklar.[1421] Jedenfalls würde es eine suk-

1417 *Hornung/Roßnagel*, K&R 2004, 263, 266.
1418 S.o. 4.2.1.2.2.
1419 S.o. 4.2.2.4.3 und 4.2.3.3.
1420 Vgl. zu den entsprechenden staatlichen Schutzpflichten oben 4.2.1.2.6.
1421 Zu den Problemen s.u. 6.4. Der Arbeitskreis Technik der Datenschutzbeauftragten hat hierzu einen Vorschlag zur Beauftragung eines Gutachtens erarbeitet, s. *AKT*, DuD 2005, 29 ff. (s.a. *ULD* 2005,

zessive Ausgabe qualifizierter Signaturkarte zunächst nur an die Antragsteller der Arbeitslosenversicherung unmöglich machen. Voraussetzung wäre vielmehr, dass bereits beim Start alle versicherten Arbeitnehmer über eine Karte verfügen; dies erscheint wenig realistisch.

Der Datenabruf ist auf die jeweils zuständigen Mitarbeiter der Arbeitsagentur zu beschränken. Hierzu kann die Verwendung von Signaturen des Mitarbeiters und des Antragstellers ein tauglicher Ansatz sein. Dies würde auch ein effektives Protokollierungsverfahren in der Zentralen Speicherstelle ermöglichen, mit dem missbräuchliche Abrufe erkannt werden könnten.

Weiterhin muss sichergestellt sein, dass nur die Daten gespeichert sind, die für die Bearbeitung eines Antrags benötigt werden. Für die Anspruchsberechnung sind im Regelfall die Daten über die versicherungspflichtigen Beschäftigungsverhältnisse der letzten 36 Monate und für die Höhe des Arbeitslosengeldes die Verdienstdaten der letzten 52 Wochen zu berücksichtigen. In Sonderfällen sind auch Daten für weiter zurückliegende Zeiträume erforderlich. Gleiches gilt für die Dauer der Fristen, während derer die Bundesagentur Leistungen noch zurückfordern kann und deshalb über eine Dokumentation verfügen muss. Letzteres begründet allerdings nicht generell die Notwendigkeit einer längeren Aufbewahrung,[1422] sondern nur in den Fällen, in denen tatsächlich eine Leistung erbracht wurde. Für die Mehrzahl der Beschäftigten sind die Daten dagegen immer dann zu löschen, wenn sie für eine hypothetische Anspruchsberechnung zum jeweiligen Zeitpunkt nicht mehr benötigt würden.[1423] Sonderfälle können sich bei laufenden Gerichts- oder Verwaltungsverfahren ergeben.

Für die zentrale Speicherung ist daher ein differenziertes Konzept zur Löschung der jeweils nicht mehr erforderlichen personenbezogenen Daten zu entwickeln. Weiterhin ist die Integrität, Authentizität und jederzeitige Verfügbarkeit der Daten sicherzustellen. Schließlich sind die Daten während ihrer Speicherung, vor allem aber bei ihrer Übertragung zu und von dem zentralen Speicher verlässlich gegen Kenntnisnahme Unberechtigter zu schützen.

Das JobCard-Verfahren verwendet zunächst die Sozialversicherungsnummer als Ordnungskriterium, allerdings nur innerhalb der Zentralen Speicherstelle.[1424] Damit ist im regulären Betrieb keine Verwendung als allgemeines Personenkennzeichen möglich. Allerdings verbleibt das Risiko eines internen Missbrauchs durch Beschäftigte, insbesondere wenn diese über Administratorrechte verfügen. Dieses Problem kann nicht technisch gelöst, sondern nur durch eine effektive Datenschutzkontrolle und die Abschreckung durch entsprechende Straftatbestände für den Datenmissbrauch vermindert werden.

Fraglich ist des Weiteren, wie lange den Mitarbeitern der Arbeitsagentur der Zugriff zu ermöglichen ist. Zum Zeitpunkt der Antragstellung hat der letzte Arbeitgeber des Arbeitslosen möglicherweise noch nicht alle Daten an die Speicherstelle übermittelt. Auch werden andere Einnahmen, insbesondere Provisionen, bisweilen erst später ermittelt werden können. Um hier eine Aktualisierung des Anspruchsumfangs ohne erneutes Erscheinen des Arbeitslosen zu ermöglichen, soll die Zugriffsberechtigung nach den Konzepten nicht nur für einen einmaligen Vorgang, sondern auch für die Zukunft gelten. Hier ist zumindest eine zeitliche Obergrenze für den Zugriff zu bestimmen, nach der der Arbeitslose eine neue Signatur vornehmen muss. Nach den Grundsätzen der Zweckbindung und Erforderlichkeit

---

16). Die Bereitschaft des zuständigen Ministeriums für Wirtschaft und Arbeit zur Auftragsvergabe scheint aber derzeit gering zu sein.

1422 So aber *Ernestus*, DuD 2004, 404, 407.

1423 S. *Hornung/Roßnagel*, K&R 2004, 263, 268.

1424 S.a. *Der Bundesbeauftragte für den Datenschutz* 2005, 41 f.

ist ein Zugriff des Mitarbeiters außerdem dann zu unterbinden, wenn der Arbeitslose eine neue Beschäftigung aufnimmt. Hierzu könnte eine Möglichkeit für diesen eingerichtet werden, der Zentralen Speicherstelle mitzuteilen, dass eine bestimmte Einverständniserklärung in Zukunft nicht mehr gültig sein soll.

4.3 Zulässigkeit nach einfachgesetzlichem Datenschutzrecht

4.3.1 Datenschutzbestimmungen des Signaturrechts

Wenn auf Chipkartenausweisen Verfahren zur Erstellung elektronischer Signaturen ablaufen, sind spezialgesetzliche Datenschutzvorschriften des Signaturrechts einschlägig.[1425] Diese gehen dem allgemeinen Datenschutzrecht vor. Dagegen enthält das Signaturrecht keine Bestimmungen für Daten, die für Verfahren der elektronischen Authentisierung und Verschlüsselung auf derselben Karte angeboten werden. Hierfür findet das Bundesdatenschutzgesetz (insbesondere § 28 Abs. 1 BDSG) Anwendung.

Für Signaturverfahren enthält das Signaturgesetz Erlaubnistatbestände in den §§ 5, 7, 8, 10 und 13 SigG. Diese richten sich an Vorgänge, die in jedem Zertifizierungsprozess nach dem Signaturgesetz ablaufen, also unabhängig von der Verwendung von Chipkartenausweisen. Sie werden deshalb nur überblicksartig behandelt.[1426] § 5 SigG regelt die Vergabe und Abrufbarkeit qualifizierter Zertifikate einschließlich der Verwendung von Attributen und Pseudonymen. § 7 SigG bestimmt enumerativ diejenigen Daten, die in einem qualifizierten Zertifikat enthalten sein müssen. Die Sperrmöglichkeit nach § 8 SigG dient neben dem Schutz des Rechtsverkehrs auch dem Schutz der Daten des Signaturschlüssel-Inhabers. Der Zertifizierungsdiensteanbieter unterliegt besonderen Datensicherungspflichten, deren Umsetzung er nach § 10 Abs. 1 SigG zu dokumentieren hat. § 10 Abs. 2 SigG gibt dem Signaturschlüssel-Inhaber ein Einsichtsrecht in die ihn betreffenden Daten und Verfahrensschritte. In § 13 SigG sind für den Fall der Einstellung der Tätigkeit des Zertifizierungsdiensteanbieters Übermittlungsmöglichkeiten an einen übernehmenden Anbieter beziehungsweise die zuständige Regulierungsbehörde für Telekommunikation und Post geregelt.

Weitere besondere Anforderungen enthält § 14 SigG. Während sich § 14 Abs. 1 und 2 SigG nur an Zertifizierungsdiensteanbieter nach § 2 Nr. 8 SigG richtet, ordnet § 14 Abs. 3 SigG die entsprechende Anwendung der Vorschrift auf Anbieter nicht qualifizierter Zertifikate an. Nach § 14 Abs. 1 Satz 1 SigG sind die Daten für das Erbringen von Zertifizierungsdiensten ausschließlich beim Betroffenen selbst zu erheben und dürfen nicht von dritten Stellen bezogen werden. Durch diese Transparenzregel wird der allgemeine Grundsatz der Direkterhebung in § 4 Abs. 2 BDSG insoweit verschärft, als die dort vorgesehenen Ausnahmen[1427] im Signaturverfahren nicht gelten. Auch die Einwilligung Dritter oder die Bestätigung der Inhalte des Attributs (§ 5 Abs. 2 SigG) ist vom Antragsteller vorzulegen und nicht direkt von der bestätigenden Stelle anzufordern.[1428] Eine Datenerhebung bei

1425 Zu den übrigen Anforderungen des Signaturrechts s.u. 5.

1426 Vgl. ausführlich Roßnagel-*Roßnagel*, Kap. 7.7; RMD-*ders*., § 14 SigG Rn. 1 ff.; s.a. Manssen-*Skrobotz*, § 14 SigG Rn. 4 ff.

1427 Bestimmung durch Rechtsvorschrift, Erforderlichkeit aufgrund einer spezifischen Verwaltungsaufgabe oder Geschäftszwecks und unverhältnismäßiger Aufwand. Es dürfen außerdem keine überwiegenden schutzwürdigen Interessen des Betroffenen vorliegen; s. näher Simitis-*Sokol*, § 4 Rn. 30 ff.

1428 Roßnagel-*Roßnagel*, Kap. 7.7, Rn. 42; RMD-*ders*., § 14 SigG Rn. 54.

Dritten ist nach § 14 Abs. 1 Satz 2 SigG nur mit ausdrücklicher Einwilligung des Betroffenen zulässig.[1429]

Der Umfang der erhobenen Daten muss sich nach § 14 Abs. 1 Satz 1 SigG auf das für die Zwecke eines qualifizierten Zertifikats Erforderliche beschränken.[1430] Allerdings dürfen nicht nur die Daten erhoben werden, die im engeren Sinn für den Inhalt des Zertifikats nach § 7 Abs. 1 SigG erforderlich sind, sondern auch solche, die der Zertifizierungsdiensteanbieter zur Erbringung der Pflichtdienstleistungen nach dem Signaturgesetz benötigt. Darunter fallen Daten, deren Erhebung, Verarbeitung und Nutzung von den Vorschriften des Signaturgesetzes für die Registrierung, Schlüsselerzeugung, Personalisierung, Übergabe, Verzeichnis- und Sperrdienste sowie die Dokumentation vorausgesetzt werden.[1431] Die in § 14 Abs. 1 Satz 1 SigG bestimmte Beschränkung auf die Zwecke eines qualifizierten Zertifikats kann nach § 14 Abs. 1 Satz 3 SigG nur dann geändert werden, wenn das Signaturgesetz selbst dies erlaubt oder der Betroffene eingewilligt hat. Andere Rechtsnormen – wie insbesondere § 28 BDSG – finden damit keine Anwendung.[1432]

Eine zulässige Zweckänderung ist in § 14 Abs. 2 SigG enthalten. Danach hat der Zertifizierungsdiensteanbieter die Daten über die Identität eines Signaturschlüssel-Inhabers zu übermitteln, soweit dies für die Verfolgung von Straftaten oder Ordnungswidrigkeiten, zur Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung oder für die Erfüllung der gesetzlichen Aufgaben der Verfassungsschutzbehörden des Bundes und der Länder, des Bundesnachrichtendienstes, des Militärischen Abschirmdienstes oder der Finanzbehörden erforderlich ist oder Gerichte dies im Rahmen anhängiger Verfahren nach Maßgabe der hierfür geltenden Bestimmungen anordnen.[1433] Die Auskünfte sind nach § 14 Abs. 2 Satz 2 SigG zu dokumentieren. Die ersuchende Behörde hat den Signaturschlüssel-Inhaber über die Übermittlung der Daten zu unterrichten, sobald dadurch die Wahrnehmung der gesetzlichen Aufgaben nicht mehr beeinträchtigt wird oder wenn das Interesse des Signaturschlüssel-Inhabers an der Unterrichtung überwiegt (§ 14 Abs. 2 Satz 3 SigG).

4.3.2 Anforderungen an die Systemgestaltung: Datenvermeidung und Datensparsamkeit

4.3.2.1 Rechtsnatur von § 3a BDSG

Nach § 3a Satz 1 BDSG haben sich Gestaltung und Auswahl von Datenverarbeitungssystemen an dem Ziel auszurichten, keine oder so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen.[1434] Die Rechtsnatur der Norm ist umstritten. Überwiegend wird vertreten, es handele sich um eine echte Rechtspflicht der verantwortlichen Stelle.[1435] Hierfür spreche insbesondere die imperative Formulierung der Norm. Nach anderer Ansicht enthält § 3a BDSG lediglich eine Zielvorgabe[1436] oder einen

1429 S. dazu noch unten 5.2.2.

1430 Näher *Herchenbach*, K&R 2000, 235, 237 f.; Roßnagel-*Roßnagel*, Kap. 7.7, Rn. 45 ff.

1431 Roßnagel-*Roßnagel*, Kap. 7.7, Rn. 44; RMD-*ders*., § 14 SigG Rn. 57.

1432 S. die amtliche Begründung, BT-Drs. 14/4662, 26; Roßnagel-*Roßnagel*, Kap. 7.7, Rn. 47.

1433 Zur Problematik der Aufdeckungsmöglichkeiten s. Roßnagel-*Roßnagel*, Kap. 7.7, Rn. 116 ff. m.w.N. und die Nachweise in Fn. 1470 (S. 252).

1434 Die Norm wurde im Rahmen der Novelle im Jahre 2001 aufgenommen. Sie hat Vorläufer in den (nach ihrer Einführung aufgehobenen) § 3 Abs. 4 TDDSG 1997 und § 12 Abs. 5 MDStV 1997; zur Gesetzgebungsgeschichte vgl. Simitis-*Bizer*, § 3a Rn. 3 ff.; Roßnagel-*Dix*, Kap. 3.5, Rn. 22 ff.

1435 *Bäumler*, DuD 1999, 258, 260 (zu § 3 Abs. 4 TDDSG); Simitis-*Bizer*, § 3a Rn. 41 (s.a. die gleich lautende Kommentierung zu § 3 Abs. 4 TDDSG 1997: RMD-*Bizer*, § 3 TDDSG 1997 Rn. 56), Roßnagel-*Dix*, Kap. 3.5, Rn. 23 (zu § 3 Abs. 4 TDDSG und § 12 Abs. 5 MDStV).

1436 In diese Richtung *Wuermeling*, DSB 7+8/1997, 6, 8 (zu § 3 Abs. 4 TDDSG 1997).

Programmsatz,[1437] da die Anforderungen der Vorschrift nicht zwangsweise durchgesetzt werden könnten.

An dieser Kritik ist richtig, dass bei einem Verstoß gegen die Norm die vorgenommene Datenverarbeitung nicht unzulässig wird. Auch kann weder die Aufsichtsbehörde Zwangsmaßnahmen ergreifen noch der Betroffene Rechte geltend machen.[1438] Möglich sind lediglich die Identifizierung von Umsetzungsdefiziten und entsprechende Anregungen seitens der Aufsichtsbehörden (§ 38 Abs. 1 Satz 1 BDSG) und Datenschutzbeauftragten (§ 4g Abs. 1 Satz 1 und § 24 Abs. 1 Satz 1 BDSG).[1439] Das ändert jedoch nichts daran, dass § 3a Satz 1 BDSG seinem Wortlaut nach eindeutig eine Pflicht beinhaltet. Zwar wird der imperative Teil der Norm durch den Inhalt des Gebots wieder relativiert, da die Pflicht darin besteht, sich am Ziel der Datenvermeidung und Datensparsamkeit „auszurichten". Gleichzeitig ist aber klar, dass mit diesem unbestimmten Rechtsbegriff keine vollständige Freiheit der zuständigen Stellen hergestellt wird. Ihnen werden Wahlmöglichkeiten eingeräumt, die sich jedoch innerhalb eines „Korridors" bewegen, dessen Grenzen nicht überschritten werden dürfen.[1440] Auch wenn es der Norm im Streitfall wegen der mangelnden Durchsetzbarkeit an Durchschlagskraft mangelt, handelt es sich damit um eine echte Rechtspflicht, die bei der Neukonzeption eines Datenverarbeitungssystems zu beachten ist. Das gilt umso mehr für staatliche Datenverarbeitung, da der Staat sich an den durch ihn selbst in der Norm vorgeschriebenen Zielen messen lassen muss.

4.3.2.2 Anforderungen an Datenverarbeitungssysteme

Die Anforderungen des § 3a BDSG gelten für die Gestaltung und Auswahl von Datenverarbeitungssystemen. Dies sind „Funktionseinheit[en] zur Verarbeitung von Daten".[1441] Darunter fallen sowohl Geräte und Baueinheiten als auch Software. Nicht erforderlich ist, dass die einzelne Funktionseinheit selbständig Daten verarbeiten kann. Es reicht vielmehr aus, dass sie „zur" Verarbeitung dient. Unabhängig von der Frage, ob auf dem jeweiligen Ausweischip selbst Daten verarbeitet werden,[1442] ist dieser damit ein Datenverarbeitungssystem im Sinne von § 3a BDSG. Die Anforderungen der Norm gelten daneben für sämtliche Einheiten des jeweiligen Ausweissystems, da jede einzelne von ihnen der Datenverarbeitung im Gesamtsystem dient. Verpflichtet ist die verantwortliche Stelle nach § 3 Abs. 7 BDSG, nicht aber Hersteller und Anbieter der Verarbeitungssysteme.[1443]

Die Regelung in § 3a BDSG soll bereits bei der Konzeption eines Datenverarbeitungssystems sicherstellen, dass im späteren Betrieb möglichst wenig Daten erhoben, verarbeitet

---

1437 *Gola/Schomerus*, § 3a Rn. 2.

1438 *Gola/Schomerus*, § 3a Rn. 2; kritisch gegenüber der jetzigen Regelung insoweit Roßnagel-*Dix*, Kap. 3.5, Rn. 37; einen Anspruch auf Anonymisierung und Pseudonymisierung fordern *Roßnagel/ Pfitzmann/Garstka* 2001, 178. Zwar kann bei einem Verstoß gegen § 3a BDSG gleichzeitig das in den Zulässigkeitstatbeständen verankerte Erforderlichkeitsprinzip verletzt sein. Dann ist die Datenverwendung jedoch nicht aufgrund von § 3a BDSG, sondern wegen des allgemeinen rechtsstaatlichen Verhältnismäßigkeitsgebots rechtswidrig; zum Verhältnis dieser beiden unten 4.3.2.2.

1439 Simitis-*Bizer*, § 3a Rn. 83. Daneben besteht die Möglichkeit einer faktischen Umsetzung über Marktmechanismen, insbesondere ein Datenschutzaudit, s. ebd., Rn. 30, 85; *Roßnagel*, NVwZ 1998, 1, 4; Roßnagel-*Dix*, Kap. 3.5, Rn. 33; *Scholz* 2003, 207.

1440 Simitis-*Bizer*, § 3a Rn. 41.

1441 Vgl. DIN 44300 Nr. 99; näher Simitis-*Ernestus/Geiger*, § 9 Rn. 90; Simitis-*Bizer*, § 3a Rn. 42. Der Begriff ist weiter als der der Datenverarbeitungsanlage, der sich nur auf die Baueinheiten bezieht.

1442 Diese Frage ist für die Anwendbarkeit des § 6c BDSG relevant; s. dazu unten 4.3.3.2.1.

1443 Simitis-*Bizer*, § 3a Rn. 34; a.A. *Duhr/Naujok/Peter/Seiffert*, DuD 2002, 5, 11; s. de lege ferenda *Roßnagel/Pfitzmann/Garstka* 2001, 143 ff. (Vorschlag einer gesetzlichen Verpflichtung der Entwickler und Hersteller, eine datenschutzgerechte Optimierung der Produkte zu prüfen).

und genutzt werden. Dahinter steht der Gedanke des Systemdatenschutzes.[1444] Danach sind unter Datenschutzgesichtspunkten technische Sicherungsmaßnahmen grundsätzlich rechtlichen Mechanismen vorzuziehen, weil erstere früher wirken und bereits eine Datenerhebung unterdrücken, während letztere lediglich die Verwendung vorhandener Datensammlungen begrenzen und damit leichter zu umgehen sind.[1445] Systemdatenschutz will also Gefährdungen des informationellen Selbstbestimmungsrechts durch eine datenschutzfreundliche Technikgestaltung proaktiv reduzieren, statt lediglich reaktiv Veränderungen der technischen Entwicklung zu begegnen.[1446]

Inhaltlich sind die Anforderungen aus § 3a BDSG allerdings in einem doppelten Sinn unscharf. Zum einen wird kein exaktes Ziel, sondern lediglich ein „Korridor" vorgegeben, innerhalb dessen sich die verantwortliche Stelle rechtmäßiger Weise bewegen kann.[1447] Zum anderen lässt sich aus der Norm kein konkretes Mittel zur Zielerreichung ableiten.[1448] Art und Weise der Umsetzung bleiben der verantwortlichen Stelle überlassen, die damit nicht nur hinsichtlich der Breite des Ziels, sondern auch hinsichtlich der Art der Umsetzung über einen Spielraum verfügt.

Dennoch muss nach § 3a BDSG für jeden erhobenen Datentyp und jede Komponente des Datenverarbeitungssystems ebenso wie für das Gesamtsystem die Frage beantwortet werden, ob diese zur Erreichung des angestrebten Zwecks erforderlich sind. Dabei ist zu beachten, dass diese Anforderung – trotz inhaltlicher Überschneidungen – nicht mit dem allgemeinen Erforderlichkeitskriterium identisch ist, dem jede Datenverarbeitung genügen muss.[1449] Folgt man der Ansicht, dass § 3a BDSG keine echte Rechtspflicht beinhaltet, so ergibt sich dies daraus, dass das Verhältnismäßigkeitsprinzip ein rechtliches Gebot ist. Der entscheidende Unterschied liegt jedoch darin, dass sich § 3a BDSG als Präferenzregel an die Gestaltung und Auswahl von Datenverarbeitungssystemen richtet, während das Verhältnismäßigkeitsprinzip das Erheben, Verarbeiten und Nutzen personenbezogener Daten auf das für den jeweils gegebenen Erhebungszweck notwendige Maß beschränkt.[1450] Inhaltlich ist das Gestaltungsprinzip der Datenvermeidung und Datensparsamkeit weiter, weil es ein aktives Einwirken auf den Organisationsprozess erfordert und von der verantwortlichen Stelle sogar verlangt, ihre Verarbeitungszwecke im Sinne einer „datensparsamen" Konkretisierung zu überdenken.[1451]

§ 3a Satz 2 BDSG setzt die Grundsätze der Datenvermeidung und -sparsamkeit in Form von Regelbeispielen um und verlangt, nach Möglichkeit von anonymen und pseudonymen Verfahren Gebrauch zu machen. Während beim Anonymisieren die Daten so verändert werden, dass ein Personenbezug nicht oder nicht mehr mit verhältnismäßigem Aufwand

---

1444 S. grundlegend *Podlech* 1982, 451 ff.; näher *Roßnagel* 1993, 241 ff.; *ders.*, DuD 1999, 253, 256; *Simitis* 1996, 35 ff.; Roßnagel-*Dix*, Kap. 3.5, Rn. 1 ff., 19 ff.; vgl. aus technischer Sicht *Pfitzmann*, DuD 1999, 405 ff.; zum europarechtlichen Hintergrund durch die DSRL *AKT*, DuD 1997, 709, 710; Simitis-*Bizer*, § 3a Rn. 32 f.; vgl. aus mehr soziologischer Perspektive *Donos* 1998, 151 ff.

1445 *Roßnagel/Pfitzmann/Garstka* 2001, 35 ff., 184 ff.; s.a. *Bäumler*, RDV 1999, 5; *Bizer* 1999, 28 ff., insbes. 45 ff.; Simitis-*Bizer*, § 3a Rn. 9 ff.; *Hassemer*, DuD 1995, 448 f.; *Simitis*, DuD 2000, 714, 725.

1446 *Roßnagel* 1994, 243; *ders.*, ZRP 1997, 26 ff.; *Bäumler*, DuD 1997, 446, 449; Simitis-*Bizer*, § 3a Rn 9; *Gola/Schomerus*, § 3a Rn. 1, 4; s.a. die Begründung zum Gesetzesentwurf der Bundesregierung zum BDSG 2001 (BT-Drs. 14/4329, S. 33) und zum IuKDG (BT-Drs. 13/7385).

1447 S.o. 4.3.2.1.

1448 Simitis-*Bizer*, § 3a Rn. 36 ff.

1449 *Roßnagel*, NVwZ 1998, 1, 4; *Bäumler*, DuD 1999, 258, 260; *Gola/Schomerus*, § 3a Rn. 5; zur Erforderlichkeit und Verhältnismäßigkeit s.o. 4.2.1.2.1.

1450 Simitis-*Bizer*, § 3a Rn. 2; Roßnagel-*Dix*, Kap. 3.5, Rn. 25; *ULD* 2000, § 4 Rn. 3; unzutreffend *Meier* 2003, 49, wonach das Prinzip der Datensparsamkeit die gesetzlichen Erlaubnistatbestände zur Datenverwendung einschränken soll.

1451 *Roßnagel/Pfitzmann/Garstka* 2001, 101 f.

hergestellt werden kann (§ 3 Abs. 6 BDSG), erfolgt beim Pseudonymisieren ein Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen (§ 3 Abs. 6a BDSG).[1452] Der Einsatz pseudonymer Verfahren ist vor allem im Geschäftsleben von Vorteil und stellt dort einen Kompromiss zwischen der notwendigen Identifizierung des Geschäftspartners und dessen Wunsch nach Anonymität dar.[1453] Die pseudonymisierende Stelle kann den Betroffenen nach wie vor identifizieren, dieser bleibt Dritten gegenüber jedoch anonym, sofern die Voraussetzungen des Aufdeckungsfalls (beispielsweise die Nichterfüllung einer vertraglichen Leistungspflicht) nicht erfüllt sind. Pseudonymisierung stellt damit zwar keine absolute, gegebenenfalls jedoch eine relative Anonymität her.[1454]

Die in § 3a BDSG enthaltenen Anforderungen stehen allerdings unter den Vorbehalten der Verhältnismäßigkeit und technischen Möglichkeit. Das wird in § 3a Satz 2 BDSG ausdrücklich angeordnet,[1455] gilt der Sache nach aber auch für Satz 1 der Vorschrift.[1456] Ob diese Kriterien erfüllt sind, muss für den jeweiligen Ausweistyp nach den einzelnen Applikationen entschieden werden.

4.3.2.3 Umsetzung bei einzelnen Ausweisen

Bei der Anwendung auf einzelne Ausweise kann typisierend zwischen den auf der Karte selbst (in visueller oder elektronischer Form) und mit ihrer Hilfe in der Peripherie gespeicherten Daten unterschieden werden.

Die Anforderungen an den Umgang mit Daten auf dem Ausweis selbst sollen am Beispiel des digitalen Personalausweises verdeutlicht werden. Auch im Rahmen seiner Identifizierungsfunktion dürfen nur so wenige Daten wie möglich erhoben, verarbeitet und genutzt werden. Ein gewisses Mindestmaß an Identifikationsdaten ist jedoch unabdingbar, weil sonst die Funktionalität beeinträchtigt würde. Erst durch die Kombination mehrer Merkmale werden eine hinreichende Sicherheit der Identifikation in unterschiedlichen Kontrollsituationen und eine Verringerung der Gefahr von Identitätsfälschungen erreicht. Bei der Auswahl der gespeicherten Merkmale nach Art und Zahl muss man den staatlichen Stellen überdies einen Einschätzungsspielraum zubilligen. Unter diesen Gesichtspunkten ist die Speicherung und Verwendung der Daten Ausweisnummer, Name, Vorname, Geburtstag, Geburtsort, Staatsangehörigkeit, Ablaufdatum, Unterschrift, Photo, Adresse, Größe und Augenfarbe auf dem bisherigen Ausweismodell nicht zu beanstanden. Gleiches gilt auch für die visuelle und elektronische Speicherung der genannten Daten auf dem digitalen Personalausweis. Die Angemessenheit der bislang gespeicherten Daten zeigt sich unter anderem auch daran, dass sich eine vergleichbare Auswahl auch auf ausländischen Identitätsdokumenten befindet.[1457]

1452 Zu den Begriffen vgl. oben 4.1.2.1.

1453 *Roßnagel*, DuD 1999, 253, 255; *ders.* 2003, Rn. 62; *Roßnagel/Pfitzmann/Garstka* 2001, 104; ausführlich *Scholz* 2003, 188 ff., 213 ff.

1454 *Gola/Schomerus*, § 3a Rn. 10.

1455 Dazu Simitis-*Bizer*, § 3a Rn. 75 ff.; *Gola/Schomerus*, § 3a Rn. 8. Problematisch ist unter Verhältnismäßigkeitsgesichtspunkten v.a. die Abwägung zwischen den (regelmäßig finanziellen) Aufwendungen der zuständigen Stelle und den (regelmäßig immateriellen) Vorteilen für das Recht auf informationelle Selbstbestimmung des Betroffenen.

1456 *Gola/Schomerus*, § 3a Rn. 7.

1457 S.o. 3. Gleichzeitig ist die Einschätzungsprärogative des Staates jedoch nicht schrankenlos. Eine Grenze ergibt sich etwa dadurch, dass die gespeicherten Daten zur Erreichung des Identifikationsziels geeignet sein müssen. Das ist nicht mehr gegeben, wenn auf dem Ausweis – wie in Macao – Daten über den Familienstand aufgenommen werden. Diese müssen dann unter anderen Gesichtspunkten gerechtfertigt werden.

Besondere Probleme entstehen bei der Verwendung biometrischer Merkmale.[1458] Den Zielen der Datenvermeidung und Datensparsamkeit kann sich der Staat unter anderem durch einen Verzicht auf die zentrale Merkmalsspeicherung, die Verwendung von Templates anstelle von Volldaten und den Einsatz von abgeschotteten Terminals zum Matching nähern.[1459] Datensparsam ist auch die Wahl eines Matching-Verfahrens, welches die zum Abgleich erhobenen Rohdaten unmittelbar danach wieder löscht. Verfahren mit einem Sensor auf der Karte gelangen schließlich sogar in den Bereich der Datenvermeidung, da hier keinerlei Daten außerhalb des Einflussbereiches des Ausweisinhabers entstehen.

Die Verwendung anonymer und pseudonymer Verfahren ist bei der Ausweisfunktion im hoheitlichen Bereich undurchführbar, weil dadurch der angestrebte Identifikationsvorgang unmöglich gemacht würde. Soweit ein Einsatz der biometrischen Merkmale jedoch auch im privaten Bereich zugelassen wird,[1460] ergeben sich Anwendungsmöglichkeiten. So können Einlasskontrollsysteme in der Regel darauf verzichten, die Identität der Nutzer festzustellen. Deshalb sind anonyme Verfahren einsetzbar.[1461] Die Entwicklung und Anwendung pseudonymer Applikationen im privaten Umfeld würde außerdem durch eine Verwendung von Templates beim digitalen Personalausweis gefördert, weil diese nach Entfernung von Identifizierungsdaten zumindest dann ein Pseudonym darstellen, wenn eine Rückwärtskonstruktion ausgeschlossen ist.[1462]

Im System der Gesundheitskarte werden mit ihrer Hilfe eine Reihe von Daten in Peripheriesystemen gespeichert und von dort wieder abgerufen. Eine Datenvermeidung ist nicht möglich, weil die verwendeten Daten für die ärztliche Behandlung erforderlich sind. Das Verfahren ist jedoch am Grundsatz der Datensparsamkeit auszurichten. Soweit es ohne eine Beeinträchtigung der Funktionalität möglich ist, sind die Daten auf der Gesundheitskarte selbst zu speichern, bei einer Ablage in der Peripherie ist nach Möglichkeit auf einen Personenbezug zu verzichten. Hierzu bietet sich der Einsatz von Pseudonymen an.[1463] Mit Hilfe der Karte können Einwegpseudonyme erzeugt werden, unter denen Daten über Geschäftsvorfälle und Dokumentationen abgespeichert werden. Auf diese Pseudonyme kann sodann mittels Pointern auf der Karte verwiesen werden, aus denen jedoch nicht umgekehrt auf die Identität des Versicherten zurückgeschlossen werden kann.[1464] Schließlich dient auch der Verzicht auf zentrale Datenhaltungen in der Peripherie der Datensparsamkeit.

Eine Anonymisierung von Daten ist demgegenüber nicht möglich, solange sie für eine spätere Behandlung dem Betroffenen wieder zugeordnet werden müssen. Anonyme Daten können jedoch insbesondere in der medizinischen Forschung und Qualitätssicherung eingesetzt werden, weil dort in der Regel kein Personenbezug benötigt wird.[1465] Das Daten-

---

1458 Vgl. *Roßnagel/Hornung*, in: Reichl/Roßnagel/Müller 2005, 130 f.

1459 Es besteht weitgehende Inhaltsgleichheit mit der Frage der Verhältnismäßigkeit der jeweiligen Verfahren; vgl. insoweit ausführlich oben 4.2.2.4.2, 4.2.2.4.3 und 4.2.2.4.4.

1460 Nach geltendem Recht bestehen erhebliche Einschränkungen, s.o. 4.2.2.5.

1461 *Gundermann/Köhntopp*, DuD 1999, 143, 147; s.a. *Donnerhacke*, DuD 1999, 151 ff.

1462 *AKT*, DuD 1997, 709, 713; *Albrecht* 2003a, 158; zum Problem der Rückwärtskonstruktion s.o. 4.2.2.4.2; dieses hat auch Auswirkungen auf den Personenbezug von Templates, s.o. 4.1.2.2.2.2.

1463 Dieser erlangt im Gesundheitswesen besondere Relevanz, s. *Menzel/Schläger*, DuD 1999, 70, 74 f.

1464 S.a. unten 6.3.2 und *BITKOM/VDAP/VHitG/ZVEI* 2003, 27 ff.; *Bultmann/Wellbrock/Biermann/Engels/Ernestus/Höhn/Wehrmann/Schurig* 2002, 29 ff.

1465 *Bäumler*, MedR 1998, 400, 405; *Beier* 1979, 107; *Lilie* 1980, 103 f.; zum Verhältnis von medizinischer Forschung und Datenschutz *Kersten*, CR 1989, 1020, 1025 f.; *Dierks* 1993, 66 ff.; *Weichert*, MedR 1996, 258 ff.; *Deutsch* 1999, Rn. 362 m.w.N.; *Klöcker/Meister* 2001, 160 ff.; *Meier* 2003, 263 ff.; allgemeiner und ausführlich *Bizer* 1992; s.a. Roßnagel-*Gerling*, Kap. 7.10, Rn. 1 ff.; zur technischen Umsetzung der Anonymisierung s. *ATG/GVG* 2004a, 24 ff., 48 ff.

schutzrecht ist dann nicht mehr anwendbar. Das entspricht auch § 15 Abs. 2 MBO-Ä 2004, wonach der Schweigepflicht unterliegende Tatsachen und Befunde zum Zwecke der wissenschaftlichen Forschung und Lehre außer bei ausdrücklicher Zustimmung des Patienten auch dann offenbart werden dürfen, wenn seine Anonymität gesichert ist.[1466]

Werden dagegen zu Forschungszwecken Langzeitstudien erstellt, so muss zumindest über ein dauerhaftes Pseudonym eine Zusammenführung der erhobenen Daten ermöglicht werden.[1467] Hierzu wurde durch das GKV-Modernisierungsgesetz eine „Arbeitsgemeinschaft für Aufgaben der Datentransparenz" eingerichtet (§§ 303a bis 303f SGB V), die von den Krankenkassen und den Mitgliedern der Kassenärztlichen Bundesvereinigung Daten erhält, diese pseudonymisiert und zu Zwecken der Strukturanalyse des Gesundheitswesens aufbereitet.[1468]

Bei der Signaturfunktion der jeweiligen Ausweise ist eine Verwendung anonymer Verfahren wegen der Rechtsverbindlichkeit der signierten Erklärungen nicht möglich und auch im Signaturgesetz nicht vorgesehen. Rechtlich betrachtet, ist die elektronische Signatur ein Funktionsäquivalent zur eigenhändigen Unterschrift.[1469] Soll sie ihre Funktion der Sicherung von Integrität und Authentizität einer Erklärung im Rechtsverkehr erfüllen, so muss zumindest im Streitfall die Feststellung der Identität des Signierenden möglich sein. Aus demselben Grund können allerdings Pseudonyme eingesetzt werden, sofern funktionierende Verfahren zur Aufdeckung existieren.[1470] Diesen Ansatz verfolgt auch die bestehende Regelung der elektronischen Signatur, da in §§ 5 Abs. 3, 7 Abs. 1 Nr. 1, 14 Abs. 2 SigG und § 8 Abs. 2 Nr. 2 SigV den Einsatz von Pseudonymen vorgesehen ist.[1471] Ebenso erfasst die Ausgestaltung der elektronischen Form in § 126a BGB das Handeln mittels eines auf ein Pseudonym ausgestellten Zertifikats.[1472] Das ist nach dem Wortlaut der Norm, der ein Hinzufügen des Namens verlang, zwar zweifelhaft, entspricht jedoch der normalen Schriftform, bei der eine Verwendung eines tatsächlich geführten Pseudonyms zur Unterschrift ausreichend ist, wenn die als Aussteller in Betracht kommende Person ohne Zweifel feststeht.[1473]

Für zukünftige weitere Anwendungen muss jeweils im Einzelfall entschieden werden, ob der Einsatz anonymer und pseudonymer Verfahren möglich und sinnvoll ist. Dabei

---

1466 Dazu Roßnagel-*Schirmer*, Kap. 7.12, Rn. 74.

1467 Roßnagel-*Gerling*, Kap. 7.10, Rn. 26 f.; s.a. *BITKOM/VDAP/VHitG/ZVEI* 2003, 62.

1468 S. näher *Goldschmidt/Goetz/Hornung*, Management-Handbuch Krankenhaus 2004, Rn. 22 ff. Der Mechanismus dient nach § 303f Abs. 2 Satz 2 SGB V der Wahrnehmung von Steuerungsaufgaben durch die Kollektivvertragspartner, der Verbesserung der Qualität der Versorgung, der Planung von Leistungsressourcen, der Erstellung von Analysen zum Erkennen von Fehlentwicklungen und Ansatzpunkten für Reformen (Längsschnitte, Behandlungsabläufe, Versorgungsgeschehen), der Unterstützung politischer Entscheidungsprozesse zur Weiterentwicklung der gesetzlichen Krankenversicherung und der Analyse und Entwicklung von sektorenübergreifenden Versorgungsformen.

1469 RMD-*Roßnagel*, § 2 SigG 1997 Rn. 25; s. näher unten 5.1.1.

1470 Hier bestehen noch ungelöste Fragen. Zwar gibt es nunmehr in § 14 Abs. 2 Satz 1 SigG – anders als in § 12 Abs. 2 Satz 1 SigG 1997 – eine Aufdeckungspflicht auch den Gerichten gegenüber. Dennoch bleibt bei einer Rechtsdurchsetzung Privater das Problem einer fehlenden ladungsfähigen Anschrift für den Klagenden bestehen, da dieser das Pseudonym nicht zuordnen kann und auch keinen selbständigen Aufdeckungsanspruch gegen den Zertifizierungsdiensteanbieter hat; s. näher Roßnagel-*Roßnagel*, Kap. 7.7, Rn. 120; *ders.*, NJW 2001, 1817, 1821; *Roßnagel/Pfitzmann/Garstka* 2001, 152; *Fuhrmann* 2001, 241 f.; *Hopp/Grünvogel*, DuD 2002, 79, 80 f. Auf die Probleme des Aufdeckungsverfahrens wurde bereits bei den Beratungen zum SigG 1997 aufmerksam gemacht, s. RMD-*Roßnagel*, Einl. SigG Rn. 83.

1471 S. näher RMD-*Roßnagel*, § 5 SigG Rn. 39 ff.; § 7 SigG Rn. 31 ff.

1472 *Bröhl/Tettenborn* 2001, 193; tlw. einschränkend Roßnagel-*Roßnagel*, Kap. 7.7, Rn. 148; *ders.*, NJW 2001, 1817, 1825.

1473 BGH, NJW 1996, 997; Palandt-*Heinrichs*, § 126 Rn. 9.

lohnt ein Blick auf die im Ausland entweder angedachten oder bereits umgesetzten Applikationen,[1474] unabhängig von der Frage, ob diese letztlich in Deutschland eingeführt werden. So kann im Rahmen eines Führerscheinsystems weder anonym noch pseudonym gehandelt werden. Denkbar wäre anonymes Handeln aber etwa bei der elektronischen Geldbörse, wenn Bezahlvorgänge unmittelbar, das heißt vergleichbar dem Vorgang bei Barzahlung erfolgen. Wird der Ausweis hingegen zur Verwaltung von Nutzerdaten (etwa in öffentlichen Bibliotheken) verwendet, so kann auf den direkten Personenbezug wiederum nicht verzichtet werden.

4.3.3 Anforderungen an den Einsatz mobiler personenbezogener Speicher- und Verarbeitungsmedien

Seit der Novelle im Jahre 2001 enthält das Bundesdatenschutzgesetz spezifische Anforderungen an „mobile personenbezogene Speicher- und Verarbeitungsmedien".[1475] § 6c Abs. 1 BDSG normiert eine Reihe von Unterrichtungspflichten. Nach § 6c Abs. 2 BDSG müssen die zur Wahrnehmung des datenschutzrechtlichen Auskunftsrechts erforderlichen Geräte und Einrichtungen unentgeltlich bereitgestellt werden. § 6c Abs. 3 BDSG fordert, dass Kommunikationsvorgänge, die auf dem Medium eine Datenverarbeitung auslösen, für den Betroffenen eindeutig erkennbar sein müssen.

Die Regelung ist nicht durch europarechtliche Vorgaben bedingt.[1476] Sie gilt für einige – jedoch nicht alle – Chipkartenausweise. Wird der jeweilige Ausweis durch öffentliche Stellen der Länder ausgegeben und verwendet, so ist § 6c BDSG aufgrund der unterschiedlichen Anforderungen der Landesdatenschutzgesetze nur teilweise anwendbar.

4.3.3.1 Rechtsnatur von § 6c BDSG

§ 6c BDSG ermächtigt nicht etwa zum Auslesen von Daten aus dem Datenträger oder zur Vornahme von Datenverarbeitungen auf diesem.[1477] Die Norm trifft auch keine Entscheidung über die technische Ausgestaltung des Datenträgers oder des Auslese- und Verarbeitungssystems, in das er eingebunden ist. Ihr Zweck ist es vielmehr, durch die Festlegung von Informationspflichten dem datenschutzrechtlichen Transparenzgebot Genüge zu tun.[1478] Dahinter steht der Gedanke, dass wegen der Intransparenz einer Verarbeitung auf mobilen personenbezogenen Speicher- und Verarbeitungsmedien erhöhte datenschutzrechtliche Gefahren für den Betroffenen entstehen.[1479] Wegen des großen Umfangs der Unterrichtungspflichten stellt die Regelung einen ersten Ansatz in Richtung auf eine Infrastrukturaufklärung hin dar.

Fraglich ist, ob § 6c BDSG eine Rechtmäßigkeitsanforderung an die Erhebung und Verarbeitung von Daten mittels des Mediums beinhaltet oder lediglich eine Verpflichtung der

---

1474 S. dazu näher oben 3.

1475 § 6c BDSG wurde erst durch einen Änderungsantrag von SPD und Bündnis90/DIE GRÜNEN im Innenausschuss eingefügt (BT-Drs. 14/5793); eine entsprechende Sondernorm im Bundestag erstmals 1997 vorgeschlagen durch § 32 des Entwurfs eines BDSG von Bündnis 90/DIE GRÜNEN (BT-Drs. 13/9082); zur Gesetzgebungsgeschichte vgl. Simitis-*Bizer*, § 6c Rn. 8 ff.; zur Rechtslage vor der Novelle *Weichert*, DuD 1997, 266 ff.; s. zum Folgenden bereits *Hornung*, DuD 2004, 15 ff.; *Roßnagel/Hornung*, in: Reichl/Roßnagel/Müller 2005, 133 ff.

1476 *Gola/Schomerus*, § 6c Rn. 1.

1477 *Gola/Schomerus*, § 6c Rn. 5.

1478 Simitis-*Bizer*, § 6c Rn. 3; *Gola/Schomerus*, § 6c Rn. 2.

1479 S. die Gesetzesbegründung, BT-Drs. 14/5793, 63. Die Gefahren bestehen v.a. im Bereich der Profilbildung und nehmen zu, je mehr Funktionalitäten auf einer einzigen Karte vereinigt werden.

Stellen, die das Medium ausgeben oder ein automatisiertes Datenverarbeitungsverfahren auf es aufbringen, ändern oder hierzu bereithalten.[1480]

Für ein Rechtmäßigkeitserfordernis spricht, dass mit der abschreckenden Wirkung einer eventuellen Rechtswidrigkeit der Datenverwendung die wirkungsvollste Umsetzung der neuartigen Anforderungen von § 6c BDSG erzielt würde. Hinzu kommt, dass die Norm eine Verfahrensanforderung des öffentlichen Rechts darstellt, deren Nichteinhaltung grundsätzlich zur Rechtswidrigkeit der Maßnahme führt.[1481] Ausnahmen hiervon sind immer ausdrücklich zu regeln.[1482] Schließlich ist die Vorschrift eng mit dem Aufklärungserfordernis nach §§ 4, 4a BDSG verwand. Hier führt ein nicht ordnungsgemäßer Hinweis zur Rechtswidrigkeit der Datenerhebung.[1483] Sowohl die Hinweispflicht nach § 4a Abs. 1 Satz 2 BDSG als auch die Unterrichtungspflicht nach § 6c BDSG zielen darauf ab, dem Betroffenen die Folgen der ihn betreffenden Datenverwendung vor Augen zu führen und ihn damit zu einer bewussten Entscheidung zu veranlassen.[1484] Deshalb könnte man argumentieren, die beiden Normen seien hinsichtlich ihrer Rechtsfolgen gleich zu behandeln.

Auf der anderen Seite weist die Gesetzesbegründung zu § 6c BDSG lediglich darauf hin, die Norm solle Transparenz für mobile Medien erreichen.[1485] Eine Rechtswidrigkeit der Datenerhebung wird nicht erwähnt. Ganz offensichtlich lag es nicht im gesetzgeberischen Willen, einen Verstoß mit den damit verbundenen weitreichenden Sanktionen zu verknüpfen.[1486] Außerdem spricht § 6c Abs. 1 BDSG davon, dass die jeweilige Stelle „unterrichten muss". Schon vom Wortlaut her besteht also ein deutlicher Unterschied zu der Fassung von Normen über die Rechtmäßigkeit der Datenerhebung, in denen es regelmäßig heißt, diese sei „nur zulässig, wenn".[1487] Ein weiteres Argument lässt sich daraus gewinnen, dass in der ersten Stufe der Novellierung des Bundesdatenschutzgesetzes im Jahre 1999 zunächst eine Vorabkontrolle für Chipkarten vorgesehen war.[1488] Diese wurde später aber wieder fallengelassen. Die Existenz von Normen, die zwar Anforderungen an die zuständige Stelle richten, jedoch nicht die Rechtmäßigkeit der Datenverwendung berühren, ist dem Datenschutzrecht auch ansonsten nicht fremd. Ein Beispiel ist etwa die Pflicht zur Verwendung von Pseudonymen.[1489] Insgesamt überwiegen damit die Argumente, in § 6c BDSG kein Rechtmäßigkeitserfordernis an die Erhebung und Verarbeitung der Daten auf dem Medium zu sehen.[1490]

1480 Vgl. zu diesem Aspekt schon *Hornung*, DuD 2004, 15, 18 f.

1481 *Maurer* 2002, § 10 Rn. 2, 9 ff. Das gilt hier, soweit § 6c BDSG öffentliche Stellen verpflichtet.

1482 Vgl. z.B. §§ 214-216 BauGB; s. näher *Dürr* 1998, Rn. 70 ff.; *Brohm* 2002, 317 ff.

1483 Simitis-*Simitis*, § 4a Rn. 73.

1484 S. jedoch zu den Unterschieden unten 4.3.3.2.3.

1485 BT-Drs. 14/5793, 63.

1486 Gespeicherte Daten wären gemäß §§ 20 Abs. 2 Nr. 1, 35 Abs. 2 Nr. 1 BDSG unverzüglich zu löschen. Daneben käme unter den Voraussetzungen der §§ 7, 8 BDSG ein Schadenersatzanspruch in Betracht. Bei einer vorsätzlichen oder fahrlässigen Verletzung der Unterrichtungspflicht müsste der Verantwortliche eine Geldbuße entrichten (§ 43 Abs. 2 Nr. 1 BDSG), bei einer vorsätzlichen Tat, die gegen Entgelt oder in Bereicherungs- oder Schädigungsabsicht vorgenommen wurde, läge eine Straftat nach § 44 Abs. 1 BDSG i.V.m. § 43 Abs. 2 Nr. 1 BDSG vor.

1487 Vgl. etwa §§ 4 Abs. 1, 13 Abs. 1 und Abs. 3, 14 Abs. 1 und 2, 15 Abs. 1, 16 Abs. 1, 28 Abs. 1, 3 und 6, 29 Abs. 1 und 2, 30 Abs. 2 BDSG.

1488 § 4d Abs. 5 Satz 2 des Referentenentwurfs v. 29.6.1999; vgl. Roßnagel-*Weichert*, Kap. 9.5, Rn. 16.

1489 Ist das Verwenden technisch möglich und i.S.v. § 3a Satz 2 BDSG angemessen, so besteht eine Pflicht dazu, derartige Verfahren auch anzubieten, s.o. 4.3.2.2. Wird dem seitens der zuständigen Stelle nicht entsprochen, so führt das aber nicht zur Rechtswidrigkeit der Datenverarbeitung ohne Pseudonym (zu den Folgen einer Verletzung von § 3a BDSG s. Simitis-*Bizer*, § 3a Rn. 83 ff. und oben 4.3.2.1).

1490 Ebenso *Gola/Schomerus*, § 6c Rn. 5; Simitis-*Bizer* § 6c Rn. 11.

Damit ist jedoch die weitere Frage noch nicht beantwortet, ob § 6c Abs. 1 BDSG einen echten, durchsetzungsfähigen Anspruch des Inhabers des Mediums enthält. Dies könnte deshalb zweifelhaft sein, weil die Norm weder in den Abschnitten über die Rechte des Betroffenen (§§ 19-21 und §§ 33-35 BDSG), noch im Rahmen von § 6 BDSG erwähnt wird. Auch die Gesetzesmaterialien sprechen lediglich von Unterrichtungspflichten, nicht jedoch explizit von korrespondierenden Rechten des Betroffenen. Allerdings kann aus der Begründung zumindest ein indirektes Argument für das Vorliegen eines subjektiven Rechtes gewonnen werden. Wenn es dort im Zusammenhang mit § 6c Abs. 1 Nr. 2 BDSG heißt, eine „detaillierte" Begründung könne nicht verlangt werden,[1491] so impliziert dies, dass Anspruch auf eine normale Begründung besteht.

Im Übrigen muss die Frage nach den allgemeinen Regeln über das Vorliegen subjektiver Rechte entschieden werden. Hierbei ist zwischen öffentlichen und nichtöffentlichen Stellen zu differenzieren.

Für die Unterrichtung durch öffentliche Stellen sind die Voraussetzungen des subjektiven öffentlichen Rechts maßgeblich. Nach der Schutznormtheorie liegt ein solches Recht dann vor, wenn der Betroffene vom Geltungsbereich des Gesetzes erfasst wird und die Norm nicht nur im öffentlichen Interesse besteht, sondern – zumindest auch – den Interessen des Betroffenen zu dienen bestimmt ist.[1492] Das ist vor allem bei einem Grundrechtsbezug der Fall. § 6c Abs. 1 BDSG dient dem Schutz des Rechts auf informationelle Selbstbestimmung des Betroffenen, indem es bereits an die Ausgabe des Mediums Unterrichtungspflichten knüpft und damit den Grundrechtsschutz in diesem besonders sensiblen Bereich vorverlegt. Insofern ist der notwendige Subjektbezug gegeben. Aus § 6c Abs. 1 Nr. 3 BDSG lässt sich überdies ableiten, dass ein enger Zusammenhang der Norm mit den Rechten aus §§ 19, 20, 34 und 35 BDSG (Auskunft, Berichtigung, Löschung, Sperrung und Widerspruch) besteht. Die Unterrichtungspflicht wirkt quasi unterstützend in deren Vorfeld. Soll § 6c Abs. 1 BDSG die tatsächliche Wirksamkeit dieser Rechte sichern, so muss die Norm selbst notwendigerweise einen durchsetzungsfähigen Anspruch eröffnen. § 6c Abs. 2 BDSG dient sogar unmittelbar der technischen Realisierung des Auskunftsrechts, während § 6c Abs. 3 BDSG den Grundsatz der Transparenz der Datenverarbeitung umsetzt und dadurch die Undurchschaubarkeit des Prozesses für den Inhaber des Mediums vermindert. Schließlich lässt sich ein Argument für das Bestehen eines subjektiven Rechts aus der Tatsache gewinnen, dass der Verstoß gegen die Verpflichtung aus § 6c BDSG nicht bußgeldbewehrt ist. Da die Verletzung der Norm die Rechtmäßigkeit der Datenverwendung nicht berührt, würde ohne einen Anspruch des Betroffenen jedes Mittel zur Durchsetzung der Regelung abgeschnitten.

Für die Unterrichtungspflicht nichtöffentlicher Stellen gilt auch im vorliegenden Zusammenhang der allgemeine Grundsatz, dass im Verhältnis zwischen Privaten der Rechtspflicht des einen regelmäßig ein Rechtsanspruch des anderen gegenüber steht.[1493] Im Ergebnis enthalten damit alle drei Absätze von § 6c BDSG für den öffentlichen und den nichtöffentlichen Bereich Ansprüche des Betroffenen. Die Inhaber von Chipkartenausweisen können diese gegen die ausgebende und diejenigen Stellen gerichtlich durchsetzen, die automatisierte Verfahren auf das Medium aufbringen, ändern oder hierzu bereithalten.

1491 BT-Drs. 14/5793, 63.

1492 *Maurer* 2002, § 8 Rn. 8; *Schenke* 2004, Rn. 495 ff.

1493 Das liegt daran, dass im Verhältnis zwischen Privaten die Funktion des Rechts darin besteht, Interessen der Bürger auszugleichen und gegeneinander abzugrenzen. Die Pflichten und Beschränkungen des einen bestehen gerade im Interesse des anderen; vgl. *Maurer* 2002, § 8 Rn. 7.

4.3.3.2 Anwendungsbereich

4.3.3.2.1 Mobile personenbezogene Speicher- und Verarbeitungsmedien

Die Pflichten des § 6c BDSG gelten nur für „mobile personenbezogene Speicher- und Verarbeitungsmedien".[1494] Dieser Terminus wird auch von einer Reihe von Landesdatenschutzgesetzen verwendet, die ihn jedoch zum Teil anders definieren als das Bundesdatenschutzgesetz. Für letzteres ergibt sich die maßgebliche Bedeutung des Begriffs aus der Legaldefinition in § 3 Abs. 10 BDSG.

4.3.3.2.1.1 Begriff

Nach § 3 Abs. 10 BDSG ist erforderlich, dass der Datenträger an den Betroffenen ausgegeben wird, auf ihm personenbezogene Daten über die Speicherung hinaus automatisiert verarbeitet werden können und der Betroffene diese Verarbeitung nur durch den Gebrauch des Mediums beeinflussen kann.

Chipkartenausweise werden bestimmungsgemäß an den Inhaber ausgegeben, womit das erste Kriterium erfüllt ist. Problematisch ist jedoch die automatisierte Verarbeitung auf dem Medium. Dieses Kriterium ist nicht in allen Landesdatenschutzgesetzen enthalten. Teilweise lassen diese einen automatisierten Datenaustausch[1495] oder eine automatisierte Verarbeitung „durch" den Datenträger[1496] ausreichen. Auch der Entwurf von Bündnis 90/DIE GRÜNEN aus dem Jahre 1997 sah lediglich die Notwendigkeit einer direkten Kommunikation mit elektronischen Lese- und Schreibgeräten vor.[1497]

Das von § 3 Abs. 10 BDSG und der Mehrzahl der Landesdatenschutzgesetze[1498] verwendete Tatbestandsmerkmal der Verarbeitung durch das Medium selbst ist insofern enger, als reine Speichermedien wie Magnetkarten nicht erfasst sind. Diese entsprechen jedoch durchaus den Definitionen derjenigen Landesdatenschutzgesetze, die einen automatisierten Datenaustausch oder ein Anstoßen von automatisierten Verarbeitungsvorgängen in der Peripherie ausreichen lassen.

Teilweise wird in der Literatur ohne Differenzierung von diesem weiten Begriff ausgegangen, was die Gefahr von Missverständnissen mit sich bringt. Vertreten wird, das entscheidende Wesensmerkmal mobiler personenbezogener Speicher- und Verarbeitungsmedien sei, dass über eine „Schnittstelle...automatisiert personenbezogene oder personenbeziehbare Daten ausgetauscht werden [können]".[1499] Dies geschieht aber auch bei reinen Speichermedien. Zwar ist es richtig, dass mit der Benutzung personenbezogener Chipkarten immer eine automatisierte Verarbeitung nach § 3 Abs. 2 BDSG angestoßen wird.[1500] Daraus kann aber nicht gefolgert werden, jede Chipkarte fiele per se unter § 3 Abs. 10 BDSG, weil diese Norm eine automatisierte Verarbeitung „über die Speicherung hinaus"

1494 S. zum Folgenden *Hornung*, DuD 2004, 15 ff.
1495 § 5b HmbDSG, § 3 Abs. 10 DSG MV.
1496 § 5 Abs. 3 BrDSG.
1497 § 32 Abs. 1 des Entwurfs, BT-Drs. 13/9082, 12.
1498 Wie das BDSG eine Verarbeitung auf dem Medium erfordernd: § 5 Abs. 1 DSG BW, § 4 Abs. 3 Nr. 9 BLnDSG, § 20a Abs. 1 BrDSG, § 8 Abs. 2 HDSG, § 35 Abs. 1 DSG Rh.-Pf., § 3 Abs. 9 SDSG, § 2 Nr. 11 DSG-LSA, § 18 Abs. 1 DSG SH, § 6a NDSG.
1499 So Roßnagel-*Weichert*, Kap. 9.5, Rn. 20.
1500 Roßnagel-*Weichert*, Kap. 9.5, Rn. 22.

verlangt und damit gerade nicht jede automatisierte Verarbeitung im Zusammenhang mit Chipkarten, sondern nur eine solche auf der Karte selbst ausreicht.[1501]

Auf welche Art und Weise die jeweilige Stelle die automatisierte Verarbeitung auf der Karte herbeiführt, ist nicht von Bedeutung. Deshalb ist die Auffassung, wonach Medien entfallen sollen, „die ein Lesegerät eingeführt, oder Chips, die in einem Lesegerät vorbeigeführt werden“[1502] (sic), nicht nur sprachlich unverständlich, sondern auch unzutreffend. Die Möglichkeit, das Medium in ein Lesegeräte einzuführen (kontaktbehafteter Chip) oder an einem solchen vorbeizuführen (kontaktlose Variante) sind zumindest bei Medien ohne eigene Stromversorgung die einzigen Mittel, auf dem Chip eine automatisierte Verarbeitung vorzunehmen. Diese Eigenschaft ist damit nicht nur kein Ausschlusskriterium für die Anwendung von § 3 Abs. 10 BDSG, sondern umgekehrt sogar eine notwendige Bedingung hierfür. Abgesehen davon stellt die Norm nicht auf die Art und Weise der Handhabung des Mediums, sondern auf die Möglichkeit einer automatisierten Verarbeitung (über die Speicherung hinaus) ab.

Unerheblich ist, ob das Medium zum Zeitpunkt seiner Ausgabe bereits ein Verarbeitungsverfahren oder zu verarbeitende Daten enthält.[1503] Besteht die technische Möglichkeit, später ein automatisiertes Verfahren zu installieren, so löst dies bereits bei der Ausgabe die Pflichten des § 6c BDSG aus, soweit die anderen Anforderungen von § 3 Abs. 10 BDSG erfüllt sind.

Mikroprozessorchipkarten sind das Hauptanwendungsbeispiel für „mobile personenbezogene Speicher- und Verarbeitungsmedien“.[1504] Dieser Begriff wurde aber gewählt, weil er für zukünftige technische Entwicklungen offen gehalten werden sollte.[1505] Nach der Gesetzesbegründung soll § 3 Abs. 10 BDSG keine Geräte mit eigener Steuerungseinheit wie Palm, Personal Digital Assistants (PDAs), Handys oder Notebooks erfassen, da hier eine vielfältige Kontrolle durch den Benutzer möglich sei.[1506] Dies ist jedoch nur unter exakt dieser Bedingung zutreffend. Sofern eines dieser Geräte über Soft- oder Hardwarebereiche verfügt, die der Kontrolle des Geräteinhabers entzogen sind und wie eine Chipkarte Daten verarbeiten, ist die Definition des § 3 Abs. 10 BDSG erfüllt.[1507] Reine Speichermedien wie Magnetkarten und Medien, die wie der bisherige Personalausweis optoelektronisch mit einem Scanner ausgelesen werden müssen, fallen schließlich nicht in den Anwendungsbereich.

4.3.3.2.1.2 Anwendung auf Chipkartenausweise

Nach dieser Begriffsbestimmung ist nunmehr zu untersuchen, unter welchen Bedingungen Chipkartenausweise den Anforderungen von § 6c BDSG unterliegen.[1508] Fraglich ist zunächst, ob die Norm auf Ausweise anwendbar ist, die verpflichtend ausgegeben werden. Ausweislich der Gesetzesmaterialien soll sie das datenschutzrechtliche Transparenzgebot dadurch fördern, dass der Betroffene darin unterstützt wird, eine bewusste Entscheidung

1501 Das wird ignoriert von Roßnagel-*Weichert*, Kap. 9.5, der das Problem der Verarbeitung „über die Speicherung hinaus“ vollständig unerwähnt lässt.
1502 *Schaffland/Wiltfang*, § 3 Rn. 108.
1503 So die Gesetzesbegründung, BT-Drs. 14/5793, 60; s.a. *Gola/Schomerus*, § 3 Rn. 58; *Schaffland/Wiltfang*, § 6c Rn. 1.
1504 *Gola/Schomerus*, § 3 Rn. 59.
1505 Roßnagel-*Weichert*, Kap. 9.5, Rn. 1.
1506 BT-Drs. 14/5793, 60; dem folgend Simitis-*Bizer*, § 6c Rn. 2; *Gola/Schomerus*, § 3 Rn. 59; *Schaffland/Wiltfang*, § 3 Rn. 108.
1507 Ebenso Roßnagel-*Weichert*, Kap. 9.5, Rn. 10.
1508 S. bereits *Hornung*, DuD 2004, 15, 16 f.

darüber zu treffen, ob er seine Daten in einem Verfahren unter Einsatz des Mediums bereitstellen will oder nicht.[1509] Das würde bei Chipkartenausweisen denkbare freiwillige Applikationen betreffen. § 6c BDSG ist nach Wortlaut wie Regelungszweck aber auch dann einschlägig, wenn Medien, wie der digitale Personalausweis und die elektronische Gesundheitskarte, zwangsweise ausgegeben werden. Auch in diesem Fall bestehen wegen der nicht unmittelbar nachvollziehbaren Datenverarbeitung auf dem Medium vorgezogene Unterrichtungspflichten.

Da ein mobiles personenbezogenes Speicher- und Verarbeitungsmedium schon dann vorliegt, wenn später ein automatisiertes Verfahren installiert werden kann, ist § 6c BDSG bereits deswegen auf eine Vielzahl von Ausweisen anzuwenden, weil sie die Möglichkeit bieten, weitere Applikationen nachzuladen.[1510] Wenn dies nicht möglich ist, sind die Prozesse auf der Karte daraufhin zu analysieren, ob eine automatisierte Verarbeitung gegeben ist. Im Folgenden werden Chipkarten in biometrischen Identifikationssystemen (wie der digitale Personalausweis), die Datenverwendung bei der elektronischen Gesundheitskarte und Signaturfunktionalitäten untersucht.

Die Anwendbarkeit von § 6c BDSG auf Chipkarten mit biometrischen Daten ist abgelehnt worden, sofern die gesetzliche Zweckbestimmung (wie § 3 Abs. 5 Satz 1 PersAuswG) nur ein Auslesen und Verwenden der Daten zur Überprüfung der Echtheit des Mediums und zur Identitätsprüfung des Inhabers zulässt.[1511] Es ist jedoch grundsätzlich unzulässig, aus der Existenz einer normativen Beschränkung der Verwendungszwecke auf die technische Funktionsweise des Mediums zu schließen. Die Definition in § 3 Abs. 10 BDSG stellt nicht darauf ab, ob auf dem Medium personenbezogene Daten über die Speicherung hinaus durch die ausgebende oder eine andere Stelle automatisiert verarbeitet werden dürfen, sondern ob sie derart verarbeitet werden „können". Mit anderen Worten könnte den Anforderungen der Zweckbeschränkung des § 3 Abs. 5 Satz 1 PersAuswG durchaus dadurch entsprochen werden, dass ein § 3 Abs. 10 BDSG unterfallendes Medium eingesetzt, dann aber durch Organisationsregeln eine Verwendung der Daten nur im Rahmen des bestimmten Zwecks sichergestellt würde. Dies würde zwar dem Gedanken des Systemdatenschutzes widersprechen, wäre aber mit § 3 Abs. 5 Satz 1 PersAuswG vereinbar. Nichtsdestotrotz würden die Unterrichtungspflicht des § 6c BDSG ausgelöst werden.

Entscheidend ist folglich stattdessen eine Analyse der Funktionsweise einer Chipkarte in biometrischen Systemen. Dafür sind die bereits beschriebenen Systemvarianten zu untersuchen:[1512] Die Daten können ausgelesen und in der Peripherie abgeglichen werden, dies ist aber auch auf der Karte möglich (Matching-On-Card). Schließlich gibt es auch Lösungen, bei denen ein Sensor auf dem Medium genutzt wird.

Betrachtet man zunächst die erste Variante, so werden Daten auf der Karte gespeichert. Das reicht nach § 3 Abs. 10 Nr. 2 BDSG aber nicht aus. In Betracht kommt zwar ein Übermitteln. Denn anders als reine Speichermedien liest die Chipkarte (eventuell nach einem Authentisierungsvorgang gegenüber dem Lesegerät) Daten aus dem internen Speicher aus und übermittelt sie aktiv. Eine solche Argumentation würde aber das Kriterium der über die Speicherung hinaus gehenden automatisierten Verarbeitung aushebeln.[1513] Wenn jedes Auslesen aus einer Chipkarte nach der Speicherung eine Übermittlung im Sinne von § 3 Abs. 4 Nr. 3 BDSG wäre, würde im Ergebnis auch eine Chipkarte erfasst, die rein tech-

1509 S. BT-Drs. 14/5793, 63.

1510 In diesem Fall ist allerdings der Umfang der Unterrichtungspflicht fraglich; s. dazu unten 4.3.3.3.3.

1511 Simitis-*Bizer*, § 6c Rn. 19; ebenso *Albrecht* 2003a, 160.

1512 S.o. 2.3.3.2.

1513 Daneben ist fraglich, ob sie vom Wortlaut gedeckt ist. Eine derartige Übermittlung fände nicht „auf", sondern eher „von" dem Medium statt.

nisch ausschließlich zur Aufbewahrung von Daten geeignet ist. Dann aber entspricht sie funktional einer Magnetkarte. Nach Wortlaut, Gesetzesbegründung und Schutzzweck von § 6c BSDG werden derartige reine Speichermedien aber von der Norm nicht erfasst. Eine Karte, die lediglich das Ablegen und automatisierte Auslesen von biometrischen und anderen Identifikationsdaten ermöglicht, fällt damit nicht unter diese Vorschrift.[1514] Dies stellt sich allerdings dann anders dar, wenn ein Verändern der Daten möglich ist. Ein Einwirken von Nichtberechtigten auf die biometrischen Daten ist zwar technisch auszuschließen. Denkbar ist jedoch, dass die ausgebende Stelle (etwa die Personalausweisbehörde) die Möglichkeit hat, eine Veränderung auf der Karte zu bewirken.[1515] In diesem Fall wäre § 6c BDSG anwendbar.

Verfügt das Medium dagegen über einen Sensor, so werden auf ihm Daten erhoben (§ 3 Abs. 3 BDSG).[1516] Fraglich ist, ob dies für § 3 Abs. 10 Nr. 2 BDSG ausreicht. Zu beachten ist, dass die Norm nicht ein Verarbeiten, sondern ein automatisiertes Verarbeiten voraussetzt.[1517] Dieser Begriff wird aber nicht in § 3 Abs. 4 BDSG, sondern in § 3 Abs. 2 BDSG definiert. Er umfasst – sprachlich missglückt[1518] – den engeren Tatbestand des Verarbeitens nach § 3 Abs. 4 BDSG, darüber hinaus aber auch die Erhebung und Nutzung personenbezogener Daten, allerdings immer unter der Voraussetzung des Einsatzes von Datenverarbeitungsanlagen. Da letzteres beim automatisierten Erheben mittels Sensors auf der Chipkarte erfüllt ist, fallen derartige Systeme unter § 3 Abs. 10 BDSG und damit auch unter § 6c BDSG.[1519]

Schließlich erfüllt auch der Vergleich biometrischer Datensätze das Merkmal der automatisierten Verarbeitung.[1520] Das gilt auch für Vergleiche auf einer Chipkarte. Im Ergebnis entsprechen Chipkarten mit biometrischen Daten dann der Definition in § 3 Abs. 10 Nr. 2 BDSG, wenn ein Verändern dieser Daten möglich ist, sie über biometrische Sensoren verfügen, auf ihnen Matching-On-Card Prozesse ablaufen oder sie für letztere vorausgerüstet sind. Da der Betroffene zumindest im Fall des digitalen Personalausweises nicht selbst auf die Daten zugreifen kann, ist auch das letzte Kriterium des § 3 Abs. 10 BDSG zu bejahen. Damit ist § 6c BDSG insoweit anwendbar.

Für die elektronische Gesundheitskarte kommt es nicht darauf an, ob sie die Definition des § 3 Abs. 10 BDSG erfüllt. Es besteht die Besonderheit, dass § 291a Abs. 2 Satz 2 und Abs. 3 Satz 5 SGB V für die verpflichtenden und die freiwilligen Funktionen der Karte die Anwendung von § 6c BDSG anordnen. Deshalb erübrigt sich eine Analyse der unterschiedlichen Applikationen hinsichtlich einer automatisierten Verarbeitung über die Speicherung hinaus.

1514 Ebenso Simitis-*Bizer*, § 3 Rn. 277.

1515 Diese Variante zieht allerdings Missbrauchsprobleme nach sich, da eine – wie auch immer gesicherte – Schreibberechtigung stets die Möglichkeit eines unberechtigten Zugriffs mit sich bringt. Sie ist deshalb für Hochsicherheitskarten wie den digitalen Personalausweis abzulehnen.

1516 Zur Verwendbarkeit von Sensoren beim digitalen Personalausweis s.o. 4.2.2.4.4.

1517 Das wird offensichtlich übersehen von Simitis-*Bizer*, § 6c Rn. 16, der eine Anwendung (auf Signaturkarten) mit dem Argument ablehnt, die Daten würden „lediglich...genutzt“. Exakt dies erfüllt aber den Tatbestand des automatisierten Verarbeitens nach § 3 Abs. 2 BDSG.

1518 *Roßnagel/Pfitzmann/Garstka* 2001, 31 f.; Simitis-*Dammann*, § 3 Rn. 64 ff.; Roßnagel-*Schild*, Kap. 4.2, Rn. 32 ff.

1519 Erhebung und Nutzung durch das Medium sind etwa ausdrücklich geregelt in § 2 Abs. 11 Nr. 2 DSG-LSA. Daraus kann aber nicht gefolgert werden, § 3 Abs. 10 BDSG erfasse im Umkehrschluss diese Varianten des Datenumgangs nicht. Denn das DSG-LSA kennt den umfassenden Begriff der automatisierten Datenverarbeitung im BDSG nicht. Deshalb müssen Erhebung und Nutzung von Daten extra aufgeführt werden, während in § 3 Abs. 10 Nr. 2 BDSG insoweit der Verweis auf § 3 Abs. 2 BDSG ausreicht.

1520 Simitis-*Dammann*, § 3 Rn. 70 (für Fingerabdrücke).

Wenn der Chipkartenausweis über die Möglichkeit verfügt, elektronische Signaturen zu erstellen (oder hierfür vorausgerüstet ist), so wird er regelmäßig auch die weiteren Funktionalitäten der Authentisierung und Verschlüsselung bieten. Diese drei Anwendungen sind Anknüpfungspunkt für eine Datenverarbeitung nach § 3 Abs. 10 Nr. 2 BDSG und getrennt zu betrachten.

Für die elektronische Signatur kommt eine automatisierte Verarbeitung sowohl für den Signaturschlüssel als auch für das Zertifikat in Frage. Ein Zertifikat ist personenbezogen, weil es die Namensangabe des Inhabers (oder sein Pseudonym)[1521] und die Zuordnung eines Schlüssels zu ihm enthält. Der Schlüssel selbst ist über das Zertifikat personenbeziehbar. Mit ihm wird auf der Chipkarte die elektronische Signatur für den Hash-Wert eines spezifischen Dokuments berechnet.[1522] Dabei wird der Schlüssel selbst zwar nicht verarbeitet, sondern lediglich im Sinne von § 3 Abs. 5 BDSG genutzt.[1523] Wie bereits erläutert, reicht dies aber für § 3 Abs. 10 Nr. 2 BDSG aus, da die Norm auf den weiten Begriff der automatisierten Verarbeitung abstellt.[1524]

Auch das qualifizierte Zertifikat des Karteninhabers kann auf dem Chip gespeichert werden.[1525] Eine geschützte Speicherung ist nicht erforderlich, da das Zertifikat selbst eine durch den Zertifizierungsdiensteanbieter signierte Datei ist, die die Zugehörigkeit eines bestimmten Schlüssels zu einer Person bestätigt. Durch eine Ablage auf dem Chip steht dem Inhaber das Zertifikat stets für eine Aufnahme in ein signiertes Dokument oder für die Übermittlung zur Verfügung. Bei diesen Vorgängen wird das Zertifikat aus der Chipkarte ausgelesen. Wie beim Auslesen der biometrischen Identifikationsdaten entspricht die Karte hier aber funktional einem reinen Speichermedium, womit eine Anwendung von § 3 Abs. 10 Nr. 2 BDSG ausscheidet.

Was die Authentisierung angeht, so arbeiten die meisten Karten im so genannten Challenge-Response-Verfahren.[1526] Dabei wird ein beliebiger Datensatz an die Karte gesendet, dort mit dem (vom Signaturschlüssel verschiedenen) Authentisierungsschlüssel verschlüsselt, zurückgesandt und beim Gegenüber mittels des öffentlichen Schlüssels des Karteninhabers entschlüsselt. Stimmt das Ergebnis dieses Vorgangs mit dem ursprünglich gesendeten Datensatz überein, ist die Authentisierung erfolgreich. Bei diesem Vorgang wird, ebenso wie bei der Signatur, ein personenbezogener Schlüssel des Karteninhabers genutzt. Deshalb liegt eine automatisierte Datenverarbeitung vor.

Die Verschlüsselungsfunktion der Signaturkarte funktioniert nach dem Hybridverfahren:[1527] Die Kartenchip des Absenders generiert einen einmaligen, symmetrischen Schlüssel, mit dem das Dokument in der Peripherie des Absenders verschlüsselt wird. Der verwendete symmetrische Schlüssel wird dann mit dem öffentlichen Schlüssel des Erklärungsempfängers verschlüsselt und zusammen mit dem verschlüsselten Dokument an diesen versandt. Der Empfänger entschlüsselt mit seinem geheimen Schlüssel auf seiner

---

1521 Die Verwendung Pseudonymen ist in diesem Fall ohne Bedeutung, weil die Stelle, die möglicherweise durch § 6c BDSG verpflichtet wird (der Zertifizierungsdiensteanbieter) über die Aufdeckungsmöglichkeit verfügt.

1522 Zur Funktionsweise der Signaturerstellung s.o. 2.3.2.

1523 Eine Übermittlung wäre schon nach § 15 Abs. 1 Satz 2 SigV unzulässig, der die Preisgabe des Schlüssels verbietet; dazu RMD-*Roßnagel/Pordesch*, § 16 SigV 1997 Rn. 41 ff.

1524 Deswegen ist die Argumentation von Simitis-*Bizer*, § 6c Rn. 16 nicht stichhaltig, der aus der Tatsache, dass die Daten „lediglich" genutzt werden, folgert, § 3 Abs. 10 BDSG sei nicht erfüllt.

1525 Das wird übersehen von Simitis-*Bizer*, § 6c Rn. 16 f., der hinsichtlich qualifizierter elektronischer Signaturen lediglich die Verwendung des Schlüssels untersucht, für fortgeschrittene Signaturen hingegen eine Speicherung und eventuelle Verarbeitung des Zertifikats auf der Karte annimmt.

1526 S. näher oben 2.3.2.

1527 S.a. oben 2.3.2.

Signaturkarte den verwendeten symmetrischen Schlüssel und entschlüsselt hiernach mit diesem außerhalb seiner Karte das empfangene Dokument. Betrachtet man dieses Verfahren unter dem Gesichtspunkt der automatisierten Verarbeitung, so wird sowohl auf der Seite des Absenders wie des Empfängers der jeweilige (personenbezogene) Schlüssel genutzt: einmal zur Generierung des symmetrischen Schlüssels, einmal zu dessen Entschlüsselung. Auch hier liegt also eine automatisierte Verarbeitung vor, die über die Speicherung hinausgeht.

Findet somit bei allen drei Funktionalitäten der Signaturkarte auf dieser eine automatisierte Verarbeitung über die Speicherung hinaus statt, so ist die Erfüllung des Tatbestands von § 3 Abs. 10 Nr. 2 BDSG trotzdem deshalb zweifelhaft, weil dieser eine automatisierte Verarbeitung durch die ausgebende oder eine andere Stelle verlangt. Nach § 3 Abs. 10 Nr. 3 BDSG ist überdies erforderlich, dass der Betroffene die Verarbeitung nur durch den Gebrauch des Mediums beeinflussen kann.

Beides könnte bereits daran scheitern, dass für alle drei Funktionalitäten eine PIN-Eingabe des Karteninhabers erforderlich ist. Eine derartige Eingabe hindert die Anwendbarkeit von § 3 Abs. 10 Nr. 2 und Nr. 3 BDSG jedoch grundsätzlich nicht,[1528] weil dieser Vorgang lediglich der Authentifizierung des Inhabers dient und damit dem eigentlichen Verarbeitungsprozess zeitlich vorgelagert ist. Findet also eine automatisierte Verarbeitung im Sinne von § 3 Abs. 10 Nr. 2 BDSG statt, und kann diese selbst durch den Betroffenen nicht beeinflusst werden, so liegt trotz vorheriger Eingabe von PIN oder Passwort ein mobiles personenbezogenes Speichermedium vor.

Bei den beschriebenen Vorgängen ist aber auch nach der Eingabe der PIN keine andere Stelle involviert. Der gesamte Vorgang des Signierens, Authentisierens und Ver- wie Entschlüsselns findet vielmehr unter der alleinigen Kontrolle des Signaturkarteninhabers statt. Damit wird dieser zwar noch nicht zur verantwortlichen Stelle im Sinne von § 3 Abs. 7 BDSG, es fehlt aber auch an einer anderen Daten verarbeitenden Stelle. Die Daten werden nicht „durch die ausgebende oder eine andere Stelle“ automatisiert verarbeitet, sondern durch den Karteninhaber. Das gilt sogar dann, wenn die Karte in einer fremden Umgebung verwendet wird, weil der ausschließliche Zugriff des Inhabers erhalten bleibt.[1529] Damit ist im Ergebnis für Signaturkarten weder § 3 Abs. 10 BDSG noch § 6c BDSG einschlägig.[1530]

4.3.3.2.2 Vorrangige Regelungen der Landesdatenschutzgesetze

§ 1 Abs. 2 Nr. 2 BDSG schließt die Anwendung des Bundesdatenschutzgesetzes auf öffentliche Stellen der Länder aus, soweit eine landesgesetzliche Regelung besteht. Damit bleibt eine Norm des Bundesgesetzes immer dann anwendbar, wenn das Landesdatenschutzgesetz keine Regelung im sachlichen Geltungsbereich dieser Norm getroffen hat.[1531] Für mobile Speicher- und Verarbeitungsmedien ist die Rechtslage in den Bundesländern uneinheitlich.[1532] Soweit einige Länder noch keine Novellierung des Datenschutzrechtes vorgenommen oder dabei auf eine Regelung zu mobilen personenbezogenen Speicher- und

1528 Simitis-*Bizer*, § 6c Rn. 26.

1529 Ob dies auch dann noch zutrifft, wenn Signaturkarten (z.B. am Arbeitsplatz) in Abhängigkeitsverhältnissen unter fest vorgegebenen Bedingungen in fremdem Interesse genutzt werden, muss der weiteren Entwicklung vorbehalten bleiben; bejahend *Steidle* 2005, Kap. 10.8.

1530 Allerdings gelten die Unterrichtungspflichten des § 6 SigG. S. zu Reichweite und Inhalt dieser Norm RMD-*Roßnagel*, § 6 SigG 1997, Rn. 24 ff.

1531 *Auernhammer*, § 1 Rn. 26; Simitis-*Dammann*, § 1 Rn. 124 f.

1532 S. bereits *Hornung*, DuD 2004, 15, 17 f.

Verarbeitungsmedien verzichtet haben,[1533] bindet § 6c BDSG auch die öffentlichen Stellen der Länder. Finden sich in den Landesgesetzen Regelungen, die – bei sprachlichen Abweichungen – inhaltlich § 6c BDSG entsprechen,[1534] so gelten für die öffentlichen Stellen der Länder die entsprechenden landesrechtlichen Normen, ohne das sich daraus allerdings sachliche Unterschiede ergeben.

In einigen Ländern weicht die Regelung von der des Bundes ab. Oben wurde bereits erläutert, dass die Landesdatenschutzgesetze teilweise keine Verarbeitung auf dem Medium selbst verlangen, sondern einen automatisierten Austausch mit dem Peripheriesystem[1535] oder das Anstoßen von Verarbeitungsvorgängen dort[1536] ausreichen lassen. Damit können auch reine Speichermedien von diesen Gesetzen erfasst sein.

Auch bei den verpflichteten Stellen gibt es Unterschiede. So entspricht § 5b des Hamburgischen Landesdatenschutzgesetzes zwar (bei starken sprachlichen und strukturellen Unterschieden) inhaltlich weitgehend § 6c BDSG, jedoch mit dem gewichtigen Unterschied, dass lediglich die ausgebende, nicht jedoch auch die ein automatisiertes Verfahren aufbringende, ändernde oder bereithaltende Stelle verpflichtet wird.[1537] Entsprechende Regelungen enthalten einige weitere Landesgesetze.[1538] In Bremen wird die „verantwortliche“ Stelle verpflichtet. Dies deutet daraufhin, dass nur die tatsächlich Daten verarbeitende oder beauftragende, nicht jedoch die Karten ausgebende Stelle verpflichtet wird.[1539] In Mecklenburg-Vorpommern gelten die Rechte gegenüber der ausgebenden und jeder anderen Stelle, die das Medium zur Datenverarbeitung einsetzt.[1540]

Nach dem nordrhein-westfälischen Landesdatenschutzgesetz ist die Ausgabe mobiler Systeme nur mit Einwilligung des Betroffenen und nach dessen Aufklärung zulässig.[1541] Andere Bundesländer lassen die Ausgabe alternativ auch aufgrund einer gesetzlichen Ermächtigung zu.[1542] In Bremen und Mecklenburg-Vorpommern ist die erforderliche Unterrichtung auf Wunsch des Betroffenen schriftlich zu erteilen.[1543] Bremen verzichtet außerdem auf die Unterrichtung über die Maßnahmen bei Verlust und Zerstörung,[1544]

1533 Das betrifft Bayern, Sachsen und Thüringen.

1534 S. etwa § 31c BLnDSG (wörtliche Übereinstimmung), § 6a NDSG und § 35 DSG Rh.-Pf. (leichte sprachliche Abweichungen), § 25 DSG-LSA (Verzicht auf eine § 6c Abs. 2 BDSG entsprechende Regelung, was jedoch wegen der im Rahmen der Betroffenenrechte geregelten Kostenfreiheit ohne Belang ist), § 20a BrDSG und § 5 Abs. 2 DSG BW (mit deutlichen sprachlichen Unterschieden und einer Verpflichtung der „verantwortlichen“ Stelle, s. dazu unten Fn. 1539).

1535 § 5b HmbDSG, § 3 Abs. 10 DSG MV.

1536 § 5 Abs. 3 BbgDSG.

1537 Unzutreffend *Gola/Schomerus*, § 6c Rn. 12 (die Regelung sei inhaltlich identisch mit § 6c BDSG).

1538 Auch § 5 Abs. 3 BbgDSG, § 29a DSG NW und § 18 DSG SH verpflichten nur die ausgebende Stelle.

1539 § 20a Abs. 2 BrDSG ist unklar formuliert, weil mit „verantwortlicher Stelle“ nach § 2 Abs. 3 Nr. 1 BrDSG jede Daten verarbeitende oder beauftragende Stelle gemeint ist. Da im Absatz vor § 20a Abs. 2 BrDSG jedoch von Ausgabe und Einsatz mobiler Medien gemeint ist, könnte auch die ausgebende Stelle erfasst sein.

1540 § 36 Abs. 4 DSG MV.

1541 § 29 DSG NW.

1542 § 25 DSG-LSA (außerdem beim Einsatz von Zugangskontrollsystemen) und § 18 DSG SH. Diese Variante wird in beiden Fällen übersehen von *Gola/Schomerus*, § 6c Rn. 12. Entsprechende Regelungen wurden zuletzt aufgenommen in § 20a Abs. 1 BrDSG und § 36 Abs. 1 DSG MV (dort ist die Verwendung darüber hinaus im Rahmen von tarifvertraglichen Regelungen und Dienstvereinbarungen zulässig).

1543 § 20a Abs. 2 Satz 1 BrDSG; § 36 Abs. 2 Satz 2 DSG MV; zum Formerfordernis nach dem BDSG s.u. 4.3.3.3.4.

1544 § 20a Abs. 2 BrDSG.

Hessen auf die über die Funktionsweise des Mediums.[1545] Die überwiegende Zahl der Länder verlangt schließlich keine Angabe über Identität und Anschrift des Verpflichteten.[1546]

Für die unterschiedlichen Chipkartenausweise kann diese Rechtszersplitterung zu mehr oder weniger großen Schwierigkeiten führen. Sofern es um Medien geht, die nur von einem Bundesland ausgegeben werden, sind die beschriebenen Unterschiede in den Landesdatenschutzgesetzen unproblematisch. Gleiches gilt, wenn die Anwendung von § 6c BDSG spezialgesetzlich angeordnet wird. Das ist bei der elektronischen Gesundheitskarte in § 291a Abs. 2 Satz 2 und Abs. 3 Satz 5 SGB V geschehen. Insoweit stellt sich die Frage einer Anwendbarkeit der Landesdatenschutzgesetze nicht.

Probleme ergeben sich jedoch für den digitalen Personalausweis. Hier gibt es zunächst Unterschiede, die sich im konkreten Fall nicht auswirken. So wird die Ermächtigung zur Ausgabe und zur Verwendung des Personalausweises in einem geänderten Personalausweisgesetz geregelt werden. Ein entsprechendes Freiwilligkeitserfordernis in den Ländern ist damit ohne Wirkung. Das Erfordernis einer Angabe von Identität und Anschrift der verpflichteten Stelle (§ 6c Abs. 1 Nr. 1 BDSG) fehlt zwar in einigen Landesgesetzten, dürfte aber in der dort geforderten Angabe über die Geltendmachung von Rechten mit enthalten sein. Schwieriger sind die Einschränkungen hinsichtlich der verpflichteten Stelle. Es ließe sich aber vertreten, dass es sich dabei nicht um eine sachliche Änderung, sondern um eine Begrenzung des Geltungsbereichs handelt. In diesem Fall bliebe das Bundesdatenschutzgesetz für den übrigen Bereich anwendbar, weil die landesrechtliche Regelung lediglich einen Ausschnitt des Bundesrechts betrifft.[1547]

Eine entsprechende Interpretation ist jedoch nicht durchweg möglich. Das betrifft vor allem Formfragen wie das Problem der Schriftlichkeit,[1548] aber auch Regelungen zum Inhalt der Aufklärung. Insoweit bleiben Unterschiede zwischen den Ländern bestehen. Das größte Problem dürfte schließlich der Verzicht einiger Landesgesetze auf ein Verarbeiten auf dem Medium selbst sein, weil hierdurch auch reine Speichermedien zur Ablage biometrischer Daten erfasst werden. Konkret würde dies bedeuten, dass ein digitaler Personalausweis, der in seiner technischen Gestaltung nicht der engeren Definition des § 3 Abs. 10 BDSG unterfiele, zwar in Brandenburg, Hamburg und Mecklenburg-Vorpommern Unterrichtungspflichten auslösen würde, nicht aber im Rest des Bundesgebietes.

Eine solche Situation ist für den Personalausweis, der als bundeseinheitlich konzipiertes Medium ausgeben wird und dessen Besitz und Funktionsweise durch Bundesgesetz geregelt sind, nicht akzeptabel. Die Neuartigkeit und komplexe Funktionsweise des digitalen Personalausweises bringt es mit sich, dass bereits aus gleichheitsrechtlichen Gesichtspunkten eine bundesweit einheitliche Unterrichtung durch einen einheitlich konzipierten Informationsakt zu fordern ist. Dies kann auf zwei Wegen erreicht werden. Eine Möglichkeit ist die Anordnung der Anwendung von § 6c BDSG wie bei der elektronischen Gesundheitskarte. Die Gesetzgebungskompetenz für eine solche Norm würde sich kraft Sachzusammenhangs mit der für den Personalausweis aus Art. 75 Nr. 5 GG bestehenden Kompetenz ergeben.[1549] Alternativ könnte eine Anpassung des Landesdatenschutzrechts erfolgen,

1545 § 8 Abs. 2 HDSG. Die Norm, obgleich seit 1999 in Kraft, fehlt in der Aufstellung von *Gola/Schomerus*, § 6c Rn. 12.

1546 Ausnahmen sind etwa § 31c BLnDSG, § 6a NDSG und § 35 DSG Rh.-Pf.

1547 Simitis-*Dammann*, § 1 Rn. 125.

1548 Auch wenn nach hier vertretener Ansicht jedenfalls für komplexe Karten wie dem digitalen Personalausweis auch nach dem BDSG eine Textform der Unterrichtung erforderlich ist, s.u. 4.3.3.3.4.

1549 Allgemein zur Kompetenz des Bundes im Bereich des Datenschutzes s. Simitis-*Simitis*, § 1 Rn. 1 ff.; Roßnagel-*Tinnefeld*, Kap. 2.6, Rn. 11 ff., jeweils m.w.N.

indem entweder die entsprechenden Regelungen § 6c BDSG angeglichen oder in den Ausführungsgesetzen zum Personalausweisgesetz entsprechende Normen speziell für den Ausweis eingeführt würden. Aus Gründen der Rechtsklarheit sollte die Variante einer Verweisung auf § 6c BDSG im Personalausweisgesetz des Bundes vorgezogen werden,[1550] zumal es wenig wahrscheinlich erscheint, dass übereinstimmende Fassungen der entsprechenden Normen der Landesdatenschutz- oder Landespersonalausweisgesetze verabschiedet würden.

4.3.3.2.3 Abgrenzung zu verwandten Normen

Im Zusammenhang mit dem Einsatz von Chipkartenausweisen können auch noch andere Aufklärungs- und Hinweispflichten eine Rolle spielen. Das betrifft insbesondere die Aufklärung vor einer Einwilligung nach § 4a Abs. 1 Satz 2 BDSG, die Information nach § 291a Abs. 3 Satz 2 SGB V und die Unterrichtungspflichten nach § 6 SigG.

Die Hinweispflicht aus § 4a Abs. 1 Satz 2 BDSG und die Unterrichtung nach § 6c Abs. 1 BDSG können inhaltlich weitgehend identisch sein. Zwar ist nach dem Wortlaut von § 4a Abs. 1 Satz 2 BDSG nur ein Hinweis auf den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung erforderlich. Sowohl Verarbeitungsziele wie -folgen lassen sich für den Betroffenen jedoch nur abschätzen, wenn die genaue Art der Daten und die Verarbeitungsbedingungen angegeben werden.[1551] Hierzu gehört im Regelfall auch die Funktionsweise eines verwendeten mobilen personenbezogenen Speicher- und Verarbeitungsmediums.

Dennoch sind die beiden Pflichten nach Tatbestand und Rechtsfolgen strikt voneinander zu trennen.[1552] § 4a BDSG findet keine Anwendung, wenn ein Medium per Gesetz eingeführt wird, während § 6c BDSG auch in diesem Fall einschlägig ist. Umgekehrt kann jedoch bei einem freiwillig abgegebenen Medium § 6c Abs. 1 BDSG schon weit vor der Hinweispflicht nach § 4a Abs. 1 Satz 2 BDSG eingreifen, wenn es sich um ein Medium handelt, dass zur automatisierten Verarbeitung lediglich vorausgerüstet ist. Die Norm begründet insoweit vorgezogene Informationspflichten. Es kommt nicht darauf an, ob unmittelbar nach der Ausgabe des mobilen personenbezogenen Speicher- und Verarbeitungsmediums eine Speicherung von Daten erfolgt, oder ob das Verfahren zur automatisierten Datenverarbeitung unmittelbar nach der Aufbringung, Änderung oder Bereithaltung Daten verarbeitet. Auch bei großem zeitlichen Abstand zwischen dem Tatbestand, der die Informationspflichten auslöst, und der letztlichen Datenverarbeitung muss die Aufklärung nach § 6c Abs. 1 BDSG sofort erfolgen. Schließlich sind die Rechtsfolgen nach § 6c Abs. 1 BDSG weitergehend, weil sie auch eine Unterrichtung über die Ausübung von Betroffenenrechten und die notwendigen Maßnahmen bei Verlust und Zerstörung beinhalten. Derartiges wird von § 4a Abs. 1 Satz 2 BDSG nicht gefordert.

Gemäß § 291a Abs. 3 Satz 2 SGB V hat die Krankenkasse die Versicherten spätestens bei der Versendung der Gesundheitskarte umfassend und in allgemein verständlicher Form über deren Funktionsweise, einschließlich der Art der auf ihr oder durch sie zu erhebenden, zu verarbeitenden oder zu nutzenden personenbezogenen Daten zu informieren. Diese Anforderung entspricht inhaltlich § 6c Abs. 1 Nr. 2 BDSG, soweit diese Norm die ausgebende Stelle (nämlich die Krankenkassen) betrifft. Sie ist angesichts des ausdrücklichen

1550 S. *Roßnagel/Hornung*, in: Reichl/Roßnagel/Müller 2005, 230.
1551 Simitis-*Simitis*, § 4a Rn. 69.
1552 Die beiden vermengend etwa Roßnagel-*Weichert*, Kap. 9.5, Rn. 47 ff.

Verweises in § 291a Abs. 3 Satz 5 SGB V auf den gesamten § 6c BDSG überflüssig, ohne dass sich inhaltliche Kollisionsprobleme ergeben.

Das Verhältnis zur Unterrichtungspflicht nach § 6 SigG[1553] ist unproblematisch, weil § 6c BDSG auf Signaturverfahren keine Anwendung findet.[1554] Wenn der Chipkartenausweis aufgrund anderer Funktionalitäten die Definition des § 3 Abs. 10 BDSG erfüllt, sind § 6 SigG und § 6c BDSG nebeneinander anwendbar.

4.3.3.3 Unterrichtungspflichten nach § 6c Abs. 1 BDSG

4.3.3.3.1 Verpflichtete Stelle

§ 6c Abs. 1 BDSG verpflichtet mehrere Stellen, nämlich solche, die ein mobiles personenbezogenes Speicher- und Verarbeitungsmedium ausgeben oder ein Verfahren zur automatisierten Verarbeitung personenbezogener Daten, das ganz oder teilweise auf einem solchen Medium abläuft, auf dieses aufbringen, ändern oder hierzu bereithalten.[1555] Angesichts dieses Wortlauts ist die Auffassung falsch, Normadressat sei nur „die ausgebende Stelle".[1556]

Ein Bereithalten kann etwa darin liegen, dass automatisierte Verfahren zur Installation durch den Betroffenen (beispielsweise nach Herunterladen aus dem Internet)[1557] vertrieben werden. Hinter dieser Verpflichtung zur Unterrichtung steht der Gedanke, dass durch das Aufbringen oder Verändern derartiger Verfahren das tatsächliche Potential, und damit die datenschutzrechtliche Relevanz des mobilen Mediums verändert wird. Deshalb soll eine Aufklärung erfolgen.

Nach dem Wortlaut von § 6c Abs. 1 BDSG macht es keinen Unterschied, in welchem Stadium das Verfahren auf dem Medium aufgebracht oder geändert wird. Danach wären auch solche Stellen verpflichtet, die vor der Ausgabe des Mediums automatisierte Verarbeitungsverfahren aufbringen oder ändern. Hiervon wären insbesondere die Hersteller der Medien betroffen. Gegen eine solche Interpretation der Norm spricht allerdings, dass das Verarbeitungsverfahren regelmäßig im Auftrag der ausgebenden Stelle auf das Medium aufgebracht werden wird. Diese ist jedoch ohnehin zur umfassenden Unterrichtung nach § 6c Abs. 1 BDSG verpflichtet, die auch die Einzelheiten des Verfahrens umfassen muss. Auf der anderen Seite können die Unterrichtungspflichten dann am effektivsten umgesetzt werden, wenn die Aufklärung durch die Stelle vorgenommen wird, die für das jeweilige Verfahren am kompetentesten ist. Dies wird regelmäßig der Hersteller sein. Denkbar wäre deshalb, eine Verpflichtung aller beteiligten Stellen zur Konzeption eines einheitlichen Informationsakts anzunehmen.[1558]

Eine derart gleichmäßig verteilte Aufklärungspflicht verursacht jedoch kaum zu überwindende praktische Schwierigkeiten. So wäre die Frage zu klären, in welchem Umfang die im Hintergrund bleibende Stelle selbständige Unterrichtungspflichten für den Fall wahrzunehmen hätte, dass die ausgebende Stelle ihrer Verpflichtung nicht nachkommt. Es ist dem Hersteller weder möglich noch zumutbar nachzuprüfen, ob seine Kunden, die

1553 Zu dessen Reichweite vgl. RMD-*Roßnagel*, § 6 SigG 1997 Rn. 24 ff.
1554 S.o. 4.3.3.2.1.2.
1555 Vgl. zu den Unterrichtungspflichten bereits *Hornung*, DuD 2004, 15, 19 f.
1556 So aber *Schaffland/Wiltfang*, § 6c Rn. 2.
1557 S. die Gesetzesbegründung, BT-Drs. 14/5793, 63.
1558 Eine separate Unterrichtung der beteiligten Stellen wäre ebenfalls denkbar, jedoch ökonomisch unsinnig und aus teleologischer Sicht kontraproduktiv, da sie den Betroffenen, der mehrere Unterrichtungen über dasselbe Medium erhielte, eher verwirren würde.

Chipkarten (beispielsweise als Arbeitgeber an ihre Beschäftigten) ausgeben, die Anforderungen von § 6c Abs. 1 BDSG erfüllen. Außerdem ist der Fall denkbar, dass die beteiligten Stellen unterschiedliche oder sich widersprechende Vorstellungen über die Konzeption des Informationsakts haben.

Die angesprochene technische Kompetenz der Stelle, die – wie der Hersteller – das Verfahren selbst gestaltet, spricht aber entscheidend dagegen, diese vollständig aus ihrer Pflicht zu entlassen. Da eine gleichberechtigte Teilnahme an der Unterrichtung jedoch unpraktikabel ist und kein direkter Kontakt mit dem Betroffenen besteht (regelmäßig wird der Hersteller diesen nicht einmal kennen), verwandelt sich die Pflicht zur Unterrichtung des Betroffenen in eine Pflicht, der ausgebenden Stelle alle Informationen zukommen zu lassen, die diese für eine ordnungsgemäße und vollständige Unterrichtung benötigt. Eine solche Pflicht wird außerdem regelmäßig bereits aus dem Vertrag zwischen der ausgebenden Stelle und der Stelle im Hintergrund (etwa ein Hersteller biometrischer Identifikationssysteme) folgen. Informiert der Hersteller die ausgebende Stelle über sein auf der Karte ablaufendes automatisiertes Verarbeitungsverfahren, so genügt er auch den Anforderungen aus § 6c Abs. 1 BDSG.

Für den digitalen Personalausweis ist zunächst zu klären, wer die ausgebende Stelle im Sinne von § 6c Abs. 1 BDSG ist. Der Ausweis selbst wird in der Personalausweisbehörde[1559] beantragt und abgeholt. Gleichzeitig handelt es sich jedoch um ein bundeseinheitliches Dokument. Außerdem gründet sich die Pflicht, einen Personalausweis zu besitzen, auf ein Bundesgesetz (§ 1 Abs. 1 Satz 1 PersAuswG). Schließlich bestimmt § 1 Abs. 7 Satz 2 PersAuswG, dass der Personalausweis Eigentum der Bundesrepublik Deutschland ist.[1560] Das würde für deren Verpflichtung sprechen. Auf der anderen Seite bezweckt § 6c Abs. 1 BDSG erkennbar, dass die Unterrichtungspflichten durch die Stelle wahrgenommen werden, die dem Betroffenen unmittelbar gegenüber tritt. Dies sind die Personalausweisbehörden. Der Bund ist demgegenüber eine im Hintergrund agierende Stelle und somit eher mit dem Hersteller vergleichbar, der ein biometrisches Verfahren auf den Ausweis aufbringt.[1561] Diese beiden Instanzen müssen nach den vorstehenden Überlegungen an der Konzeption eines Informationsaktes mitwirken, der danach jedoch allein durch die Personalausweisbehörde durchgeführt wird. Eigenständige Unterrichtungspflichten ergeben sich dann, wenn der digitale Personalausweis zum Nachladen von Zusatzapplikationen geeignet sein sollte. In diesem Fall müssen die Stellen, die derartige Verfahren auf den Ausweis aufbringen, ändern oder hierzu bereithalten, den Betroffenen informieren.

Die elektronische Gesundheitskarte wird nach § 291 Abs. 1 Satz 1 in Verbindung mit § 291a Abs. 1 SGB V von den gesetzlichen Krankenkassen ausgegeben. Damit treffen sie die Pflichten des § 6c BDSG. Die Hersteller der Karten haben sie bei der Ausarbeitung des Unterrichtungsvorgangs zu unterstützen. Andere Stellen sind nur dann beteiligt, wenn die Karte neben den Funktionen nach § 291a Abs. 2 Satz 1 und Abs. 3 Satz 1 SGB V noch über die Möglichkeit zum Nachladen weiterer Anwendungen verfügt.

Für alle Chipkartenausweise gilt schließlich, dass Zertifizierungsdiensteanbieter in keinem Fall § 6c BDSG unterliegen.

1559 S. die Übersicht in Fn. 158 (S. 50).

1560 Dies wird in den Ausführungsgesetzen der Länder regelmäßig wiederholt, z.B. § 1 Abs. 7 LPersAuswG Bln., § 1 Abs. 5 LPersAuswG Rh.-Pf.

1561 Dies unter der Voraussetzung, dass ein automatisiertes Verarbeiten über die Speicherung hinaus vorliegt; s. dazu oben 4.3.3.2.1.2.

4.3.3.3.2 Berechtigter

Die Unterrichtungspflichten sind dem „Betroffenen“ gegenüber zu erfüllen. Nach § 3 Abs. 1 BDSG fällt darunter zunächst der Inhaber des Mediums. Wird jedoch über ein Medium informiert, das noch keine Verfahren enthält oder Daten verarbeitet, so ist der Begriff des Betroffenen in § 6c BDSG weiter als die allgemeine Definition in § 3 Abs. 1 BDSG und meint auch den zukünftig Betroffenen.[1562]

Fraglich ist, ob auch andere Betroffene außer dem Karteninhaber nach § 6c BDSG informiert werden müssen. Dies könnte dann der Fall sein, wenn neben Daten des Inhabers auch Daten eines Dritten auf dem Medium automatisiert verarbeitet werden.[1563] Zwar ist die Norm von ihrer Konzeption her auf eine Unterrichtung des Inhabers des Mediums ausgerichtet. Wortlaut und Schutzzweck erfassen jedoch auch den Fall, dass Daten eines Dritten betroffen sind. In diesem Fall können bei der Umsetzung allerdings organisatorische Probleme auftreten. Außerdem verändert sich der Inhalt der Unterrichtung: Eine Aufklärung über die bei Verlust oder Zerstörung des Mediums zu ergreifenden Maßnahmen (§ 6c Abs. 1 Nr. 4 BDSG) entfällt, weil der Dritte nicht Inhaber des Mediums ist und dementsprechend weder von dessen Verlust oder Zerstörung Kenntnis nehmen noch Maßnahmen ergreifen kann.

Für Chipkartenausweise ist danach die Unterrichtungspflicht in jedem Fall dem Inhaber gegenüber zu erfüllen. Beim digitalen Personalausweis werden nur Daten des Inhabers verwendet, sodass keine Dritten beteiligt sind. Dies ist bei der elektronischen Gesundheitskarte zumindest bezüglich der Leistungserbringer anders: Daten über die Behandlung des Versicherten enthalten auch personenbezogene Daten über den jeweiligen Leistungserbringer. Allerdings ist es dieser selbst, der die Verarbeitung auf der Karte bewirkt. Deshalb besteht ihm gegenüber keine Unterrichtungspflicht nach § 6c Abs. 1 BDSG.

4.3.3.3.3 Umfang der Unterrichtung

§ 6c Abs. 1 Nr. 1 BDSG verpflichtet die unterrichtende Stelle zunächst zur Angabe ihrer Identität und Anschrift um das Geltendmachen von Rechten zu erleichtern.[1564] Deshalb muss die Art und Weise der Unterrichtung den datenschutzrechtlichen Auskunftsanspruch nach §§ 19, 34 BDSG sowie eine eventuelle gerichtliche Durchsetzung ermöglichen und hierzu den Anforderungen des § 130 Nr. 1 ZPO genügen.[1565] Nicht mit dem Wortlaut von § 6c Abs. 1 Nr. 1 BDSG vereinbar ist die Auffassung, die Information über die Anschrift könne „in aller Regel“ entfallen.[1566] Nur wenn der jeweilige Chipkartenausweis (wie der digitale Personalausweis) die Identität der unterrichtenden Stelle in aufgedruckter Form erkennen lässt, kann dies im Einzelfall überflüssig sein.

Nach § 6c Abs. 1 Nr. 2 BDSG bezieht sich die Unterrichtungspflicht auch auf die Funktionsweise des Mediums einschließlich der Art der zu verarbeitenden personenbezogenen Daten.[1567] Das betrifft eine sehr breite Gruppe von Fragestellungen, etwa bezüglich des verwendeten Chips und Betriebssystems, der verwendeten Daten, der Zugriffsbefugnisse verschiedener Stellen, des Ablaufs von Auslesevorgängen (einschließlich etwaiger außer-

1562 Vgl. die Gesetzesbegründung, BT-Drs. 14/5793, 60; ebenso Simitis-*Bizer*, § 6c Rn 31.
1563 Simitis-*Bizer*, § 6c Rn. 33.
1564 S. die Gesetzesbegründung, BT-Drs. 14/5793, 63.
1565 Vgl. im Einzelnen Simitis-*Bizer*, § 6c Rn. 39; zu den Anforderungen gemäß § 130 Nr. 1 ZPO vgl. Baumbach-*Hartmann*, § 130 Rn. 7 ff. m.w.N.
1566 So aber *Schaffland/Wiltfang*, § 6c Rn. 3.
1567 S. die Gesetzesbegründung, BT-Drs. 14/5793, 63; Simitis-*Bizer*, § 6c Rn. 44 ff.

halb des mobilen Mediums ablaufender Verfahrensschritte),[1568] der Sicherungsmechanismen gegen unbefugtes Auslesen durch Dritte (insbesondere durch Verschlüsselung), der Verfügbarkeit von Zusatzapplikationen, des Potentials des Mediums für zukünftige Nutzbarkeiten bis hin zur Handhabung im Alltag.

Hinsichtlich des Umfangs der Unterrichtungspflicht nennt § 6c Abs. 1 Nr. 2 BDSG die Funktionsweise „des Mediums". Das spricht dafür, auch Applikationen, die für sich nicht den Tatbestand des § 3 Abs. 10 BDSG erfüllen, in die Unterrichtung mit einzubeziehen. Gleiches könnte sogar für eine Verwendung ohne Einsatz elektronischer Schreib- und Lesegeräte, beispielsweise bei Sichtkontrollen, gelten. Andererseits liegt der spezifische Schutzzweck von § 6c BDSG gerade in der für den Betroffenen intransparenten Datenverarbeitung auf der Karte,[1569] die bei einer Verwendung im Rahmen einer Sichtkontrolle oder bei reinen Speichervorgängen jedoch nicht gegeben ist. Daneben würden auch praktische Probleme auftreten. So würde etwa bei einer ausschließlich zur Datenspeicherung eingesetzten Karte mit Prozessorchip das Freihalten eines kleinen Teils des Speichers für den Fall des späteren Ablegens weiterer Daten eine umfassende Unterrichtungspflicht allein deshalb auslösen, weil dieser Teil theoretisch auch zur automatisierten Datenverarbeitung genutzt werden könnte. Auf den digitalen Personalausweis bezogen würde die Reservierung eines Speicherteils bedeuten, dass die Personalausweisbehörden als ausgebende Stellen – und nicht die Zertifizierungsdiensteanbieter – eine umfassende Unterrichtung über die Funktionsweise der elektronischen Signatur vornehmen müssten. Das ist aber weder sinnvoll noch vom Gesetz gewollt. Eine Aufklärungspflicht besteht damit nur für die Anwendungen, die die Unterrichtungspflicht auslösen. Andere Applikationen können allenfalls dann erfasst sein, sofern sie mit den erstgenannten interagieren.

Je nach Chipkartenausweis ist die Unterrichtung unterschiedlich auszugestalten. Aufgrund der soeben beschriebenen Einschränkung muss nach § 6c Abs. 1 Nr. 2 BDSG keinesfalls eine Information über eine eventuelle Signaturfunktion erfolgen; diese Anforderung ergibt sich allein aus § 6 SigG. Beim digitalen Personalausweis ist insbesondere zu informieren über die Arbeitsweisen der Identifizierungsfunktion und möglicher Zusatzapplikationen, bestehende Mechanismen zur Datentrennung, die Arbeitsweise des biometrischen Identifizierungsmerkmals (einschließlich der Fehlerraten und der eingerichteten Rückfallsysteme), sowie die weitere Verarbeitung von ausgelesenen Daten in automatisierten Verarbeitungssystemen.[1570] Ebenso ist eine detaillierte Erläuterung der Funktionsweise der elektronischen Gesundheitskarte erforderlich,[1571] die getrennt nach den einzelnen Anwendungen aus § 291a Abs. 2 Satz 1 und Abs. 3 Satz 1 SGB V zu erfolgen hat. Insbesondere die Handhabung der technischen Autorisierung nach § 291a Abs. 5 Satz 2 SGB V, die Zugriffsbefugnisse der Leistungserbringer und die Verwendung von Daten, die mittels der Gesundheitskarte in peripheren Datennetzen gespeichert werden, sind zu erklären.

Hervorzuheben ist, dass die Unterrichtung nach § 6c Abs. 1 Nr. 2 BDSG in „allgemein verständlicher Form" erfolgen muss. Dahinter steht die Erkenntnis, dass eine ausführliche, technisch-wissenschaftlich exakte, jedoch der Mehrheit der Benutzer unverständliche Form der Unterrichtung jeden Informationseffekt verfehlen würde. Unumgänglich ist vor allem

1568 Vgl. die Begründung, BT-Drs. 14/5793, 63; zur Notwendigkeit einer Gesamtsicht von Karte und Peripherie zur Einschätzung der datenschutzrechtlichen Risiken bereits *Roßnagel* 1994b, 268 f.; *Der hessische Datenschutzbeauftragte* 1995, unter 17.3; ferner *Weichert*, DuD 1997, 266, 268; *ders*., DuD 2004, 391, 393.

1569 Das hebt die Gesetzesbegründung hervor, s. BT-Drs. 14/5793, 63; s.a. *Gola/Schomerus*, § 6c Rn. 2.

1570 Dies immer unter der Voraussetzung der Anwendbarkeit von § 6c BDSG (s.o. 4.3.3.2.1.2) oder der Einführung einer Verweisungsnorm.

1571 Zum Verhältnis zu § 291a Abs. 3 Satz 2 SGB V s. bereits oben 4.3.3.2.3.

eine dem Nutzer verständliche Sprache. Die besondere Herausforderung liegt darin, Ausdrucksformen für komplizierte technische Vorgänge zu finden, die für möglichst jeden Nutzer verständlich, gleichzeitig aber nicht durch eine zu starke Vereinfachung des technischen Ablaufs inkorrekt sind. Da eine Vereinheitlichung des Unterrichtungsvorgangs unvermeidbar ist, muss dieser sich an den typischerweise vom Medium betroffenen Personen orientieren.[1572] Insbesondere bei groß angelegten und sensiblen Projekten wie dem digitalen Personalausweis bieten sich Tests an, bevor eine allgemeine Unterrichtung erfolgt.

Das Gesetz fordert keine Angabe über die Möglichkeit, sich weiterführende Informationen über die technische Funktionsweise des Mediums zu beschaffen, die dann nicht mehr allgemein verständlich sein müssten.[1573] Hierdurch könnte allerdings die Transparenz wesentlich erhöht werden, weil informierten Benutzern und Interessengruppen damit ein Instrument in die Hand gegeben würde, sich ein genaueres Bild von der Arbeitsweise des Mediums und seiner datenschutzrechtlichen Relevanz zu machen.

§ 6c Abs. 1 Nr. 3 BDSG verpflichtet zur Unterrichtung über die Ausübbarkeit der Betroffenenrechte aus §§ 19, 20, 34 und 35 BDSG, nämlich auf Auskunft, Berichtigung, Löschung und Sperrung von Daten im öffentlichen wie nichtöffentlichen Bereich, sowie über das für den öffentlichen Bereich geltende Widerspruchsrecht. Inhalt dieser Unterrichtung ist zunächst die (allerdings bereits nach § 6c Abs. 1 Nr. 1 BDSG erforderliche) Angabe von Identität und Anschrift des Verpflichteten. Es ist jedoch nicht zutreffend, dass die Anforderungen nach § 6c Abs. 1 Nr. 3 BDSG bereits mit der Angabe der Adresse der verantwortlichen Stelle erfüllt werden.[1574] Erforderlich ist eine Unterrichtung darüber „wie" die Rechte geltend gemacht werden können, nicht etwa (lediglich) „wem gegenüber" dies geschehen kann. Damit müssen auch Erläuterungen zum Verfahrensablauf gegeben werden.

§ 6c Abs. 1 Nr. 3 BDSG ist außerdem mit § 6c Abs. 2 BDSG verknüpft.[1575] Über die dort genannten Geräte oder Einrichtungen zur Wahrnehmung des Auskunftsrechts, für deren Verfügbarkeit die in § 6c Abs. 1 BDSG genannten Stellen verantwortlich sind, ist auch im Rahmen von § 6c Abs. 1 Nr. 3 BDSG aufzuklären.[1576] Das betrifft insbesondere den Standort und die Funktionsweise der Geräte. Sollten also für den jeweiligen Chipkartenausweis öffentliche Terminals zur Verfügung stehen,[1577] so müsste bereits bei der Ausgabe des Ausweises über diese aufgeklärt werden.

Schließlich muss die verpflichtete Stelle gemäß § 6c Abs. 1 Nr. 4 BDSG über die Maßnahmen unterrichten, die der Betroffene bei Verlust oder Zerstörung des Mediums zu treffen hat. Für den digitalen Personalausweis enthalten die Ausführungsgesetze der Länder entsprechende Pflichten des Ausweisinhabers. Danach ist der Verlust des Ausweises unverzüglich anzuzeigen, ein wiederaufgefundener Ausweis abzugeben und bei Verlust, Beschädigung oder unbefugter Veränderung ein neuer Ausweis zu beantragen.[1578] Entsprechende gesetzliche Regelungen gibt es bislang für die elektronische Gesundheitskarte

1572 Simitis-*Bizer*, § 6c Rn. 49.

1573 Auch die Gesetzesbegründung (BT-Drs. 14/5793, 63) betont, dass detaillierte technische Beschreibungen aus § 6c Abs. 1 BDSG nicht beansprucht werden können.

1574 So aber *Schaffland/Wiltfang*, § 6c Rn. 5.

1575 Dazu unten 4.3.3.4.

1576 *Gola/Schomerus*, § 6c Rn. 7; *Duhr/Naujok/Peter/Seiffert*, DuD 2002, 5, 31.

1577 Denkbar wären diese in den Personalausweisbehörden (für den digitalen Personalausweis) und in Arztpraxen oder Zweigstellen der Krankenkassen (für die elektronische Gesundheitskarte).

1578 S. etwa § 6 LPersAuswG Rh.-Pf., § 6 LPersAuswG Bln., § 6 LPersAuswG Bbg; näher *Medert/Süßmuth* 1998, Teil C Rn. 56 ff.

nicht. Aufzuklären ist jedoch auch über Maßnahmen, die die jeweilige Krankenkasse von ihren Mitgliedern verlangt. Mangels Anwendbarkeit auf das Signaturverfahren muss im Rahmen von § 6c BDSG dagegen nicht über die Abläufe des Sperrverfahrens nach § 8 SigG und § 7 SigV unterrichtet werden. Für Zusatzapplikationen ist die Frage je nach konkreter Anwendung zu beantworten.

4.3.3.3.4 Form und Zeitpunkt

§ 6c Abs. 1 BDSG trifft keine Aussage zur Frage des Ablaufs des Unterrichtungsvorgangs und des zu verwendenden Mediums. Insbesondere wird keine Pflicht normiert, die Schriftform zu wählen. Denkbar wäre allerdings, in einer Analogie zu §§ 4a Abs. 1 Satz 3, 34 Abs. 3 BDSG und § 6 Abs. 3 Satz 1 SigG auch für § 6c Abs. 1 BDSG eine Unterrichtung in Schrift- oder Textform (§ 126 oder § 126a BGB) zu fordern. Die Einwilligung in die Datenverarbeitung hat nach § 4a Abs. 1 Satz 3 BDSG schriftlich zu erfolgen, sofern nicht wegen besonderer Umstände eine andere Form angemessen ist. Gleiches gilt (unter denselben Einschränkungen) für die allgemeine Auskunft im nichtöffentlichen Bereich nach § 34 Abs. 3 BDSG.[1579] Die Unterrichtung über die Funktionen der Signaturkarte und die Rechtsfolgen der elektronischen Signatur hat nach § 6 Abs. 3 Satz 1 SigG durch eine Belehrung in Textform zu erfolgen.[1580]

Der Verzicht auf die (generelle) Schrift- oder Textform der Unterrichtung nach § 6c BDSG war jedoch vom Gesetzgeber gewollt, denn die Begründung spricht davon, es liege „in der Eigenverantwortung des Betroffenen, ihm ausgehändigte Handzettel und Broschüren aufzubewahren bzw. sich Notizen über erfolgte Unterrichtungen zu machen“.[1581] Damit fehlt es an einer Regelungslücke, die für eine Analogie erforderlich wäre.[1582] Eine Analogie zu § 4a Abs. 1 Satz 3 BDSG würde darüber hinaus auch an der Vergleichbarkeit scheitern. § 4a BDSG betrifft eine Erklärung des Betroffenen, während es bei § 6c BDSG um eine Unterrichtungshandlung durch die verpflichtete Stelle geht. Damit bleibt es zunächst beim Grundsatz der Formfreiheit des Verwaltungsverfahrens (§ 37 Abs. 2 Satz 1 VwVfG), beziehungsweise bei der Wahlfreiheit privater Anbieter.

Dies kann sich allerdings anders darstellen, wenn bestimmte Formen der Unterrichtung deren Wirkung gefährden würden. Das Erfordernis der Effektivität der Unterrichtungspflicht gebietet eine Unterrichtung über die Ausübung von Betroffenenrechten nach § 6c Abs. 1 Nr. 3 BDSG in einer Art und Weise, die den Betroffenen in den Stand setzt, zu dem Zeitpunkt auf ihren Inhalt zurückzugreifen, in dem er eines dieser Rechte wahrnehmen möchte. Bei der weitaus größten Zahl mobiler personenbezogener Speicher- und Verarbeitungsmedien kann wegen der Komplexität der Funktionsweise der Karte und der verwendeten Verarbeitungsverfahren und auch wegen des inhaltlichen Umfangs der Unterrichtungspflicht von einer effektiven Information nur gesprochen werden, wenn die Inhalte dem Karteninhaber dauerhaft, das heißt entweder schriftlich oder in Textform (beispiels-

1579 Hingegen wird die Form der Auskunftserteilung im öffentlichen Bereich gemäß § 19 Abs. 1 Satz 4 BDSG von der zuständigen Stelle nach pflichtgemäßem Ermessen bestimmt.

1580 Bis zum Ersten Gesetz zur Änderung des Signaturgesetzes (v. 4.1.2005, BGBl I, 2; dazu unten 5.1.2) war noch eine schriftliche Belehrung erforderlich.

1581 BT-Drs. 14/5793, 64.

1582 Methodisch inkorrekt insoweit Simitis-*Bizer*, § 6c Rn. 35 f., der dennoch eine „Orientierung“ an der Schriftform nach §§ 4a Abs. 1 Satz 4, 34 Abs. 3 BDSG fordert; zutreffend demgegenüber *Schaffland/Wiltfang*, § 6c Rn. 3, die allerdings übersehen, dass in weiten Bereichen dennoch eine Schriftform erforderlich ist (s. dazu im Folgenden); zu den Erfordernissen der rechtlichen Analogiebildung vgl. allgemein *Larenz/Canaris* 1995, 191 ff.; *Pawlowski* 1999, 210 ff.; *Zippelius* 2005, 64 ff.; *Rüthers* 2005, 559 ff.

weise auf einem Datenträger), übergeben werden. Selbst bei sehr simplen Medien ist zumindest die Angabe der Anschrift des Verpflichteten nach § 6c Abs. 1 Nr. 1 BDSG nur dann effektiv, wenn sie auf einem dauerhaften Medium erfolgt.

Dieses Ergebnis ähnelt inhaltlich weitgehend der Auffassung, die Unterrichtung „sollte" auf einem dauerhaften Datenträger ausgehändigt werden beziehungsweise sich an der Schriftform „orientieren".[1583] Im Unterschied zu diesen Zweckmäßigkeitsüberlegungen ergeben sich jedoch aus dem Effektivitätserfordernis zwingende rechtliche Anforderungen an die Form, die die verpflichtete Stelle zu wählen hat.

Für den digitalen Personalausweises und die elektronische Gesundheitskarte gilt danach, dass eine effektive Unterrichtung nur schriftlich oder in Textform vorgenommen werden kann. Dies folgt für die Gesundheitskarte aus der Komplexität der Funktionalitäten und der Handhabung. Ferner ist eine mündliche Unterrichtung unmöglich, falls die Gesundheitskarte wie bisher mit der Post versandt werden sollte. Auch der Personalausweis verfügt über neuartige Verwendungsmöglichkeiten. Insbesondere die Handhabung der biometrischen Systeme und ihre datenschutzrechtlichen Implikationen erfordern eine Unterrichtung, auf die der Betroffene auch nach längerer Zeit noch zurückgreifen kann. Eine einheitlich standardisierte Unterrichtungsbroschüre ist auch im Interesse der ausgebenden Stellen. Überdies wäre es unter Gleichheitsgesichtspunkten bedenklich, nicht jedem Bürger dieselben Informationen über den neuen Personalausweis und die elektronische Gesundheitskarte zukommen zu lassen. Das ist aber nur durch die Schrift- oder Textform der Darstellung zu gewährleisten.

Der Zeitpunkt der Unterrichtung wird in § 6c BDSG nicht genannt. Ihrem Sinn und Zweck nach muss sie aber so früh wie möglich durchgeführt werden. Die spezifischen Eigenschaften von Multiapplikationskarten bringen es mit sich, dass der Betroffene darauf angewiesen ist, von Beginn an über die Funktionsweise und Verarbeitungsmöglichkeiten informiert zu sein. Könnte der Betroffene das Medium vor der Aufklärung bereits nutzen, so würde der Zweck der Norm gefährdet. So werden etwa zusätzliche Funktionen, die ein unabhängiger Dienstleister zu einem späteren Zeitpunkt für das Medium anbietet, je nach dessen Arbeitsweise und bereits vorhandenen Funktionen unterschiedliche datenschutzrechtliche Implikationen mit sich bringen. Deshalb ist der Karteninhaber bei der Entscheidung, ob er die Zusatzfunktion im Hinblick auf diese Implikationen für sich selbst für vertretbar hält, auf die Informationen angewiesen, die ihm nach § 6c Abs. 1 BDSG zur Verfügung gestellt werden müssen. Die Unterrichtung muss damit zum Zeitpunkt der Übergabe des Mediums beziehungsweise der Aufbringung oder Änderung des Verfahrens vorgenommen werden.[1584] Etwas anderes gilt allerdings für das Bereithalten automatisierter Verfahren. Hier kann die Tätigkeit selbst nicht mit einer individuellen Unterrichtung verbunden werden, weil sie sich an eine Vielzahl von Inhabern des jeweiligen Mediums richtet. Die Unterrichtung muss deshalb so erfolgen, dass bei einer Kontaktaufnahme durch den Inhaber die relevanten Informationen zur Verfügung stehen.[1585]

4.3.3.3.5 Anderweitige Kenntnisnahme

Eine Einschränkung der Unterrichtungspflicht enthält § 6c Abs. 1 BDSG am Ende. Danach entfällt die Pflicht, sofern „der Betroffene...bereits Kenntnis erlangt hat". Auf den ersten Blick fällt die sprachliche Parallele zu § 19a Abs. 2 Nr. 1 BDSG und § 33 Abs. 2 Nr.

1583 Simitis-*Bizer*, § 6c Rn. 35 f.
1584 Dies wird für die Übergabe z.B. in § 5b Satz 2 HmbDSG vorgeschrieben.
1585 Insofern lässt sich eine Parallele zur Anbieterkennzeichnung nach § 6 TDG ziehen; s. dazu näher RMD-*Brönneke*, § 6 TDG Rn. 36 ff. m.w.N.

1 BDSG auf, wonach „eine Pflicht zur Benachrichtigung...nicht [besteht], wenn der Betroffene auf andere Weise Kenntnis von der Speicherung oder der Übermittlung erlangt hat". Damit ist jeder Fall erfasst, in dem eine solche Kenntnis auf anderem Wege als durch Benachrichtigung der zuständigen Stelle zustande gekommen ist.[1586] Ausweislich der Gesetzesmaterialien ist dies bei § 6c Abs. 1 BDSG jedoch nicht gemeint.[1587] Dort soll es vielmehr nur darum gehen, bei einer Änderung der angesprochenen Verfahren die Informationspflicht auf den Umfang der Änderung zu beschränken. Damit ist keine erneute umfassende Unterrichtung erforderlich, sondern es obliegt dem Betroffenen, frühere Informationsquellen aufzubewahren.

Angesichts dieser eindeutigen Gesetzesbegründung ist eine andere Interpretation der Einschränkung in § 6c Abs. 1 BDSG nicht möglich.[1588] Eine Verneinung der Unterrichtungspflicht in all den Fällen, in denen der Betroffene auf anderem Wege als durch Unterrichtung der verpflichteten Stelle Kenntnis erlangt hat, würde auch der Eindeutigkeit und Effektivität der Unterrichtung widersprechen und die Anbieter von mobilen Medien und den darauf ablaufenden automatisierten Verarbeitungsverfahren unnötig aus ihrer Informationspflicht entlassen. Das ändert aber nichts daran, dass die Gesetzesformulierung missglückt ist. Sowohl die sprachliche Fassung der Einschränkung selbst als auch die Gesetzessystematik lassen den gesetzgeberischen Willen nicht erkennen, sondern deuten eher auf eine Auslegung der „anderweitigen Kenntnisnahme" entsprechend der zu § 19a Abs. 2 Nr. 1 BDSG und § 33 Abs. 2 Nr. 1 BDSG hin. § 6c Abs. 1 BDSG sollte deshalb im Wege der Gesetzesänderung klargestellt werden.

4.3.3.4 Sonstige Pflichten (§ 6c Abs. 2 und 3 BDSG)

Bei mobilen personenbezogenen Speicher- und Verarbeitungsmedien hat der Karteninhaber zwar die physische Verfügungsgewalt über den Datenträger, er ist aber regelmäßig nicht dazu in der Lage, den Inhalt der gespeicherten Daten zu erkennen.[1589] Deshalb hat gemäß § 6c Abs. 2 BDSG die nach § 6c Abs. 1 BDSG verpflichtete Stelle die Pflicht, Geräte oder Einrichtungen[1590] für die Wahrnehmung des allgemeinen Auskunftsrechts in angemessenem Umfang kostenlos zur Verfügung zu stellen.

§ 6c Abs. 2 BDSG normiert zwar keinen eigenen Auskunftsanspruch, sondern bezieht sich auf die Rechte aus §§ 19 und 34 BDSG[1591] und spezielle Ansprüche (beispielsweise § 3 Abs. 5 Satz 2 PersAuswG und § 291a Abs. 4 Satz 2 SGB V[1592]). Die Regelung führt aber zu einer gewichtigen Verschiebung der Verantwortlichkeiten. Die Auffassung, die Geräte seien „durch die verantwortliche Stelle" bereitzustellen,[1593] ist nämlich nicht zutreffend.

1586 *Gola/Schomerus*, § 33 Rn. 29; Simitis-*Mallmann*, § 33 Rn. 47 f. Erfasst ist auch die Kenntnis durch Mitteilung von dritter Seite. Nach tlw. vertretener Auffassung soll sogar darauf abgestellt werden, ob bei Betroffenen Kenntnis vorhanden sein müsste, s. *Gola/Schomerus*, § 33 Rn. 29; *Schaffland/Wiltfang*, § 33 Rn. 39; einschränkend demgegenüber Simitis-*Mallmann*, § 33 Rn. 49 m.w.N.

1587 Vgl. BT-Drs. 14/5793, 64.

1588 S.a. *Gola/Schomerus*, § 6c Rn. 8; a.A. anscheinend *Bizer* (2002, 31), der die Einschränkung wegen der Beweispflicht der ausgebenden und Daten verarbeitenden Stelle über den Umstand der anderweitigen Kenntniserlangung für praktisch folgenlos hält. Das kann sich nur auf eine anderweitige Kenntnisnahme außerhalb eines früheren Informationsakts beziehen, weil dieser durch die Behörde leicht beweisbar ist.

1589 Simitis-*Bizer*, § 6c Rn. 3; allgemein *Weichert*, DuD 1997, 266, 267 und 271.

1590 Näher zu diesem Begriff Simitis-*Bizer*, § 6c Rn. 61 ff.

1591 S. dazu unten 4.3.7.

1592 Diese Regelung beinhaltet trotz ihres missverständlichen Wortlauts für die überwiegende Zahl der Anwendungen kein technisches Zugriffs-, sondern lediglich ein Auskunftsrecht, s.u. 4.3.7.3.

1593 So *Schaffland/Wiltfang*, § 6c Rn 6.

Der Begriff der verantwortlichen Stelle wird in § 3 Abs. 7 BDSG legaldefiniert als „jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt“. Dies kann, muss jedoch nicht die Stelle sein, die das Medium ausgibt. § 6c Abs. 2 BDSG verpflichtet überdies auch Stellen, die Verfahren auf das Medium aufbringen, auf diesem ändern oder hierzu bereithalten. Diese werden sogar regelmäßig nicht mit der verantwortlichen Stelle identisch sein.

Während die verantwortliche Stelle im Sinne von § 3 Abs. 7 BDSG nach wie vor für die Realisierung des Auskunftsrechts des Betroffenen verantwortlich ist, verpflichtet § 6c Abs. 2 BDSG die Medien ausgebende oder mit einem Verfahren befasste Stelle dazu, die infrastrukturellen Voraussetzungen für die Wahrnehmung des Auskunftsrechts zu schaffen. Je nach Medium und Verfahren können hiermit erhebliche finanzielle Belastungen verbunden sein. Das betrifft insbesondere die Stelle, die das Medium ausgibt, weil sie Geräte und Einrichtungen für alle Verfahren, die auf diesem ablaufen, zur Verfügung stellen muss. Dagegen sind Stellen, die nur mit einem einzigen Verfahren auf dem Medium befasst sind, auch nur insoweit verpflichtet, die technischen Voraussetzungen zu schaffen. Schließlich muss § 6c Abs. 2 BDSG – entsprechend der Unterrichtungspflicht nach § 6c Abs. 1 BDSG[1594] – einschränkend dahingehend interpretiert werden, dass Stellen, die vor der Ausgabe des Mediums im Rahmen des Herstellungsprozesses Verfahren auf dieses aufbringen, nicht selbst für die technische Infrastruktur zur Umsetzung des Auskunftsrecht verantwortlich sind. Sie sind allerdings in angemessenem Umfang zu Hinweisen und zur Mitwirkung verpflichtet, falls dies erforderlich ist.

Die Unentgeltlichkeit der Auskunft ist bereits im Zusammenhang mit den Auskunftsrechten normiert, auf die sich § 6c Abs. 2 BDSG bezieht.[1595] § 6c Abs. 2 BDSG stellt aber klar, dass dies auch dann gilt, wenn zur Wahrnehmung des Auskunftsrechts (möglicherweise teure) Geräte oder Einrichtungen erforderlich sind.[1596] Deren Kosten gehen damit zu Lasten der nach § 6c Abs. 1 BDSG verpflichteten Stelle. Letztlich wird allerdings im Regelfall die Gesamtheit der Betroffenen die Kosten für die Geräte und Einrichtungen tragen, da die verpflichtete Stelle diese über Gebühren oder Preise auf die Anschaffungs- oder laufenden Kosten abwälzen wird. Dennoch ist die Kostenfreiheit des individuellen Informationsvorgangs wichtig, da der Berechtigte sonst von der Ausübung seines Rechtes abgeschreckt werden könnte.

Mit der Beschränkung, dass Geräte und Einrichtungen „in angemessenem Umfang“ zur Verfügung zu stellen sind, wird auf den konkreten Einzelfall verwiesen. Dabei können Faktoren wie die Sensibilität der betroffenen personenbezogenen Daten, der wirtschaftliche Aufwand der Auskunftserteilung, die Verbreitung eines Verfahrens und der technischen Fortschritt in die Bewertung mit einfließen.[1597] Eine Ausgabe entsprechender Lesegeräte an die Betroffenen ist möglich,[1598] kann aber aus § 6c Abs. 2 BDSG nicht beansprucht werden.[1599]

Für den digitalen Personalausweis bedeutet dies, dass die Personalausweisbehörde und alle weiteren nach § 6c Abs. 1 BDSG beteiligten Stellen für die entsprechenden Geräte oder Einrichtungen verantwortlich sind. Dies kann etwa durch ein Vorhalten von Lesegeräten bei der Personalausweisbehörde geschehen, wobei die Geräte entweder in öffentlich

1594 S. ausführlich oben 4.3.3.3.1.
1595 §§ 19 Abs. 7, 34 Abs. 5 Satz 1 BDSG.
1596 Dies war wohl schon nach alter Rechtslage der Fall, s. *Weichert*, DuD 1997, 266, 275. Auch dieser forderte allerdings eine entsprechende gesetzliche Regelung, vgl. ebd., 277.
1597 S. die Gesetzesbegründung, BT-Drs. 14/5793, 64; ebenso Simitis-*Bizer*, § 6c Rn. 66 ff.
1598 *Gola/Schomerus*, § 6c Rn. 9.
1599 So die Begründung, BT-Drs. 14/5793, 64.

zugänglichen Bereichen oder im internen Bereich installiert werden können. Im letzteren Fall würden die Daten ausgelesen und dem Karteninhaber übermittelt. Darüber hinaus wäre es aber durchaus denkbar, an zentralen Orten öffentliche Computerterminals zu installieren, die eine Abfrage ermöglichen.[1600] Bei der elektronischen Gesundheitskarte müssen die Krankenkassen und die Anbieter der automatischen Verfahren, die auf der Karte ablaufen, für die Umsetzung des Auskunftsrechts sorgen. Auch hier gibt es unterschiedliche Varianten. Möglich wäre eine Auskunft bei den Leistungserbringern, wobei aufgrund der Kostenfreiheit nach § 6c Abs. 2 BDSG hierbei die sonst übliche Praxisgebühr (§ 28 Abs. 4 SGB V) entfallen müsste.[1601] Alternativ wären Terminals in Arztpraxen oder in Zweigstellen der Krankenkassen denkbar. Diese werden von § 6c Abs. 2 BDSG aber nicht zwingend gefordert. Die Norm fordert nur eine effektive Wahrnehmungsmöglichkeit für das Auskunftsrecht, nicht jedoch die eigene technische Zugriffsmöglichkeit.[1602]

Am Beispiel der elektronischen Gesundheitskarte wird gleichzeitig eine Besonderheit der Infrastrukturverantwortung der Stelle nach § 6c Abs. 1 BDSG deutlich. Sie kann mitunter für die Auskunft über Daten verantwortlich sein, über die sie selbst nicht verfügt. Dies darf nicht zu einem unkontrollierten Datenfluss führen. So müssen die Krankenkassen Geräte und Einrichtungen zur Auskunft über Gesundheitsinformationen bereitstellen. Das bedeutet aber nicht, dass die Kassen nunmehr berechtigt wären, die Daten zuerst zu erlangen, um sie dann an den Versicherten weiterzugeben. Die Beschränkungen der Datenübermittlung zwischen Leistungserbringern und Krankenkassen werden durch § 6c Abs. 2 BDSG nicht berührt; die Norm verpflichtet lediglich dazu, technische Voraussetzungen zu schaffen.

Normiert § 6c Abs. 1 BDSG lediglich eine einmalige Informationspflicht, so muss nach § 6c Abs. 3 BDSG jeder Kommunikationsvorgang, der auf dem Medium eine Datenverarbeitung auslöst, für den Betroffenen eindeutig erkennbar sein.[1603] Rechtswidrig wäre danach etwa eine Datenverarbeitung, die ohne Kenntlichmachung, zum Beispiel beim Vorbeilaufen an einem Terminal, erfolgt.[1604] Dies kann bei Chipkartenausweisen insbesondere dann problematisch sein, wenn mit kontaktlosen Schnittstellen gearbeitet wird.

Art und Weise der Erkennbarkeit werden in § 6c Abs. 3 BDSG nicht normiert. Im Unterschied zu § 6c Abs. 1 BDSG wird man keine Erklärung in Textform verlangen können. Zumindest sind jedoch optische oder akustische Signale erforderlich, die auch eine Barrierefreiheit gewährleisten. Sie müssen den Kommunikationsvorgang so begleiten, dass ein Abbruch des Geschehensablaufs noch möglich ist. Wenn durch den Verarbeitungsvorgang dauerhaft Daten auf dem Medium geändert wurden, hat der Betroffene die Möglichkeit, sich über seinen Auskunftsanspruch hiervon Kenntnis zu verschaffen.[1605]

4.3.4 Besondere Arten personenbezogener Daten

4.3.4.1 Begriff und besondere Anforderungen

Das Bundesdatenschutzgesetz stellt erhöhte Anforderungen an besondere Arten von personenbezogenen Daten. Dies sind nach der Definition in § 3 Abs. 9 BDSG „Angaben

1600 Ein solches Verfahren gibt es etwa in Hongkong und wird für Belgien geplant, s.o. 3.2.2.3; 3.2.1.3.
1601 S.a. unten 4.3.7.3.
1602 A.A. *Schneider* 2004, 154 f.
1603 Dies wurde bereits vor Einführung von § 6c Abs. 3 BDSG de lege lata angenommen von *Weichert*, DuD 1997, 266, 274. Auch dieser forderte allerdings (ebd., 276) eine gesetzliche Klarstellung.
1604 So ausdrücklich die Gesetzesbegründung, BT-Drs. 14/5793, 64.
1605 Simitis-*Bizer*, § 6c Rn. 72.

über die rassische und ethnische Herkunft, politische Meinungen, religiöse und philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit und Sexualleben". Sie werden in der Literatur abkürzend als „sensible" oder „sensitive" Daten bezeichnet.[1606]

Die generelle Einstufung bestimmter Daten als besonders schutzwürdig entspricht den Richtlinien der Generalversammlung der Vereinten Nationen, die in Nr. 5 fordern, Angaben über rassische und ethnische Herkunft, Hautfarbe, Sexualleben, politische Anschauungen, religiöse, weltanschauliche und andere Überzeugungen sowie die Mitgliedschaft in einer Vereinigung oder Gewerkschaft nicht zu erfassen. Außerdem gibt die europäische Datenschutzrichtlinie in Art. 8 Abs. 1 exakt den Katalog von Daten vor, den auch § 3 Abs. 9 BDSG umfasst.[1607] Auch Art. 6 des Übereinkommens des Europarats fordert einen „geeigneten Schutz" für Daten über die rassische Herkunft, politische Anschauungen, religiöse oder andere Überzeugungen, die Gesundheit und das Sexualleben.[1608] Auffällig ist auch die Parallele zu den besonderen Diskriminierungsverboten in Art. 14 EMRK. Schließlich kennen die Datenschutzgesetze einer Vielzahl von Mitgliedstaaten der Europäischen Union ebenfalls derartige Sonderregeln.[1609]

Die Bildung von Datenkategorien, die unterschiedlichen Schutz genießen, steht im Widerspruch zur Grundkonzeption des deutschen Datenschutzrechts.[1610] Das Bundesverfassungsgericht formulierte bereits im Volkszählungsurteil, dass es unter den Bedingungen moderner Datenverarbeitung kein „belangloses Datum" mehr geben könne.[1611] Der Schutzbereich des Rechts auf informationelle Selbstbestimmung ist danach nicht daten-, sondern verarbeitungsbezogen zu bestimmen.[1612] Die Regelung besonderer Arten von Daten ist deshalb ein Fremdkörper im deutschen Datenschutzrecht; die Aufzählung in Art. 8 Abs. 1 DSRL und § 3 Abs. 9 BDSG lässt sich überdies mit einiger Berechtigung als „willkürlich, antiquiert und unvollständig"[1613] kritisieren. Allerdings enthält die Datenschutzrichtlinie Ausnahmen von den Verwendungsbeschränkungen, die durchweg in das deutsche Recht übernommen worden sind. Diese Ausnahmen hingegen berücksichtigen letztlich doch den jeweiligen Verarbeitungskontext. Im Ergebnis sind die Unterschiede

---

1606 In dieser Arbeit wird der Begriff „sensibel" verwendet, der näher am allgemeinen Sprachgebrauch liegt; ebenso bspw. *Gounalakis/Mand*, CR 1997, 431, 437; anders die wohl überwiegende Zahl der Verfasser, s. z.B. Simitis-*Simitis*, § 3 Rn. 257 ff.; *ders*. 1990, 469 ff.; *Roßnagel/Pfitzmann/Garstka* 2001, 24, 62, 201; *Der Berliner Beauftragte für Datenschutz*, RDV 2003, 308; *Gola/Schomerus*, § 13 Rn. 13. Der Gebrauch des Terminus „sensitiv" könnte der internationalen Diskussion entspringen. Diese wird in der Regel in englischer Sprache geführt, in welcher die Bedeutung des Wortes „sensitive" dem deutschen „sensibel" entspricht. Die Frage ist indes rein terminologischer Art.

1607 Dazu *Ehmann/Helfrich* 1999, Art. 8 Rn. 5 ff. Allerdings wurde Art. 8 Abs. 5 DSRL (Daten über Straftaten, strafrechtliche Verurteilungen und Sicherungsmaßregeln) nicht aufgenommen, s. Roßnagel-*Schild*, Kap. 4.2, Rn. 54. Insoweit bestehen aber Sonderregeln in §§ 28 Abs. 3 Nr. 4, 35 Abs. 1 Satz 2 Nr. 2 BDSG.

1608 Näher *Henke* 1986, 112 ff.; *Simitis* 1990, 469; Simitis-*Simitis*, Einl. Rn. 153. Nach Erwägungsgrund 11 der DSRL konkretisiert und erweitert die Richtlinie die Grundsätze des Übereinkommens.

1609 S. *Simitis* 1990, 469 ff.; *Geis*, CR 1995, 171, 173 ff.; speziell zur Situation in Großbritannien (vgl. s.2 Data Protection Act 1998) s. *Jay/Hamilton* 2003, 188 ff.

1610 Simitis-*Simitis*, § 3 Rn. 257 ff.; *Dammann/Simitis* 1997, Art. 8 Rn. 3 ff.; *Geis*, CR 1995, 171, 173 f.; *Gola*, RDV 2001, 125, 126; *Gounalakis/Mand*, CR 1997, 431, 437 f.; *Roßnagel/Pfitzmann/Garstka* 2001, 61 ff.; *Ehmann/Helfrich* 1999, Art. 8 Rn. 8; *Der Berliner Beauftragte für Datenschutz*, RDV 2003, 308.

1611 BVerfGE 65, 1 (45).

1612 S. schon *Simitis*, DVR 1973, 138, 143 ff.; *ders*., NJW 1984, 394, 402; *Denninger*, KJ 1985, 215, 220; *Konferenz der Datenschutzbeauftragten*, DÖV 1984, 504, 505; AK GG-*Podlech* (2. Auflage 1989), Art. 2 Abs. 1 Rn. 37.

1613 Simitis-*Simitis*, § 3 Rn. 265; s.a. Simitis-*Sokol*, § 13 Rn. 33 m.w.N.; *Duhr/Naujok/Peter/Seiffert*, DuD 2002, 5, 10 f.; *Geis*, CR 1995, 171, 174.

zwischen den beiden Konzepten daher weit weniger relevant, als es zunächst den Anschein hat.[1614]

Unabhängig von diesen Fragen ist indes bei der Analyse de lege lata von den besonderen Anforderungen des Bundesdatenschutzgesetzes auszugehen. Die Tatbestandsmerkmale des § 3 Abs. 9 BDSG sind dabei weit auszulegen.[1615] Insbesondere kann sich die Eigenschaft als „besondere Art personenbezogener Daten" auch mittelbar aus dem Gesamtzusammenhang ergeben.[1616]

Für die in § 3 Abs. 9 BDSG genannten Arten von Daten besteht eine Reihe von Verwendungsbeschränkungen. Die Einwilligung in die Erhebung, Verarbeitung oder Nutzung der Daten hat sich nach § 4a Abs. 3 BDSG ausdrücklich auch auf diese Form der Daten zu beziehen. Daneben gibt es Beschränkungen für die Erhebung, Verarbeitung und Nutzung in den §§ 13 Abs. 2, 14 Abs. 5 und Abs. 6, 16 Abs. 1 Satz 2 BDSG (öffentliche Stellen) beziehungsweise §§ 28 Abs. 6 bis 9, 29 Abs. 5, 30 Abs. 5 BDSG (nicht-öffentliche Stellen).

4.3.4.2 Anwendung auf Chipkartenausweise

4.3.4.2.1 Digitaler Personalausweis

Beim digitalen Personalausweis ist insbesondere zu klären, inwieweit biometrische Daten besondere Arten personenbezogener Daten sind. Das gilt zunächst für das Gesicht, weil sich aus ihm Angaben über die rassische und ethnische Herkunft ergeben.[1617] Fingerabdruck und Iris können demgegenüber die bereits erwähnten Angaben über die Gesundheit enthalten.[1618] Mitunter wird sogar ein Zusammenhang zwischen Fingerabdrucksmuster und Homosexualität behauptet.[1619] Dieser sollte allerdings außer Betracht bleiben, solange völlig ungesichert ist, welchen Einfluss angeborene Faktoren einerseits und Sozialisationseffekte andererseits in diesem Zusammenhang haben.[1620] Die Darstellung beschränkt sich deshalb im Folgenden auf den Zusammenhang mit Gesundheitsinformationen, die in biometrischen Daten enthalten sein können.

Besonderheiten können sich für Templates ergeben.[1621] Nicht zutreffend ist allerdings, dass diese niemals derartige Zusatzinformationen enthalten.[1622] Die Eigenschaft als beson-

---

1614 S. *Dammann/Simitis* 1997, Einl. Rn. 45; Simitis-*Simitis*, § 3 Rn. 260; *Gola/Schomerus*, § 13 Rn. 13. Auch ausländische Datenschutzgesetze enthalten regelmäßig Ausnahmeregelungen, s. *Simitis* 1990, 476.

1615 S. für den Begriff der „Gesundheit" nach der DSRL EuGH, Rs. C-101/01 – Lindqvist ./. Schweden, MMR 2004, 95, 96 (zu der Entscheidung vgl. *Brühann*, DuD 2004, 201 ff.; *Taraschka*, CR 204, 280 ff.; *Siemen*, EuR 2004, 306, 317 ff.).

1616 *Gola/Schomerus*, § 3 Rn. 56a; Simitis-*Simitis*, § 3 Rn. 270; *Meier* 2003, 58 f.

1617 Zwar zeigt sich an dieser Stelle, dass ein genereller Schutz derartiger Daten wenig sinnvoll ist, weil er zu besonderen Anforderungen bei Angaben führen kann, die jedermann in seinem Umfeld wahrnimmt. So ist die automatisierte biometrische Verwendung von Gesichtsdaten zwar grundsätzlich problematisch (s.o. 4.2.2.4.1.2), die Verwendung im Rahmen von Sichtkontrollen jedoch weit weniger. Die gesetzlichen Bestimmungen sind aber eindeutig.

1618 S.o. 4.2.2.4.1.2.

1619 S. *Hall*/*Kimura*, Behavioral Neuroscience 1994, 1203 ff. Dabei wurden die Fingerabdrucksmuster von 182 hetero- und 66 homosexuellen Männern verglichen und ein statistisch signifikanter Zusammenhang zwischen einer bestimmten Musterform und der sexuellen Orientierung festgestellt; s.a. LeVay 1996, 157 f.

1620 S. dazu bspw. *Wintemute* 1995, 15 ff. et passim; *Koppelman*, Michigan Law Review 1997, 1636 ff.; *Halley*, Stanford Law Review 1994, 503 ff.; *Stein* 1999, 93 ff., 119 ff.

1621 Das gilt, sofern man – wie im Rahmen dieser Arbeit – unter diesem Terminus ausschließlich extrahierte Daten und nicht auch standardisierte Volldatensätze versteht; s. zur Terminologie oben 2.3.3.2.

deres Datum scheidet nur dann aus, wenn bei ihrer Berechnung die Datenteile, die Informationen im Sinne des § 3 Abs. 9 BDSG enthalten, vollständig entfernt werden. Dagegen können jedenfalls stabile Zusatzinformationen – beispielsweise chronische Krankheiten – durchaus in der Template-Struktur enthalten sein.[1623] Auch wenn das nicht der Fall ist, arbeitet das Gesamtsystem immer dann mit besonderen Arten personenbezogener Daten, wenn beim Matching Rohdaten erhoben werden, die Zusatzinformationen enthalten.

Problematisch ist, dass die Zusammenhänge zwischen biometrischen Daten und Gesundheitsinformationen wissenschaftlich umstritten sind und immer nur Aussagen mit einer gewissen Wahrscheinlichkeit getroffen werden können. Hierzu wird vertreten, die Sondervorschriften über besondere Arten personenbezogener Daten seien bereits dann unanwendbar, wenn Zweifel über den Zusammenhang eines Datums mit einer der in § 3 Abs. 9 BDSG genannten Kategorien bestehen[1624] beziehungsweise aus einem Datum „nur mit einer statistischen Wahrscheinlichkeit" derartige Rückschlüsse gezogen werden können.[1625] Ob dies zutreffend ist, muss vom Schutzzweck der Regelungen her bestimmt werden. Verhindert werden soll, dass dem Betroffenen aufgrund der besonderen Sensibilität der in den Daten enthaltenen Informationen Nachteile zugefügt werden. Das Gemeinsame an den Kategorien des Katalogs ist gerade, dass bei ihnen in besonderer Weise die Gefahr diskriminierender Verwendung besteht.[1626] Für eine Diskriminierung genügt es jedoch, dass aus einem Datum mit einer hinreichenden Wahrscheinlichkeit auf eine Krankheit geschlossen werden kann. Sofern ein derart hoher statistischer Zusammenhang vorliegt, ist ein Datum als besondere Art personenbezogener Daten zu qualifizieren.

Die gegenteilige Auffassung ist vom Versuch geprägt, auch im Rahmen von § 3 Abs. 9 BDSG den konkreten Verwendungszusammenhang zum Maßstab zu machen. Bezeichnend sind etwa Formulierungen, es komme darauf an, ob die „Sensitivität" eines Datums für die verantwortliche Stelle „zufällig" sei oder diese die Daten gezielt auf „sensitive Reflexe" hin untersuche.[1627] Das mag in der Tat „sachgerecht" sein, widerspricht aber sowohl der Zielrichtung der Datenschutzrichtlinie als auch dem Wortlaut von § 3 Abs. 9 BDSG. De lege lata besteht gerade kein Unterschied nach dem Zweck der Verwendung. Die Auslegung des deutschen Rechts hat sich vielmehr eng an die Datenschutzrichtlinie anzulehnen.[1628]

Im Ergebnis genügt ein hinreichend wahrscheinlicher Zusammenhang mit einer Krankheit oder anderen in § 3 Abs. 9 BDSG genannten Information. Daran darf sich nichts ändern, wenn wissenschaftliche Zweifel am Informationsgehalt bestehen, denn der Betroffene muss damit rechnen, dass Dritte den Zusammenhang dennoch für gegeben halten und ihm hierdurch Nachteile widerfahren. Hier kommt es allerdings auf den Grad der Zweifel an. Nicht jeder bloß behauptete Zusammenhang eines Datums mit einer der Kategorien in § 3 Abs. 9 BDSG kann dazu führen, dieses den Sonderregeln über besondere Arten von Daten zu unterwerfen.[1629]

1622 So aber *Bäumler/Gundermann/Probst* 2001, 19; Roßnagel-*Gundermann/Probst*, Kap. 9.6, Rn. 68; *Albrecht* 2003a, 174; s. hierzu oben 4.2.2.4.2.

1623 Vgl. *Bromba* 2003.

1624 Simitis-*Simitis*, § 3 Rn. 272.

1625 *Der Berliner Beauftragte für Datenschutz*, RDV 2003, 308, 309.

1626 *Dammann/Simitis* 1997, Art. 8 Rn. 6; Simitis-*Simitis*, § 3 Rn. 264; Simitis-*Sokol*, § 13 Rn. 33; *Tinnefeld*, NJW 2001, 3078, 3082; *Der Berliner Beauftragte für Datenschutz*, RDV 2003, 308.

1627 *Der Berliner Beauftragte für Datenschutz*, RDV 2003, 308, 309.

1628 Simitis-*Sokol*, § 13 Rn. 33.

1629 Das gilt etwa für den Zusammenhang zwischen Fingerabdruck und Homosexualität (s.o. Fn. 1620), der eher zweifelhaft sein dürfte.

Biometrische Daten von Gesicht, Fingern und Iris sind danach – mit Ausnahme von Templates, aus denen die entsprechenden Zusatzinformationen endgültig entfernt wurden – als besondere Arten personenbezogener Daten einzustufen.[1630] Ihre Verwendung durch öffentliche Stellen richtet sich damit an sich nach den §§ 13 Abs. 2, 14 Abs. 5 und Abs. 6 BDSG. Beim digitalen Personalausweis besteht jedoch die Besonderheit, dass bereits aufgrund der rechtsstaatlichen Anforderungen des Gesetzesvorbehalts und des Bestimmtheitsgrundsatzes eine genaue gesetzliche Regelung über die Erhebung, Verarbeitung und Nutzung der Daten erforderlich ist.[1631] Aus europarechtlicher Sicht sind derartige Spezialregelungen zur Verwendung besonderer Arten personenbezogener Daten Ausnahmen nach Art. 8 Abs. 4 DSRL. Gemäß Art. 8 Abs. 6 DSRL besteht für sie eine Mitteilungspflicht an die Kommission. Da die Richtlinie jedoch für den Bereich des Personalausweisrechts nicht anwendbar ist,[1632] entfällt diese Pflicht für den Personalausweis.[1633]

Gegenüber der noch zu schaffenden spezialgesetzlichen Regelung zur Verwendung von Biometrie im Personalausweis wäre das Bundesdatenschutzgesetz nach § 1 Abs. 3 Satz 1 BDSG subsidiär, sodass es auf die Sonderbestimmungen zu besonderen Arten personenbezogener Daten nicht ankommt.

4.3.4.2.2 Elektronische Gesundheitskarte

Auch bei der elektronischen Gesundheitskarte werden besondere Arten personenbezogener Daten verarbeitet. Hier besteht eine erhebliche Gefährdungslage wegen der Vielzahl von Informationen über den Gesundheitszustand des jeweiligen Versicherten.[1634] Der Begriff des Datums über die Gesundheit ist grundsätzlich umfassend zu verstehen. Er schließt bereits die Tatsache eines Arztbesuches ein,[1635] wie auch die Angabe einer Erkrankung, den Namen des behandelnden Arztes und die Heilungskosten.[1636] Auch in Art. 8 Abs. 1 DSRL ist nach der Rechtsprechung des Europäischen Gerichtshofs der „Begriff `Daten über die Gesundheit` in dem Sinne weit auszulegen, dass er sich auf alle Informationen bezieht, die die Gesundheit einer Person unter allen Aspekten – körperlichen wie psychischen – betreffen".[1637] In richtlinienkonformer Auslegung[1638] gilt dies auch für § 3 Abs. 9 BDSG.

Die ganz überwiegende Zahl der Angaben, die nach § 291a Abs. 3 Satz 1 SGB V im Rahmen der freiwilligen Funktionen verwendet werden, stellen damit besondere Arten personenbezogener Daten dar. Das gilt auch für die Patientenquittung nach § 291a Abs. 3 Satz 1 Nr. 6 SGB V, weil in ihr Behandlungsfälle dokumentiert werden. Vom Versicherten selbst zur Verfügung gestellte Daten sind differenziert zu beurteilen. Der Organspende-

1630 S.a. *Art. 29 DPWP* 2003, 10.
1631 S.o. 4.2.2.2.
1632 S.o. 4.1.1.1 a.E. Das bedeutet allerdings nicht, dass die einfachgesetzlichen Bestimmungen, die die Richtlinie im BDSG umsetzen, nicht anwendbar wären.
1633 Dies würde sich für den Einsatz von Biometrie in anderen hoheitlichen Bereichen anders darstellen.
1634 Man kann in den Daten, die im Gesundheitswesen anfallen, sogar die sensibelsten Daten überhaupt sehen, vgl. *Kilian* 1979, 119 m.w.N.
1635 *Der Berliner Beauftragte für Datenschutz*, RDV 2003, 308, 309. Das entspricht dem Schutzbereich von § 203 StGB, s.o. 4.2.3.5.1.
1636 Simitis-*o.V.*, § 14 Rn. 117.
1637 EuGH, Rs. C-101/01 – Lindqvist/Schweden, MMR 2004, 95, 96; zu dieser weiten Auslegung s. *Roßnagel*, MMR 2004, 99; *Brühann*, DuD 2004, 201, 202.
1638 S.o. Einl. zu 4.1.1.

ausweis enthält beispielsweise keine Informationen über die Gesundheit.[1639] Die Protokolldaten über die Zugriffe auf die elektronische Gesundheitskarte (§ 291a Abs. 6 Satz 2 SGB V) sind dagegen besondere Arten personenbezogener Daten, da aus ihnen Untersuchungs- und Behandlungsabläufe rekonstruiert werden können.

Hinsichtlich der verpflichtenden Applikationen erfasst § 3 Abs. 9 BDSG das elektronische Rezept.[1640] Aus einer Verschreibung können nämlich unmittelbare Rückschlüsse auf die Gesundheit gezogen werden.[1641] Keine Angaben über die Gesundheit enthält dagegen der europäische Berechtigungsnachweis nach § 291a Abs. 2 Satz 1 Nr. 2 SGB V. Auch die Versicherungsstammdaten in ihrer bisherigen Form fallen nicht darunter. Aus der bloßen Tatsache des Bestehens eines Versicherungsverhältnisses kann nicht auf die Gesundheit des Versicherten geschlossen werden.

Allerdings ergeben sich aufgrund der Neuerungen des GKV-Modernisierungsgesetzes zwei Probleme. Zunächst wird die Gesundheitskarte nach § 291 Abs. 2 SGB V – außer bei Versicherten bis zum 16. Lebensjahr und Personen, deren Mitwirkung bei der Erstellung des Lichtbildes nicht möglich ist – mit einem Photo versehen werden. Diese umstrittene[1642] Neuerung bringt ähnlich wie beim digitalen Personalausweis die Verwendung eines Datums mit sich, das Angaben über die ethnische und rassische Herkunft enthält.

Daneben werden die Versicherungsstammdaten nach § 291 Abs. 2 Satz 1 Nr. 8 SGB V um eine Angabe über den Zuzahlungsstatus erweitert. Diese ist in jedem Fall personenbezogen; fraglich ist aber, ob es sich um eine Angabe über die Gesundheit handelt. Da eine solche auch vorliegen kann, wenn lediglich ein mittelbarer Schluss auf den Zustand des Versicherten möglich ist, kommt es auf die Voraussetzungen der Befreiung von der Zuzahlung an.

Nach dem neuen § 62 SGB V gibt es keine vollständige Befreiung von Zuzahlungen mehr.[1643] Bei Sonderregelungen für die Bestimmung des Bruttoeinkommens gilt künftig im

---

1639 Nach der Allgemeinen Verwaltungsvorschrift über die Festelegung eines Musters für einen Organspendeausweis v. 29.5.1998 (BAnz. Nr. 103a v. 6.6.1998) enthält dieser Namen, Geburtstag und Adresse sowie Angaben über zu entnehmende Organe oder eine Vertrauensperson, der die Entscheidung übertragen wurde.

1640 Nicht zutreffend ist damit die Angabe der Bundesregierung, das „Erheben, Verarbeiten und Nutzen von medizinischen Daten mittels der elektronischen Gesundheitskarte [ist] nur mit dem Einverständnis des Versicherten…zulässig“ (s. die Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten *Sehling*, *Storm*, *Widmann-Mauz*, weiterer Abgeordneter und der Fraktion der CDU/CSU v. 30.3.2004, BT-Drs 15/2810, 16; ähnlich *Bales/Holland* 2004, 16; *Grätzel v. Grätz* 2004c, 126). Beim elektronischen Rezept handelt es sich sehr wohl um ein medizinisches Datum.

1641 Simitis-*Simitis*, § 3 Rn. 267.

1642 Nach *Dämmer/Männel*, BKK 2003, 279, 284 f. kostet die Einführung des Lichtbildes mehrere hundert Mio. Euro. Ähnliche Äußerungen kamen im Frühjahr 2005 vom Vorstandsvorsitzenden der Kaufmännischen Krankenkasse, *Kailuweit* (250 Mio. Euro, s. http://www.heise.de/newsticker/meldung/58304). In Österreich wurde aus Kostengründen auf das Bild verzichtet, s. ebd. Die genaue Höhe der Kosten dürfte schwer abschätzbar sein. Richtig ist allerdings, dass alternativ auch eine kumulative Verwendung von Gesundheitskarte und Personalausweis in Frage käme. In diesem Fall könnte auf das Lichtbild verzichtet werden. Dagegen geht das Argument, ein Jugend-Lichtbild entspreche nicht dem Stand biometrisch zuverlässiger Erkennung (*Dämmer/Männel*, BKK 2003, 279, 284 f.), angesichts der bisherigen Gültigkeit der Krankenversichertenkarte von wenigen Jahren an der Sache vorbei.

1643 Nach alter Rechtslage erfolgte eine vollständige Befreiung nach § 61 SGB V a.F. bei unzumutbarer Belastung, die bei Bruttoeinnahmen unter 40 % der Bezugsgröße nach § 18 SGB IV, beim Bezug von Hilfe zum Lebensunterhalt, Arbeitslosenhilfe und Ausbildungsförderung und bei einer von einem Sozialhilfeträger finanzierten Heimunterbringung angenommen wurde. Eine teilweise Befreiung bedeutete nach § 62 SGB V a.F. die Befreiung jenseits einer Belastungsgrenze. Diese betrug im Regelfall 2 % des Bruttojahreseinkommens. Bei chronisch Kranken entfielen die Zuzahlungen für die chronische Krankheit, sobald ein Jahr lang 1 % des Einkommens aufgewendet wurde.

Regelfall eine Belastungsgrenze von 2 % des Bruttojahreseinkommens. Für chronisch Kranke beträgt diese 1 %.[1644] Sobald die Zuzahlungen in einem Kalenderjahr die individuelle Belastungsgrenze erreicht haben, stellen die Krankenkassen nach § 62 Abs. 1 Satz 1, 2. Halbsatz SGB V eine Bescheinigung darüber aus, dass für den Rest des Jahres keine Zuzahlungen mehr zu leisten sind. Gemäß § 292 Abs. 2 Nr. 8 SGB V wird diese Information als „Zuzahlungsstatus" auf der Gesundheitskarte gespeichert. Sie soll je nach Bedarf durch die Krankenkassen aktualisiert werden.

Damit deutet eine Befreiung auf gesundheitliche Probleme von erheblichem Umfang hin. Wie bereits erläutert, erfolgt der besondere Schutz der in § 3 Abs. 9 BDSG genannten Daten wegen der Auswirkungen, die ihr Bekanntwerden in bestimmten sozialen Zusammenhängen haben kann. Für diese Auswirkungen sind aber nicht so sehr die konkreten Krankheiten, sondern vielmehr die aus diesen resultierenden Folgen maßgeblich. So ist etwa für einen Arbeitgeber die Information, dass bei einem Arbeitnehmer aufgrund einer schweren oder chronischen Krankheit mutmaßlich hohe Fehlzeiten zu erwarten sind, viel wichtiger als die Frage, welche konkrete Krankheit hierfür die Ursache ist. Deshalb muss der Gesundheitsbegriff zumindest im Rahmen von § 3 Abs. 9 BDSG und der auf ihn verweisenden Normen so weit verstanden werden, dass eine exakte Krankheitsangabe nicht erforderlich ist, sofern das Datum einen Rückschluss auf den generellen Gesundheitszustand des Betroffenen ermöglicht. Dies ist bei der Befreiung von der Zuzahlung der Fall.

Die Genauigkeit der Information wird zwar dadurch eingeschränkt, dass bei einem geringen Bruttojahreseinkommen die Belastungsgrenze möglicherweise bereits bei nicht so schwerwiegenden Erkrankungen erreicht wird. Auch hier bleibt aber das Risiko, dass Interaktionspartner eine chronische Krankheit vermuten und ihr Verhalten dementsprechend zum Nachteil des Versicherten verändern. Außerdem kann bei einer Befreiung zu einem frühen Zeitpunkt im Jahr in jedem Fall auf eine schwere Krankheit geschlossen werden. Darüber hinaus besteht die Gefahr, dass Daten sammelnde Instanzen über Zusatzinformationen verfügen, aus denen sie die Belastungsgrenze, und damit die tatsächlich bereits geleisteten Zuzahlungen, bestimmen können.[1645] Dies trifft insbesondere auf den Arbeitgeber zu, da dieser Kenntnis vom Bruttojahreseinkommen des Versicherten hat. Wenn die Höhe der Heilungskosten ein Datum über die Gesundheit ist,[1646] so trifft dies auch auf die Zuzahlungsbefreiung zu.

Im Ergebnis sind damit alle Angaben nach § 291a Abs. 3 Satz 1 (mit Ausnahme einiger selbst zur Verfügung gestellter Daten), die Angabe über eine Befreiung von der Zuzahlung und die Protokolldaten über die Zugriffe auf die elektronische Gesundheitskarte besondere Arten personenbezogener Daten. Für diese gelten die Verwendungsbeschränkungen in § 28 Abs. 6 bis 9 BDSG.[1647] Von diesen sind für die Gesundheitskarte insbesondere § 28 Abs. 6 und 7 BDSG relevant. § 28 Abs. 6 BDSG schließt zunächst die Anwendung von § 28 Abs. 1 BDSG aus: Es ist nicht möglich, die Datenverwendung durch ein schlichtes Berufen auf die Zweckbestimmung des Vertragsverhältnisses zu legitimieren.[1648] § 28 Abs. 6 BDSG

1644 Im Unterschied zur alten Regelung gilt die Grenze allgemein, nicht nur für die chronische Krankheit.

1645 So es auf derartige Zusatzinformationen ankommt, kann es – ausgehend von der unter 4.1.2.1 beschriebenen Relativität des Personenbezugs – dazu kommen, dass das Datum für eine verantwortliche Stelle unter § 3 Abs. 9 BDSG fällt, für eine andere jedoch nicht.

1646 Simitis-*o.V.*, § 14 Rn. 117.

1647 Das gilt, soweit nicht-öffentliche Stellen betroffen sind. Dies ist für alle Vertragsärzte und – je nach Bundesland – für die meisten Krankenhäuser der Fall, s. *Hermeler* 2000, 69 ff. und oben 4.1.1.2. Für öffentliche Stellen gelten die §§ 13 Abs. 2, 14 Abs. 5 und 6 BDSG. Inhaltlich ergibt sich dabei eine weitgehende Übereinstimmung, was das Gesundheitswesen angeht.

1648 Unzutreffend insoweit Roßnagel-*Schirmer*, Kap. 7.12, Rn. 78; wie hier *Der Berliner Beauftragte für Datenschutz*, RDV 2003, 308, 309; *Dierks/Nitz/Grau* 2003, 46.

formuliert enge Erlaubnistatbestände für die Datenverwendung; daneben ist eine solche nur nach einer ausdrücklichen Einwilligung gemäß § 4a Abs. 3 BDSG zulässig.

Im Bereich des Gesundheitswesens findet jedoch für die Gesundheitsvorsorge, die medizinische Diagnostik, die Gesundheitsversorgung und Behandlung sowie für die Verwaltung von Gesundheitsdiensten § 28 Abs. 7 Satz 1 BDSG Anwendung.[1649] Danach ist das Erheben von besonderen Arten von Daten zu diesen Zwecken zulässig, wenn die Verarbeitung durch ärztliches Personal oder sonstige geheimhaltungspflichtige Personen erfolgt. Gemäß § 28 Abs. 7 Satz 2 BDSG richtet sich die weitere Verarbeitung und Nutzung nach den entsprechenden Geheimhaltungspflichten. Außerhalb des Anwendungsbereichs von § 28 Abs. 7 BDSG sind Gesundheitsdaten nach § 28 Abs. 6 BDSG zu behandeln.[1650] § 28 Abs. 7 BDSG schließt jedoch den administrativen Teil der Versorgung (Verwaltung und Abrechnung) mit ein, sodass sämtliche Tätigkeiten der Leistungserbringer umfasst sind. Unanwendbar ist die Norm dagegen auf Krankenkassen.[1651]

Zu klären bleibt der Anwendungsbereich von § 28 Abs. 7 Satz 1 BDSG. Sein Wortlaut ist extrem weit: Losgelöst von jeder Mitwirkung des Versicherten spricht die Norm nur davon, das Erheben sei zulässig, „wenn es zum Zweck" der genannten Funktionen „erforderlich ist". Davon wäre auch eine Datenerhebung ohne oder sogar gegen den Willen des Betroffenen erfasst, wenn sie objektiv seiner Gesundheitsversorgung dienen würde. Eine solche Auslegung widerspräche jedoch der grundlegenden Patientenautonomie, die neben der Entscheidung über eine Untersuchung und Behandlung auch die Verfügungsgewalt über Gesundheitsdaten beinhaltet.[1652] Sinn und Zweck von § 28 Abs. 7 BDSG ist es jedoch nur, den Leistungserbringern die Dokumentation des Behandlungsvorgangs sowie die weitere Verwendung dieser Daten zu Abrechnungs- oder Beweiszwecken zu ermöglichen, ohne dass der Patient hierzu für jedes Datum schriftlich einwilligen müsste oder für eine einzelne Information seine Einwilligung verweigern könnte.[1653] Die Norm schafft also keinen Ermächtigungstatbestand für Datenerhebungen ohne oder gegen den Willen des Versicherten, sondern erfasst nur Situationen, in denen ein freiwilliger Kontakt zwischen Versichertem und Leistungserbringer hergestellt wurde.[1654] Im Ergebnis ist damit das Erheben, Verarbeiten und Nutzen von Gesundheitsdaten durch Arztpraxen, Apotheken, alle öffentlichen und privaten Krankenhäuser und sonstige Leistungserbringer zu den in § 28 Abs. 7 BDSG genannten Zwecken zulässig, allerdings nur, wenn diese Daten vom Versicherten freiwillig offenbart wurden. Das gilt auch für Datenverwendungen im Zusammenhang mit der elektronischen Gesundheitskarte.

1649 Das macht von der Ausnahme in Art. 8 Abs. 3 DSRL Gebrauch; s. dazu *Meier* 2003, 62 ff. m.w.N.

1650 Simitis-*Simitis*, § 28 Rn. 338 f.

1651 S. Simitis-*Simitis*, § 28 Rn. 342; *Gola/Schomerus*, § 13 Rn. 22. Hier ist eine Einwilligung erforderlich.

1652 Zu einem ähnlichen Problem im Rahmen des Zugriffs auf die Gesundheitskarte vgl. oben 4.2.3.4.2.2.

1653 Vgl. die Begründung, BT-Drs. 14/4329, 39, 43; *Gola/Schomerus*, § 13 Rn. 22; § 14 Rn. 33; *Meier* 2003, 66.

1654 Zumindest missverständlich *Dierks/Nitz/Grau* 2003, 239 (wonach aufgrund von § 28 Abs. 7 Satz 2 BDSG „kein datenschutzrechtliches Einwilligungserfordernis" bestehen soll); *Meier* 2003, 68 („wer einer der ärztlichen Schweigepflichten aus § 203 StGB…unterliegt,…darf sensitive Daten erheben") und *Berg*, MedR 2004, 413 (§ 28 Abs. 7 Satz 1 BDSG beinhalte eine „Abkehr vom…Einwilligungserfordernis"; s. allerdings die korrekte Darstellung ebd., 414: eine Einwilligung des Patienten bleibt erforderlich, sie kann jedoch auch konkludent erklärt werden).

4.3.4.2.3 Der Einsatz von Biometrie bei Signaturkarten

Die datenschutzrechtliche[1655] Zulässigkeit des Einsatzes von Biometrie im Rahmen der elektronischen Signatur ist nach §§ 4a, 28 Abs. 6 bis 9 BDSG zu beurteilen. Da die Ausnahmen von der Verwendungsbeschränkung in § 28 BDSG nicht einschlägig sind, ist eine Einwilligung erforderlich. Diese hat sich nach § 4a Abs. 3 BDSG ausdrücklich auf die Verwendung biometrischer Daten als besondere Arten personenbezogener Daten zu beziehen. Das gilt auch bei der Speicherung von Templates auf der Karte, da zum Matching in jedem Fall Rohdaten erhoben werden. Die Einwilligung bedarf nach § 4a Abs. 1 Satz 3 BDSG der Schriftform, weil keine Umstände vorliegen, nach denen eine andere Form angemessen wäre. Sie kann in den Vertrag mit dem Zertifizierungsdiensteanbieter mit aufgenommen oder bei Anlass des Abschlusses erteilt werden.

4.3.5 Automatisierte Einzelentscheidung (§ 6a BDSG)

Biometrische Authentifikationssysteme verarbeiten in automatisierter Art und Weise personenbezogene Daten. Führt der Verarbeitungsvorgang zu einer Einzelentscheidung, so schränkt § 6a Abs. 1 BDSG die Zulässigkeit des Vorgangs ein: Wenn die Entscheidung für den Betroffenen eine rechtliche Folge nach sich zieht oder ihn erheblich beeinträchtigt, darf sie nicht ausschließlich auf eine automatisierte Verarbeitung personenbezogener Daten gestützt werden, die der Bewertung einzelner Persönlichkeitsmerkmale dient.

Ein derartiger Prozess könnte dann gegeben sein, wenn ein biometrisches System ohne die Möglichkeit manueller Nachkontrolle eine endgültige Entscheidung über die Zugehörigkeit eines vorgezeigten Chipkartenausweises zu einer Person fällen würde.[1656] Eine Entscheidung läge hier vor, die den Betroffenen bei einer Zurückweisung auch erheblich beeinträchtigen würde. Fraglich ist aber, ob die automatisierte Verarbeitung biometrischer Daten der Bewertung einzelner Persönlichkeitsmerkmale dient. Nach der Intention des Gesetzgebers ist das ausdrücklich nicht der Fall.[1657] § 6a BDSG bezweckt vielmehr den Schutz vor den Risiken einer wertenden Entscheidung über Profildaten, die dann entstehen, wenn diese in einem automatischen und undurchschaubaren Prozess gefällt werden.[1658] Die Norm setzt außerdem Art. 15 DSRL um. Dort werden als Persönlichkeitsmerkmale beispielhaft die berufliche Leistungsfähigkeit, die Kreditwürdigkeit, die Zuverlässigkeit oder das Verhalten einer Person genannt.[1659] Mit diesen bewertenden Kriterien kann jedoch eine biometrische Erfassung nicht verglichen werden. Hinter § 6a BDSG steht der Gedanke, dass wertende Entscheidungen der Beurteilung durch einen Menschen bedürfen.[1660] Das ist bei der Biometrie nicht der Fall. In einigen Bereichen (beispielsweise bei der Iriserkennung) ist eine Entscheidung sogar ausschließlich mittels Datenverarbeitungsanlagen möglich.

Zutreffend ist demgegenüber sicherlich, dass § 6a BDSG anwendbar ist, wenn in einem größeren Verarbeitungssystem nach erfolgter Identifizierung mittels Biometrie eine wer-

---

1655 Zu den signaturrechtlichen Problem s.u. 5.2.6.

1656 Sobald eine manuelle Nachkontrolle vorgesehen ist, ist § 6a BDSG unanwendbar, s. die Gesetzesbegründung, BT-Drs. 14/4329, 37; Simitis-*Bizer*, § 6a Rn. 27; *Schaffland/Wiltfang*, § 6a Rn. 2; Einzelbeispiele bei *Koch*, MMR 1998, 458, 459 f.

1657 Vgl. die Begründung zu § 6a BDSG, BT-Drs. 14/4329, 37.

1658 Näher *Gola/Schomerus*, § 6a Rn. 7 ff.; Simitis-*Bizer*, § 6a Rn. 2 ff.; s.a. *Ehmann/Helfrich* 1999, Art. 15 Rn. 11 ff. (zur DSRL).

1659 Hierauf verweist die Gesetzesbegründung ausdrücklich, s. BT-Drs. 14/4329, 37.

1660 Roßnagel-*Duhr*, Kap. 7.5, Rn. 50.

tende Entscheidung über einzelne Persönlichkeitsmerkmale erfolgt.[1661] Daraus kann jedoch nicht auf die Anwendbarkeit von § 6a BDSG auf biometrische Systeme geschlossen werden, weil der Tatbestand der Norm dann nicht durch den Einsatz der Biometrie begründet wird, sondern durch die automatisierte Entscheidung, die der Identifizierung nachfolgt. Unzutreffend ist es schließlich, eine automatisierte Einzelentscheidung im Sinne von § 6a Abs. 1 BDSG deshalb anzunehmen, weil biometrische Systeme eine falsche Entscheidung ohne Korrekturmöglichkeit treffen können, die erhebliche rechtliche und finanzielle Nachteile für den Betroffenen verursachen kann.[1662] Hierdurch wird zwar das Merkmal der erheblichen Beeinträchtigung erfüllt, es ergibt sich aber kein Argument für das Vorliegen einer Bewertung einzelner Persönlichkeitsmerkmale.

Von Wortlaut, Entstehungsgeschichte und Normzweck ist § 6a BDSG damit nicht auf biometrische Systeme anwendbar. Er betrifft wertende Entscheidungen, die zum Schutz des Betroffenen nicht in automatisierter Form anhand abstrakter Kriterien getroffen werden sollen. Bei biometrischen Verfahren besteht diese Gefahr jedoch nicht. Der einfache Abgleich biometrischer Daten mit Referenzdaten beinhaltet keine Bewertung der Person, sondern eine Entscheidung darüber, ob diese Person die ist, die sie zu sein vorgibt. § 6a BDSG ist damit im vorliegenden Fall nicht anwendbar.[1663]

Davon abgesehen bleibt darauf hinzuweisen, dass eine absolut automatisierte Kontrolle mittels Biometrie aus anderen Gründen unzulässig ist. Der Einsatz von Biometrie ist aufgrund der Fehleranfälligkeit der Systeme nur dann geeignet und für die Betroffenen objektiv zumutbar, wenn diskriminierungsfreie Alternativverfahren bereitgehalten werden.[1664] Hierzu gehört auch die Ermöglichung manueller Nachkontrollen.

4.3.6 Probleme der Datenübermittlung

Je mehr Anwendungen auf einem Chipkartenausweis vereint werden, desto wahrscheinlicher ist es, dass mehr als eine verantwortliche Stelle auf diesen zugreifen kann. Mit der Komplexität des jeweiligen Verfahrens nimmt überdies die Zahl der Stellen zu, die an einer einzelnen Anwendung beteiligt sind. Schließlich kann es sinnvoll sein, dass nicht alle Stellen, sondern nur die ausgebende Instanz in einen direkten Kontakt mit dem Ausweisinhaber tritt (insbesondere, wenn der Ausweis signaturfähig ist und der Zertifizierungsdiensteanbieter nicht über ein eigenes Vertriebssystem verfügt). Diese drei Faktoren führen dazu, dass vor der Ausgabe, aber auch auf oder mittels der Karte eine Vielzahl von Daten übermittelt werden. Für diese Vorgänge bestehen datenschutzrechtliche Bestimmungen.

1661 So wohl Simitis-*Bizer*, § 6a Rn. 37. Die Formulierung „Die Regelung findet...Anwendung, wenn biometrische Identifikationsmerkmale zur Bewertung von Persönlichkeitsmerkmalen als Grundlage für eine Entscheidung automatisiert verarbeitet werden“ (identisch bei *Albrecht* 2003a, 184) scheint in diese Richtung zu gehen, auch wenn sie an sich wenig Sinn ergibt: Zwar ist eine gestufte automatisierte Entscheidung denkbar, in der zunächst mittels Biometrie über die Identität einer Person, und danach (wertend) über einzelne Persönlichkeitsmerkmale entschieden wird. In einem solchen Verfahren werden aber nicht die biometrischen Daten „zur Bewertung“ von Persönlichkeitsmerkmalen verarbeitet, weil die Identität einer Person begrifflich nicht zur Bewertung ihrer Merkmale dienen kann.

1662 So aber *Albrecht* 2003a, 184 f.; ähnlich *Golembiewski/Probst* 2003, 28.

1663 *Roßnagel/Hornung*, in: Reichl/Roßnagel/Müller 2005, 141; ebenso *Gola/Schomerus*, § 6a Rn. 8; *Duhr/Naujok/Peter/Seiffert*, DuD 2002, 5, 26; für die DSRL *Prins*, Computer Law & Security Report 1998, 159, 163; ohne Meinung Roßnagel-*Gundermann/Probst*, Kap. 9.6, Rn. 71 (man „könnte der Auffassung sein“, biometrische Verfahren fielen in den Anwendungsbereich von Art. 15 DSRL).

1664 S.o. 4.2.2.4.7.

4.3.6.1 Zulässigkeit nach dem Teledienstedatenschutzrecht

Zunächst sind als verdrängende Spezialregelungen für die Einbeziehung externer Dienstleister die Vorschriften des Teledienstedatenschutzrechts zu prüfen. Diese sind für die Identifizierungsfunktion des digitalen Personalausweises nicht einschlägig, weil er insoweit keinen funktionalen Anschluss an periphere Strukturen hat.[1665] Bei der Übermittlung von Zertifikatsdaten vom Ausweis und im Rahmen von OCSP-Prüfungen handelt es sich um ein allgemeines datenschutzrechtliches Problem der elektronischen Signatur; die Übermittlung ist eine notwendige Voraussetzung der Verwendung der Signaturkarte und deshalb zulässig.[1666]

Dagegen kommen für die elektronische Gesundheitskarte vorrangige Bestimmungen des Teledienstedatenschutzrechts in Betracht.[1667] Dazu ist erforderlich, dass es sich bei den jeweiligen Anwendungen um Teledienste handelt. Es ist zwischen den unterschiedlichen Möglichkeiten der Organisation der Datenspeicherung und des Datentransfers (auf der Karte, in einem verteilten System oder auf zentralen Servern) zu unterscheiden. Bei einer Speicherung auf der Karte sind keine externen Instanzen beteiligt. In verteilten Systemen können Dritte die Organisation der Speicherorte und der Zugriffsbefugnisse durchführen. In Serverlösungen übernehmen Dienstleister die Datenspeicherung, eventuell auch die Aufbereitung und Zusammenführung.

Teledienste sind gemäß § 2 Abs. 1 TDG „elektronische Informations- und Kommunikationsdienste, die für eine individuelle Nutzung von kombinierbaren Daten wie Zeichen, Bilder oder Töne bestimmt sind und denen eine Übermittlung mittels Telekommunikation zugrunde liegt".[1668] Bei einer Speicherung auf Servern liegt sowohl der Ablage als auch dem Abruf Telekommunikation zugrunde. Da die Nutzung der Gesundheitsinformationen den wesentlichen Inhalt des Vorgangs bildet, geht dieser auch über die reine Telekommunikationsebene hinaus.[1669] Der Dienst wird auch individuell genutzt, weil es immer um den Zugriff eines einzelnen Leistungserbringers gemäß dessen Zugriffsrechten zur Erbringung einer individuellen Leistung geht.[1670] Anwendungen wie die Telearchivierung medizinischer Daten, das Outsourcing mittels elektronischer Übertragung und die elektronische Patientenakte sind deshalb als Teledienste zu qualifizieren.[1671] Auf sie ist das Teledienste-

1665 Das gilt vorbehaltlich eines denkbaren Abgleichs mit Fahndungsdatenbanken. Dabei handelt es sich aber nicht um Teledienste.

1666 Roßnagel-*Roßnagel*, Kap. 7.7, Rn. 80 ff., insbes. Rn. 83.

1667 Die folgende Darstellung beschränkt sich auf das System der Gesundheitskarte. Allgemeine Datenschutzprobleme des Outsourcings im Gesundheitswesen bleiben außen vor; s. dazu *Müthlein/Heck* 1997; *Dammann/Rabenhorst*, CR 1998, 643 f.; *Hermeler* 2000, 181 ff. Für diesen Bereich existieren tlw. landesrechtliche Regelungen, s. *Hermeler* 2000, 186 ff. Das Problem der elektronischen Datenverarbeitung durch Dritte hat einen Vorläufer in der Frage der Zulässigkeit von Mikroverfilmungen medizinischer Daten außerhalb des Daten erhebenden Krankenhauses; s. dazu BVerfG, NJW 1991, 2952 f.; BayVerfGH, NJW 1989, 2939 ff., jeweils zu Art. 26 Abs. 4 Satz 5 BayKrankenhausG 1986, GVBl. S. 147, der dieses Vorgehen untersagte; zur gegenwärtigen Rechtslage s. Art. 27 Abs. 4 Satz 5 und 6 BayKrankenhausG.

1668 Näher RMD-*Spindler*, § 2 TDG 1997, Rn. 13 ff. m.w.N.; Hoeren/Sieber-*Holznagel/Kibele*, Kap. 5, Rn. 54 ff. m.w.N.

1669 Das kann dann anders sein, wenn ein Dienstleister lediglich Speicherkapazitäten für einen einzelnen Leistungserbringer vermietet. In diesem Fall beschränkt sich das Verhältnis auf die reine Telekommunikation. Das System der Gesundheitskarte wird aber über derartige Prozesse deutlich hinausgehen.

1670 Deshalb ist nicht der MDStV, sondern das TDG auf die Übermittlung medizinischer Daten an Leistungserbringer anwendbar, auch wenn diese Daten einem grundsätzlich unbestimmten Personenkreis zur Verfügung stehen. Dafür spricht auch die Entstehungsgeschichte, s. *Engel-Flechsig*, RDV 1997, 59, 62; *Hermeler* 2000, 158.

1671 Näher *Geis*, DuD 1997, 582, 583; *Hermeler* 2000, 158; allgemeiner *Schaar*, RDV 2003, 59, 65 f.

datenschutzgesetz anwendbar. Dieses schützt allerdings nach § 1 Abs. 1 Satz 1 TDDSG nur die personenbezogenen Daten der jeweiligen Nutzer. Nutzer ist gemäß § 2 Nr. 2 TDDSG „jede natürliche Person, die Teledienste in Anspruch nimmt, insbesondere um Informationen zu erlangen oder zugänglich zu machen“.[1672] Dies trifft zunächst auf den Leistungserbringer zu, der den Dienst nutzt, um Informationen über den Versicherten zu erhalten. Fraglich ist aber, ob daneben auch der Versicherte Nutzer ist.

Hiergegen spricht, dass dieser im System der Gesundheitskarte mit Ausnahme der auf der Karte gespeicherten, selbst zur Verfügung gestellten Daten keine eigene Zugriffsmöglichkeit auf die gespeicherten Angaben hat.[1673] Andererseits gilt dies nach § 291a Abs. 5 Satz 2 SGB V zumindest für die freiwilligen Anwendungen nach § 291a Abs. 3 Satz 1 Nr. 2 bis 6 SGB V[1674] auch umgekehrt: Dem Leistungserbringer ist ohne die Mitwirkung des Versicherten und den Einsatz seiner elektronischen Gesundheitskarte ein Zugriff nicht möglich. Gegen eine Nutzereigenschaft des Versicherten könnte auch sprechen, dass zwischen ihm und dem Dienstleister keine vertraglichen Beziehungen bestehen. Diese sind jedoch weder nach dem Wortlaut des Gesetzes noch nach dessen ausdrücklicher Begründung erforderlich.[1675] Schließlich „nutzt“ der Versicherte umgangssprachlich das System, da dessen Einrichtung nicht Selbstzweck ist, sondern seiner Versorgung dient. Es ließe sich etwa argumentieren, der Leistungserbringer greife im Auftrag des Versicherten auf die Daten zu, womit der Letztere zum wahren Nutzer des Systems werde.

Nichtsdestotrotz ist eine derartige Interpretation bedenklich. Zunächst dient das Teledienstedatenschutzgesetz insbesondere dem Schutz von Bestands-, Nutzungs- und Abrechnungsdaten des Nutzers.[1676] Derartige Daten fallen aber für den Versicherten nicht an, da der Diensteanbieter diesen weder kennt noch direkt mit ihm in Kontakt tritt. Darüber hinaus handelt der Leistungserbringer zwar auf Wunsch des Patienten, benutzt die Daten jedoch, um seine eigene Leistung zu erbringen und nicht, um sie etwa dem Versicherten zur Verfügung zu stellen. Nur in diesem Fall hätte der Versicherte aber eine so übergeordnete Position, dass er als der wahre Nutzer des Dienstes angesehen werden könnte. Schließlich wird die Verbindung zum Anbieter durch den Leistungserbringer hergestellt; über seine Datenverarbeitungsanlage werden die Informationen abgerufen, bereitgestellt und weiterverarbeitet. Der tatsächliche Vorgang des Bedienens wird damit durch den Leistungserbringer gesteuert. Da der Begriff des „Nutzers“ sich auf Teilnehmer am Kommunikationsprozess beschränkt,[1677] kann auch aus diesem Grund nicht von einem Nutzen durch den Versicherten gesprochen werden. Der Dienst wird vielmehr vom Leistungserbringer zum Zwecke der Versorgung des Versicherten genutzt. Dadurch wird Letzterer aber nicht selbst zum Nutzer.

Die Anforderungen des Teledienstedatenschutzgesetzes müssen damit im Ergebnis zwar vom Dienstleister befolgt werden, jedoch nur, soweit personenbezogenen Daten der Leistungserbringer betroffen sind, die den Dienst in Anspruch nehmen.[1678] Zusätzlich sind diesen gegenüber auch die allgemeinen und besonderen Informationspflichten nach §§ 6, 7

1672 Zum Begriff s. RMD-*Schulz*, § 2 TDDSG 1997 Rn. 19 ff.; RMD-*Waldenberger*, § 3 TDG 1997 Rn. 26 ff. (jeweils zur Legaldefinition nach der alten Gesetzesfassung, die sich aber – für den vorliegenden Kontext – nicht wesentlich von der aktuellen Definition unterscheidet).

1673 S.u. 4.3.7.3.

1674 Diese Nutzungsformen sind im vorliegenden Zusammenhang nur relevant, sofern ein Teledienst überhaupt vorliegt, d.h. insbesondere nicht bei der Speicherung auf der Gesundheitskarte selbst.

1675 S. BT-Drs. 13/7385, 22; RMD-*Schulz*, § 2 TDDSG 1997 Rn. 20.

1676 RMD-*Bizer*, § 3 TDDSG 1997 Rn. 75; *Hermeler* 2000, 161; Roßnagel-*Roßnagel*, Kap. 7.9, Rn. 53 ff.

1677 RMD-*Waldenberger*, § 3 TDG 1997 Rn. 12 (für das TDG).

1678 Im Ergebnis ebenso *Hermeler* 2000, 161.

TDG und die Regelungen über die Verantwortlichkeit im 3. Abschnitt des Teledienstegesetzes zu beachten.[1679] Beides ist allerdings unproblematisch, weil es um einen festen Nutzerkreis geht, der mit der Funktionsweise des Systems ohnehin vertraut sein wird.

Auf die medizinischen Informationen, die im Rahmen der Anwendungen der elektronischen Gesundheitskarte übertragen werden, ist das Teledienstedatenschutzrecht keinesfalls anwendbar. Hierbei handelt es sich um die Inhaltsdaten des Teledienstes. Für derartige Daten gilt das Teledienstedatenschutzgesetz jedoch nicht, weil es auf Daten beschränkt ist, die spezifisch für die Inanspruchnahme des Dienstes erhoben, verarbeitet oder genutzt werden.[1680] Auch wenn man den Versicherten selbst neben oder an Stelle des Leistungserbringers als Nutzer des Teledienstes ansähe, blieben die übermittelten Gesundheitsinformationen Inhaltsdaten, die unter das allgemeine Datenschutzrecht fielen.[1681]

4.3.6.2 Datenverarbeitung im Auftrag oder Funktionsübertragung?

Die Frage der datenschutzrechtlichen Zulässigkeit der Einbindung externer Dienstleister in das System der Gesundheitskarte bestimmt sich damit im Wesentlichen nach dem allgemeinen Datenschutzrecht. Beim digitalen Personalausweis kann es zu einer Zusammenarbeit zwischen Personalausweisbehörden und Zertifizierungsdiensteanbietern kommen. Für die datenschutzrechtliche Bewertung ist in beiden Fällen maßgebend, ob eine Datenverarbeitung im Auftrag oder eine Funktionsübertragung vorliegt.

4.3.6.2.1 Abgrenzung

Das Bundesdatenschutzgesetz regelt in § 11 BDSG (der Art. 17 Abs. 2 bis 4 DSRL umsetzt) nur die Datenverarbeitung im Auftrag. Die Norm konzentriert die datenschutzrechtlichen Verantwortlichkeiten beim Auftraggeber. Dieser soll sich seinen Pflichten nicht durch die Auslagerung der Erhebung, Verarbeitung oder Nutzung der Daten entziehen und diese auf nachgelagerte, ihm weisungsabhängige Stellen verschieben können.

§ 11 BDSG ist deshalb nur bei einem ausgeprägten Über-Unterordnungsverhältnis zu Lasten des Auftragnehmers anwendbar. Dieser ist in hohem Maße an die Weisungen des Auftraggebers gebunden, wird aber von einer Bindung an das Bundesdatenschutzgesetz

---

1679 Auch im Rahmen des TDG sind ausschließlich die Leistungserbringer Nutzer. Der Nutzerbegriff des TDG und des TDDSG ist zwar nicht mehr (wie vor der Reform) wortgleich. Inhaltlich bestehen im hier relevanten Zusammenhang jedoch keine Unterschiede.

1680 *Bäumler*, DuD 1999, 258, 259; RMD-*Bizer*, § 3 TDDSG 1997 Rn. 61; RMD-*Engel-Flechsig*, Einl. TDDSG 1997 Rn. 60; Roßnagel-*Roßnagel*, Kap. 7.9, Rn. 36 f., 59; a.A. *Geis*, RDV 2000, 208, 209; Hoeren/Sieber-*Schmitz*, Kap. 16.4, Rn. 99; *ders.* 2000, 127 ff., wonach sämtliche bei der Teledienstenutzung anfallenden Daten vom TDDSG erfasst sein sollen. § 3 Abs. 1 TDDSG (alte wie neue Fassung) erfasst aber nur Daten „zur Durchführung von Telediensten". Die ebd. ausgeführte Berufung auf RMD-*Dix*, § 5 TDDSG 1997 Rn. 52; *Büllesbach*, DuD 1999, 263, 265 und *Engel-Flechsig*, DuD 1997, 8, 11 geht im Übrigen fehl: *Dix* weist zwar auf die Problematik einer Trennung zwischen Transport- und Inhaltsebene hin, kommt aber „gegenwärtig" zu dem Ergebnis, dass diese gesetzlich vorgegeben ist. Nach *Büllesbach* sind die Inhaltsdaten nach dem BDSG zu behandeln, da ansonsten eine unangemessene Differenzierung danach erfolge, ob diese durch einen Teledienst oder auf anderem Wege erfasst würden. *Engel-Flechsig* spricht zwar davon, das TDDSG gelte „generell beim Umgang mit personenbezogenen Daten bei Telediensten". Dies erfolgt jedoch nicht in Abgrenzung zum BDSG, sondern zur Klarstellung, dass sich der Anwendungsbereich „nicht auf eine bestimmte Verarbeitungsstufe" beschränkt, sondern Erhebung, Verarbeitung und Nutzung erfasst.

1681 Die hauptsächlichen datenschutzrechtlichen Risiken des Einsatzes von Telematik im Gesundheitswesen liegen damit in der Inhaltsebene, s. *Garstka*, ZaeFQ 1999, 781, 783; *Dierks/Nitz/Grau* 2003, 83 f.

weitgehend freigestellt.[1682] Der Begriff des Auftrags ist zwar weit, also nicht nur im Sinne von § 662 BGB zu verstehen.[1683] Für eine Datenverarbeitung im Auftrag ist jedoch eine vollständige Abhängigkeit hinsichtlich des Umgangs mit den Daten erforderlich.[1684] Die Grenze zur Funktionsübertragung ist dann überschritten, wenn der Dritte über Hilfs- und Unterstützungsfunktionen hinaus tätig wird.[1685] Besitzt der Auftragnehmer eine rechtliche Zuständigkeit für eine eigene Aufgabe,[1686] beziehungsweise erfüllt er überwiegend eigene Geschäftszwecke,[1687] so ist eine Funktionsübertragung anzunehmen.

Bei einer Datenverarbeitung im Auftrag ist der Auftragnehmer nach § 3 Abs. 8 Satz 2 BDSG nicht Dritter im Sinne des Gesetzes, ein Datentransfer an ihn ist keine Übermittlung.[1688] Dennoch ist eine Einwilligung des Betroffenen erforderlich, da im Transfer eine Nutzung der Daten liegt.[1689] Allerdings bleibt der Auftraggeber nach § 3 Abs. 7 BDSG verantwortliche Stelle und nach § 11 Abs. 1 Satz 1 BDSG für die Einhaltung der datenschutzrechtlichen Vorschriften verantwortlich. Der Betroffene hat gemäß § 11 Abs. 1 Satz 2 BDSG ihm gegenüber seine Rechte geltend zu machen. Der Auftraggeber muss den Auftragnehmer nach § 11 Abs. 1 Satz 1 und Satz 2 BDSG sorgfältig auswählen und die Datenerhebung, -verarbeitung und -nutzung sowie die technischen und organisatorischen Maßnahmen schriftlich im Auftrag festhalten.[1690] Außerdem besteht nach § 11 Abs. 1 Satz 4 BDSG die Pflicht, sich von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen. Die Kontrolle des Auftragnehmers durch den Auftraggeber hat vor Auftragsvergabe, aber auch während des Auftragsverhältnisses, etwa mit Hilfe von Stichproben, zu erfolgen.[1691] Hierzu sind vertraglich geeignete Mittel zu vereinbaren, etwa Zutrittsrechte des Auftraggebers oder die Pflicht des Auftragnehmers, auf Aufforderung Unterlagen vorzulegen. Der betriebliche Datenschutzbeauftragte des Auftraggebers ist auch für die Datenverarbeitung beim Auftragnehmer zuständig.[1692] Der Auftragnehmer ist demgegenüber nach § 11 Abs. 3 BDSG weisungsgebunden[1693] und muss den Auftraggeber unverzüglich auf etwaige von diesem ausgehende datenschutzrechtswidrige Weisungen aufmerksam machen.

1682 Roßnagel-*Hoeren*, Kap. 4.6, Rn. 105; *Sutschet*, RDV 2004, 97, 98. Die anwendbaren Regelungen sind in § 11 Abs. 4 BDSG aufgelistet. Sie betreffen lediglich das Datengeheimnis (§ 5 BDSG), die technischen und organisatorischen Maßnahmen nach § 9 BDSG i.V.m. der Anlage sowie in eingeschränktem Maße die Regelungen aus dem Bußgeld-, Straf- und Aufsichtsbereich.

1683 *Gola/Schomerus*, § 11 Rn. 6; *Sutschet*, RDV 2004, 97, 99 m.w.N.

1684 *Gola/Schomerus*, § 11 Rn. 3; *Müthlein*, RDV 1993, 165, 166; für den Bereich der Finanzdienstleistungen vgl. *Evers/Kiene*, DuD 2003, 341, 343.

1685 *Bergmann/Möhrle/Herb*, § 11 Rn. 8; *Gola/Schomerus*, § 11 Rn. 3, 9; *Tinnefeld/Ehmann* 1998, 245; Simitis-*Walz*, § 11 Rn. 18; *Schaffland/Wiltfang*, § 11 Rn. 1; skeptisch gegenüber diesem Kriterium Roßnagel-*Hoeren*, Kap. 4.6, Rn. 99; *Sutschet*, RDV 2004, 97, 99; zu Abgrenzungsproblemen s. *Wronka*, RDV 2003, 132, 133 ff.

1686 *Gola/Schomerus*, § 11 Rn. 9; *Müthlein*, RDV 1993, 165, 166; *Wächter*, CR 1991, 333; kritisch *Sutschet*, RDV 2004, 97, 99.

1687 Simitis-*Walz*, § 11 Rn. 18; s.a. die Kriterien bei *Kramer/Herrmann*, CR 2003, 938 ff.

1688 *Gola/Schomerus*, § 11 Rn. 4.

1689 Simitis-*Dammann*, § 3 Rn. 164; Roßnagel-*Hoeren*, Kap. 4.6, Rn. 101; Roßnagel-*Schild*, Kap. 4.2, Rn. 70. Das wird übersehen von *Dierks/Nitz/Grau* 2003, 233; *Meier* 2003, 124; *Sutschet*, RDV 2004, 97, wonach die Weiterleitung der Daten ohne weiteres möglich sein soll.

1690 Zu den Einzelheiten s. Simitis-*Walz*, § 11 Rn. 49 ff.; *Wächter*, CR 1991, 333, 334; *Aufsichtsbehörde Baden-Württemberg*, StAnz BW 1993, 5 (unter 2).

1691 *Gola/Schomerus*, § 11 Rn. 22; Roßnagel-*Hoeren*, Kap. 4.6, Rn. 103; Simitis-*Walz*, § 11 Rn. 47; zu den Möglichkeiten *Dolderer/v. Garrel/Müthlein/Schlumberger*, RDV 2001, 223, 225.

1692 *Gola/Schomerus*, § 11 Rn. 22; Roßnagel-*Hoeren*, Kap. 4.6, Rn. 102 f.; *Aufsichtsbehörde Baden-Württemberg*, StAnz BW 1980, 5, unter 4; *Schaffland/Wiltfang*, § 11 Rn. 9a.

1693 Dazu Simitis-*Walz*, § 11 Rn. 55 ff., 66; *Sutschet*, RDV 2004, 97, 101 f.

Liegt dagegen eine Funktionsübertragung vor, so ist der Datentransfer an den Dritten regelmäßig[1694] eine Übermittlung im Sinne von § 3 Abs. 4 Nr. 3 BDSG, sodass die entsprechenden Zulässigkeitsvoraussetzungen (Einwilligung des Betroffenen oder gesetzliche Ermächtigung) zu erfüllen sind.[1695] Der Betroffene muss seine datenschutzrechtlichen Rechte gegenüber dem Dritten geltend machen. Für die Ausgestaltung des Verhältnisses der beiden verantwortlichen Stellen bestehen im Datenschutzrecht keine expliziten Regelungen.[1696]

4.3.6.2.2 Anwendung auf Chipkartenausweise

4.3.6.2.2.1 Verarbeitung von Gesundheitsdaten im System der Gesundheitskarte

Nach diesen Kriterien kann im Gesundheitswesen etwa eine Datenverarbeitung im Auftrag vorliegen, wenn eine Arztpraxis ein externes Archiv mit der Datenspeicherung beauftragt.[1697] In diesem Fall nimmt das Archiv eine reine Hilfsfunktion wahr, die datenschutzrechtlich zulässig ist, wenn die Anforderungen des § 11 BDSG erfüllt werden. Strikt hiervon zu trennen ist allerdings die Frage einer strafrechtlichen Verantwortlichkeit. Die Regelungen zur Auftragsdatenverarbeitung begründen keine Offenbarungsbefugnis im Sinne von § 203 StGB.[1698] Deshalb ist zur Rechtfertigung einer eventuellen Offenbarung die Einwilligung des Versicherten erforderlich.[1699]

Auch eine einrichtungsübergreifende serverbasierte Datenhaltung (wie etwa für die elektronische Patientenakte) wird teilweise als eine Datenverarbeitung im Auftrag angesehen.[1700] Der Tatbestand des § 11 BDSG ist jedoch nicht einschlägig.[1701] Zwar könnte auch im Verhältnis zwischen einem Dienstleister und einer Vielzahl von Leistungserbringern rein sprachlich eine ebenso große Anzahl von Auftragsverhältnissen angenommen werden. Es fehlt jedoch an der untergeordneten, weisungsabhängigen Hilfsfunktion des Dienstleisters. Die einzelnen Leistungserbringer können allenfalls für die von ihnen übermittelten oder abgerufenen Daten als Auftraggeber angesehen werden. Es ist aber weder technisch noch organisatorisch umsetzbar, dass der jeweilige Leistungserbringer für genau diese Daten Weisungen ausspricht oder Kontrollbefugnisse ausübt.[1702] Die Datenverarbeitung hat vielmehr aus technischen Gründen, aber auch zur Gewährleistung von Rechtsgleichheit und datenschutzrechtlicher Transparenz, nach einheitlichen Maßstäben und Verfahren abzulaufen, die nicht vom Einfluss einzelner Leistungserbringer abhängig sein können.

1694 Zu den Einschränkungen durch Verschlüsselungs-, Anonymisierungs- und Pseudonymisierungsverfahren s.u. 4.3.6.2.2.1.

1695 Die Übermittlung kann ohne Einwilligung auch bei Verstoß gegen Schweigepflichten unzulässig sein, s. dazu bereits oben 4.2.3.5.1.

1696 Zur Notwendigkeit einer solchen Regelung vgl. *Roßnagel/Pfitzmann/Garstka* 2001, 124 ff.

1697 *Bultmann/Wellbrock/Biermann/Engels/Ernestus/Höhn/Wehrmann/Schurig* 2002, 7; *Hermeler* 2000, 181 ff.

1698 Das folgt ausdrücklich aus § 1 Abs. 3 Satz 2 BDSG; s.a. *Auernhammer*, § 11 Rn. 10; *ULD* 2002, unter 1; Simitis-*Walz*, § 11 Rn. 31 ff.; zumindest missverständlich *Wehrmann/Wellbrock*, CR 1997, 754, 757.

1699 S. näher oben 4.2.3.5.1.

1700 *Bultmann/Wellbrock/Biermann/Engels/Ernestus/Höhn/Wehrmann/Schurig* 2002, 7 f. i.V.m. 15, 17; ähnlich, wenn auch sehr undifferenziert, *Fuest* 1999, 158; ohne Kriterium für die Unterscheidung *Dierks/Nitz/Grau* 2003, 79.

1701 S. hierzu schon *Hornung* 2004a, 233 f.

1702 *Hermeler* 2000, 167.

Allenfalls wäre eine Vertragsgestaltung vorstellbar, in der die Standesorganisationen auf Bundesebene als Auftraggeber fungieren.[1703] Auch diese Lösung stößt indes auf unüberwindbare Hindernisse. Zunächst müssten sämtliche Leistungserbringer (und zwar mangels gesetzlicher Regelung[1704] freiwillig) diesen Organisationen ein entsprechendes Mandat erteilen. Ohne eine solche Vollmacht könnte etwa die Bundesärztekammer nicht als Auftraggeber auftreten, da nicht sie, sondern die in ihr vertretenen Ärzte verantwortliche Stellen nach § 3 Abs. 7 BDSG sind. Schließlich bedingen die Organisation und der Betrieb eines zentralen Datenverarbeitungssystems im Gesundheitswesen einen Umfang und Komplexitätsgrad, der nicht mehr als Hilfsfunktion angesehen werden kann. Hier handelt es sich um eine eigene Aufgabe des Dienstleisters.[1705] Genau dies ist jedoch das Kriterium für eine Funktionsübertragung.

Auch in einem verteilten System, in dem die Datenspeicherung ausschließlich bei den Leistungserbringern erfolgt, liegt kein Auftrag vor. Aufgrund der gleichberechtigten Stellung ergibt sich kein Über-Unterordnungsverhältnis.[1706] Im Ergebnis besteht damit bei der Einbeziehung externer Dienstleister im System der Gesundheitskarte unabhängig von der konkreten Organisation der Datenspeicherung und des Zugriffs keine Datenverarbeitung im Auftrag, sondern eine Funktionsübertragung.

Im Regelfall sind in einem derartigen System Datentransfers als Übermittlungen im Sinne von § 3 Abs. 4 Nr. 3 BDSG anzusehen mit der Folge, dass nach § 4 Abs. 1 BDSG eine gesetzliche Ermächtigung oder eine Einwilligung des Betroffenen erforderlich ist. Fraglich ist aber, ob dies ausnahmslos gilt. Im Rahmen des Betriebs der Serversysteme sind nämlich schon aus Datensicherheitsgründen sichere Verschlüsselungsverfahren bei der Datenübermittlung und Speicherung zu verwenden.[1707] Darüber hinaus müssen nach Möglichkeit Anonymisierungs- und Pseudonymisierungsverfahren eingesetzt werden.[1708] Wird hierdurch eine Kenntnisnahme des Inhalts oder des Personenbezugs der Daten durch die empfangende Stelle ausgeschlossen, so könnte es an einem „Bekanntgeben" personenbezogener Daten im Sinne von § 3 Abs. 4 Nr. 3 BDSG fehlen. Dann käme es auch auf die Unterscheidung zwischen Datenverarbeitung im Auftrag und Funktionsübertragung nicht an, weil beide die Verwendung personenbezogener Daten voraussetzen.

Wenn anonyme Angaben übertragen werden, fehlt es an einem solchen Datum.[1709] Bei pseudonymisierten Daten kommt es auf die Verfügungsgewalt über die Zuordnungsregel an. Wenn diese Regel dem Dienstleister nicht zugänglich ist, gilt dasselbe wie bei anonymisierten Daten. Für die Verschlüsselung wird vertreten, aufgrund der theoretischen Möglichkeit einer Entschlüsselung – wenn auch mittels großen Zeitaufwands und enormer Rechenkapazität – müsse von einem personenbezogenen Datum und damit von einer Übermittlung ausgegangen werden.[1710] Dem kann jedoch nicht gefolgt werden.[1711] Personenbezug wie Bekanntgeben im Rahmen einer Übermittlung müssen stets relativ zur jeweiligen Stelle betrachtet werden. Eine Übermittlung liegt deshalb immer dann vor, wenn

1703 So *Hermeler* 2000, 167.

1704 Die Bestimmungen über die Gesellschaft für Telematik in §§ 291a, 291b SGB V beinhalten zwar eine Aufgabenzuweisung für die technische Normierung der Infrastruktur, aber keine Befugnis i.S.v. § 4 Abs. 1 BDSG.

1705 Eine solche ist regelmäßig bei einer Datenverarbeitung für mehrere Dritte gegeben, s. *Der Berliner Beauftragte für Datenschutz* 1998, 189.

1706 *Hermeler* 2000, 170.

1707 S. näher unten 4.3.8.2.2, 6.1.1 und 6.3.1.

1708 S.o. 4.3.2.2 und unten 6.3.2.

1709 S.o. 4.1.2.1.

1710 *Hermeler* 2000, 168 i.V.m. 152 ff.

1711 So auch Simitis-*Dammann*, § 3 Rn. 34; *Dierks/Nitz/Grau* 2003, 77.

der Empfänger die Möglichkeit hat, unbehindert vom Weitergebenden die Information zur Kenntnis zu nehmen.[1712] Dies ist aber etwa dann nicht der Fall, wenn im Rahmen einer externen Archivierung ein Datum übermittelt und wieder abgerufen wird, das mit einem Verschlüsselungsverfahren gesichert ist, welches nur mit Rechnerkapazitäten kompromittiert werden kann, die nach dem aktuellen Stand der Technik auch in Rechnerverbünden nicht erreicht werden können. Hier kann nicht davon gesprochen werden, dass ein Bekanntgeben an die Archivierungsstelle erfolgt, auch wenn dies eine „streng rechtsdogmatische“[1713] Betrachtung sein sollte.

Solange nicht über die konkrete technische Ausgestaltung des Umgangs mit den Daten entschieden ist, kann keine abschließende Bewertung für das System der Gesundheitskarte vorgenommen werden. Erfolgt etwa eine Anonymisierung, so kommt es darauf an, ob die übermittelnde oder die Daten empfangende Stelle den Personenbezug beseitigt.[1714] Im zweiten Fall liegt zunächst eine Übermittlung vor. Wird demgegenüber etwa mit Hilfe eines mehrstufigen Verfahrens ein Rückschluss aus den Daten konkreter Behandlungsfälle auf den jeweiligen Versicherten ausgeschlossen,[1715] so sind die Behandlungsdaten für die speichernde Stelle nicht mehr personenbezogen, da sie keine Möglichkeit der Zuordnung hat. Dies gilt umso mehr, wenn darüber hinaus eine verschlüsselte Speicherung erfolgt. Die Frage, ob eine Übermittlung vorliegt, hängt also vom jeweiligen Verfahren, den Verschlüsselungsmechanismen und der verschlüsselnden Stelle ab.

Ist nach diesen Kriterien eine Übermittlung anzunehmen, so ist hierfür entweder eine Einwilligung oder eine gesetzliche Grundlage erforderlich. Letztere könnte sich für Vertragsärzte aus § 28 Abs. 7 BDSG, für die Krankenhäuser aus teilweise bestehenden landesrechtlichen Regelungen ergeben.[1716] Im konkreten Fall kommen allerdings für alle freiwilligen Anwendungen der elektronischen Gesundheitskarte (§ 291a Abs. 3 Satz 1 SGB V) die allgemeinen gesetzlichen Ermächtigungen ohnehin nicht in Betracht. § 291a Abs. 3 Satz 3 SGB V schreibt insoweit das Erfordernis einer Einwilligung für alle Anwendungen nach § 291a Abs. 3 Satz 1 SGB V vor. Aus demselben Grund kommt es bei den freiwilligen Anwendungen für die Frage einer Einwilligungsbedürftigkeit im Ergebnis auch nicht darauf an, ob man in der Übertragung anonymer, pseudonymer und verschlüsselter Daten eine Übermittlung sieht. Auch wenn dies richtigerweise verneint wird, ist nach § 291a Abs. 3 Satz 3 SGB V eine Einwilligung in das Verfahren erforderlich. Zu unterschiedlichen Rechtsfolgen kommen die Auffassungen allerdings dann, wenn es um die Anwendbarkeit einer datenschutzrechtlichen Vorschrift geht, die eine Verarbeitung nach § 3 Abs. 4 BDSG voraussetzt (welche dann in Form einer Übermittlung vorliegt oder nicht vorliegt).

Die Daten des elektronischen Rezepts werden unabhängig vom Willen des Versicherten gespeichert. Gleichzeitig hat sich der Gesetzgeber aber nicht zwischen der serverbasierten Variante und einer Speicherung auf der Gesundheitskarte entschieden. Deshalb fehlt es auch an einer speziellen gesetzlichen Ermächtigung für die Übermittlung an externe Dienstleister. Das Problem wird allerdings entschärft, wenn unter dem Gesichtspunkt der Verhältnismäßigkeit für das elektronische Rezept die Speicherung auf der Gesundheitskarte selbst gewählt wird,[1717] weil dann keine Datenübermittlung an externe Dritte vorliegt. Bei einer Übertragung über Server muss nach geltendem Recht eine sichere Ende-zu-Ende-

1712 Simitis-*Dammann*, § 3 Rn. 152.
1713 So *Hermeler* 2000, 152. Unverständlich bleibt, warum diese Formulierung dort abwertend gebraucht wird.
1714 Zu den unterschiedlichen Möglichkeiten s. *ATG/GVG* 2004a, insbesondere 24 ff., 48 ff.
1715 Zur Funktionsweise s. *BITKOM/VDAP/VHitG/ZVEI* 2003, 27 ff., 30 ff. und unten 6.3.2.
1716 Vgl. für die Rechtslage im Jahr 1999 den Überblick bei *Hermeler* 2000, 174 ff.
1717 S.o. 4.2.3.3.

Verschlüsselung eingesetzt werden, bei der der verordnende Leistungserbringer das Rezept mit dem öffentlichen Schlüssel der Gesundheitskarte verschlüsselt. Dadurch wird eine Kenntnisnahme Dritter ausgeschlossen, sodass externe Dienstleister den Datentransport übernehmen dürfen.

4.3.6.2.2.2 Datenerhebungen zu Zwecken der elektronischen Signatur

Auch wenn die Stelle, die den Chipkartenausweis ausgibt, gleichzeitig für andere Stellen tätig wird, kann sich das Problem der Datenverarbeitung im Auftrag stellen. Eine solche Organisation bietet sich insbesondere dann an, wenn ein Anbieter nicht über ein flächendeckendes Filialnetz verfügt, jedoch aus Sicherheitsgründen nach Möglichkeit in einen direkten Kontakt mit dem Ausweisinhaber treten will.

Ein Beispiel dafür ist die elektronische Signatur. Wenn der digitale Personalausweis in einer Personalausweisbehörde beantragt wird, so können je nach dem gewählten Geschäftsmodell zugleich die Daten für den Zertifizierungsdiensteanbieter erhoben werden.[1718] Eine Übermittlung von Daten aus dem Personalausweisregister ist allerdings aufgrund der Zweckbindungsregelung in § 2b PersAuswG ausgeschlossen.[1719] Danach dürfen die Personalausweisbehörden personenbezogene Daten nur nach Maßgabe des Personalausweisgesetzes, anderer Gesetze oder Rechtsverordnungen erheben, übermitteln, sonst verarbeiten oder nutzen.

Diese Regelung kann auch nicht durch eine Einwilligung des Betroffenen umgangen werden, weil die Befugnisse der Behörde insoweit abschließend gesetzlich festgelegt sind.[1720] Ohne eine gesetzliche Ausnahmeregelung können daher keine Daten des Registers an den Zertifizierungsdiensteanbieter weitergegeben werden.

Wenn die Daten jedoch nicht aus dem Register übermittelt, sondern bei der Beantragung des Personalausweises ausdrücklich für den Zertifizierungsdiensteanbieter erhoben werden,[1721] so liegt kein Fall des § 2b PersAuswG vor.[1722] Diese Form der Datenerhebung und -weitergabe durch die Personalausweisbehörde stellt vielmehr eine zusätzliche Tätigkeit dar, die im Rahmen des Registrierungsprozesses eine reine Hilfsfunktion für den Zertifizierungsdiensteanbieter ist. Auch wenn eine solche Tätigkeit einer öffentlichen Stelle im Auftrag von privaten Unternehmen in der bisherigen Praxis ungewöhnlich ist,[1723] wird dieses Verhältnis zwischen Behörde und Anbieter erfasst, da der Begriff des Auftrags im Rahmen von § 11 BDSG weit zu verstehen ist. Die Anwendung der Norm ist auch angemessen, weil sie etwa dafür sorgt, dass der Zertifizierungsdiensteanbieter nach § 11 Abs. 1 Satz 2 BDSG für das Auskunftsrecht der Signaturschlüssel-Inhaber zuständig ist.

Dennoch bereitet die Umsetzung der Anforderungen des § 11 BDSG in dieser Konstellation Probleme. Zunächst könnten die Kontrollrechte (Zutritt, Einsicht in Unterlagen und andere) und Weisungsbefugnisse, die sich aus dem Über-Unterordnungsverhältnis zu

---

1718 Zu den denkbaren Organisationsabläufen s.u. 5.2.2.

1719 Vgl. zum Folgenden *Roßnagel/Hornung*, in: Reichl/Roßnagel/Müller 2005, 129.

1720 Deswegen greift hier auch die seit dem 11.1.2005 bestehende Möglichkeit (s.u. 5.1.2) nicht ein, mit Einwilligung des Antragstellers auf bereits vorliegende Identifizierungsdaten zurückzugreifen.

1721 Das impliziert keine vollständig getrennten Erhebungsvorgänge. Denkbar wäre auch, die Daten nur einmal zu erheben und dann (nach Einwilligung des Antragstellers zur Weitergabe an den Zertifizierungsdiensteanbieter) gleichzeitig in das Register aufzunehmen und an den Anbieter zu übermitteln. Auch dies wäre keine Übermittlung aus dem Register.

1722 Vgl. *Roßnagel/Hornung*, in: Reichl/Roßnagel/Müller 2005, 129.

1723 Eine ähnliche Konstellation könnte sich im Rahmen von neueren Ansätzen im Electronic Government zum sog. „Lebenslagenkonzept“ ergeben, bei dem Daten einmalig erhoben und dann an unterschiedliche staatliche und private Anbieter weitergeleitet werden, s. *Wulff* 2002.

Lasten der Behörde ergeben, in Widerspruch zu deren hoheitlicher Tätigkeit stehen. Dies ließe sich dadurch vermeiden, dass die Kontrollrechte strikt auf den Prozess der Registrierung beschränkt würden.[1724] Der normale Verfahrensablauf in der Behörde würde davon nicht berührt. Schwierigkeiten ergeben sich aber daraus, dass die Personalausweisbehörde die beschriebenen Funktionen grundsätzlich für jeden Zertifizierungsdiensteanbieter am deutschen oder europäischen Markt erfüllen müsste. Auch wenn die Behörde an sich im Rahmen der Datenerhebung und Kartenausgabe eine reine Hilfsfunktion ausübt, ist es nicht praktikabel, jedem Anbieter für seinen konkreten Datenerhebungs- und Kartenausgabeprozess ein Weisungsrecht gegenüber der Behörde einzuräumen. Als Lösung bietet sich an, diese Prozesse als gesetzliche Pflicht der Behörde zu normieren.[1725] Die Daten für die Zertifizierungsdiensteanbieter würden dann in einer standardisierten Form über eine Schnittstelle angeboten, die Signaturkarten in einer bestimmten Form angeliefert und in einem identischen Verfahren ausgegeben werden.

Die Problematik stellt sich auch für andere vergleichbare geplante Ausgabeprozesse, wie zum Beispiel für den elektronischen Heilberufsausweis. Würde dieser von den berufständischen Kammern ausgestellt, so wäre es denkbar, dass diese wie die Personalausweisbehörden die Datenerhebung für die Zertifizierungsdiensteanbieter übernehmen. Der neue § 291a Abs. 5a SGB V überträgt die Bestimmung der Ausgabeprozesse auf die Bundesländer. Diese bereiten derzeit gesetzliche Regelungen vor.[1726]

4.3.6.3 Einrichtung automatisierter Abrufverfahren (§ 10 BDSG)

Neben § 11 BDSG enthält auch § 10 BDSG eine Regelung für die Übermittlung von Daten. Er betrifft allerdings nicht die Zulässigkeit des Abrufs von Daten in automatisierten Verfahren, sondern die der Einrichtung des Verfahrens selbst.[1727] Dahinter steht der Gedanke, dass bereits hierdurch ein Gefährdungspotential für das Recht auf informationelle Selbstbestimmung begründet wird.[1728]

4.3.6.3.1 Anwendbarkeit

§ 10 BDSG greift dann nicht ein, wenn für den jeweiligen Chipkartenausweis speziellere Bestimmungen einschlägig sind. Das ist bei einer Übermittlung aus dem Personalausweisregister der Fall. Nach § 2b Abs. 3 PersAuswG ist hier ein Ersuchen der anfragenden Behörde formelle Voraussetzung. Das schließt automatisierte Abrufverfahren aus.[1729] Für das JobCard-Verfahren wird es eine spezialgesetzliche Regelung geben, die die Befugnis des Mitarbeiters der Arbeitsagentur zum Datenabruf und die technischen Anforderungen (qualifizierte Signatur des Antragstellers und des Mitarbeiters) regeln und § 10 BDSG verdrängen wird.

1724 So bestünden etwa keine Weisungs- oder Zugriffsbefugnis hinsichtlich der Daten, die für den Zertifizierungsdiensteanbieter irrelevant sind, nämlich Ordens- und Künstlername (es sei denn, sie werden als Pseudonym verwendet), Größe und Augenfarbe.

1725 S. *Roßnagel/Hornung*, in: Reichl/Roßnagel/Müller 2005, 225.

1726 S. näher unten 5.2.2.

1727 Insofern kann man von einer zweistufigen Zulässigkeitsprüfung sprechen, s. *Bergmann/Möhrle/Herb*, § 10 Rn. 6; Simitis-*Ehmann*, § 10 Rn. 37; *Gola/Schomerus*, § 10 Rn. 4. § 10 BDSG ist neben den oben angesprochenen Normen des TDDSG anwendbar, s. RMD-*Bizer*, § 3 TDDSG 1997 Rn. 51 ff.; Roßnagel-*Roßnagel*, Kap. 7.9, Rn. 38.

1728 *Lennartz*, RDV 1990, 25, 29 f.; *Gola/Schomerus*, § 10 Rn. 2.

1729 AG Stuttgart, DuD 2003, 649, 651 (zur gleichlautenden Norm des § 22 PassG) und oben 2.2.1.4.

Fraglich ist, ob auch bei der elektronischen Gesundheitskarte derartige Spezialregelungen existieren. § 291a Abs. 4 SGB V betrifft lediglich die Zulässigkeit der einzelnen Abrufe, nicht aber die der Einrichtung des Verfahrens selbst. § 10 BDSG wird auch nicht von § 291a Abs. 7 und § 291b SGB V verdrängt, wonach die Spitzenverbände der Beteiligten an der Selbstverwaltung die Einrichtung der Telematik-Infrastruktur vereinbaren. Diese haben vielmehr bei der Regelung der Struktur umgekehrt die Anforderungen des § 10 BDSG zu beachten.

Für die Anwendbarkeit der Norm muss es sich um ein automatisiertes Verfahren handeln, das die Übermittlung personenbezogener Daten durch Abruf ermöglicht. Hierfür kommen im System der Gesundheitskarte zwei Sachverhalte in Betracht: zum einen die Einbeziehung externer Dritter, die Daten vorhalten, zum anderen aber auch die verteilte Datenhaltung durch Leistungserbringer, sofern ein Abruf und keine Überprüfung und Übermittlung im Einzelfall erfolgt.

In beiden Fällen liegt ein automatisiertes Verfahren vor. Für eine Übermittlung (§ 3 Abs. 4 Nr. 3 BDSG) müssten die Leistungserbringer im Verhältnis zueinander beziehungsweise zum externen Dienstleister Dritte im Sinne von § 3 Abs. 8 Satz 2 und 3 BDSG sein. Es wurde bereits im Rahmen der Abgrenzung zwischen Datenverarbeitung im Auftrag und Funktionsübertragung festgestellt, dass dies der Fall ist.[1730] Die oben angesprochenen Probleme anonymer, pseudonymer und verschlüsselter Daten stellen sich hier insofern nicht, als die Daten bei der abrufenden Instanz stets lesbar und personenbezogen vorliegen müssen. Sofern eine Transportverschlüsselung vorgenommen wird, liegt zumindest im Verhältnis zwischen dem absendenden und dem empfangenden Leistungserbringer eine Übermittlung vor. Damit ist dieses Tatbestandsmerkmal von § 10 Abs. 1 BDSG erfüllt. Im Übrigen wäre auch dann, wenn nur wenige personenbezogene Daten im System übermittelt werden, das gesamte Verfahren von § 10 BDSG erfasst.[1731]

§ 10 BDSG betrifft auch Verfahren, an denen eine Vielzahl von Stellen beteiligt ist, wie beispielsweise Netze im Gesundheitswesen zum gegenseitigen Zugriff auf Datenbestände.[1732] Soweit also im Rahmen des Einsatzes der Gesundheitskarte externe Server oder wechselseitige Zugriffsverfahren zwischen den Leistungserbringern eingesetzt werden, ist § 10 BDSG anwendbar.[1733]

4.3.6.3.2 Angemessenheit der Einrichtung (§ 10 Abs. 1 BDSG)

Nach § 10 Abs. 1 Satz 1 BDSG ist eine Angemessenheitsprüfung des automatisierten Abrufverfahrens vorzunehmen, wobei unter anderem[1734] die schutzwürdigen Interessen der Betroffenen und die Aufgaben oder Geschäftszwecke der beteiligten Stellen abzuwägen sind. Auf der Seite der Betroffenen sind insbesondere die spezifischen Gefahren für das Recht auf informationelle Selbstbestimmung zu berücksichtigen.[1735] Diese sind umso größer, je mehr Daten über einen einzelnen Betroffenen zum Abruf bereitgestellt werden, und verstärken sich dann, wenn es sich um besondere Arten personenbezogener Daten oder

1730 S.o. 4.3.6.2.2.1. Automatisiertes Abrufverfahren und Datenverarbeitung im Auftrag schließen sich gegenseitig aus.

1731 Simitis-*Ehmann*, § 10 Rn. 28.

1732 Simitis-*Ehmann*, § 10 Rn. 9, 14.

1733 Ebenso *Hermeler* 2000, 169; *Bultmann/Wellbrock/Biermann/Engels/Ernestus/Höhn/Wehrmann/Schurig* 2002, 9 (allerdings ohne nähere Begründung).

1734 Die Aufzählung ist nicht abschließend, s. Simitis-*Ehmann* § 10 Rn. 55. Indizien für weitere Faktoren können sich insbesondere aus den nach § 10 Abs. 2 BDSG schriftlich festzuhaltenden Elementen ergeben, s. *Stange* 1992, Rn. 133; Simitis-*Ehmann*, § 10 Rn. 51, 56 ff.

1735 *Gola/Schomerus*, § 10 Rn. 11; Simitis-*Ehmann*, § 10 Rn. 48; s.a. *Lennartz*, RDV 1990, 25, 29.

Angaben handelt, die einem Berufsgeheimnis unterfallen.[1736] Auf der anderen Seite können technische und organisatorische Maßnahmen nach § 9 BDSG und der zugehörigen Anlage die schutzwürdigen Interessen der Betroffenen wahren und damit die Angemessenheit begründen.[1737] Gleiches gilt für Massenverfahren, die nur in automatisierter Form durchgeführt werden können.[1738] Eine Beschleunigung des Ablaufs und Wirtschaftlichkeitserwägungen begründen nicht per se eine Angemessenheit des Verfahrens.[1739] Sie sind jedoch dann zu berücksichtigen, wenn sie zu konkreten Verbilligungen für die Betroffenen führen.[1740]

Gegen die Angemessenheit der Einrichtung eines automatisierten Abrufverfahrens bei der elektronischen Gesundheitskarte spricht, dass es sich bei den Gesundheitsdaten um besondere Arten personenbezogener Daten im Sinne von § 3 Abs. 9 BDSG handelt,[1741] die überdies durch die gesetzliche Schweigepflicht geschützt sind. Außerdem können gerade bei chronisch Kranken durch die Masse der Daten sensible Informationsmengen entstehen. Auf der anderen Seite dient die Einrichtung des Verfahrens der Verbesserung der medizinischen Versorgung der Betroffenen und der Beitragsstabilität. Letzteres, also eine Verbilligung des Verfahrens, vermag zwar nicht allein den Ausschlag zu geben. Gegen das Argument, ein billigeres Verfahren beim Anbieter diene letztlich auch dem Kunden, ist nämlich einzuwenden, dass Rationalisierungsmaßnahmen zumindest teilweise auch der Gewinnsteigerung des Verwenders des Verfahrens dienen. Die Situation ist im Bereich der gesetzlichen Krankenkassen jedoch anders, weil diese nicht auf Gewinnerzielung ausgerichtet sind, sondern die Einsparungen aufgrund der paritätischen Finanzierung unmittelbar den Versicherten zugute kommen. Hierin liegt ein grundlegender Unterschied zum Normalfall des § 10 BDSG. Darüber hinaus sprechen für eine Angemessenheit des Abrufverfahrens die im Rahmen des Systems zu erfüllenden Anforderungen an die Datensicherheit.[1742] Hierdurch werden die Risiken für die Betroffenen wesentlich reduziert.

Vom typischen Fall eines automatisierten Abrufverfahrens unterscheidet sich das Abrufverfahren mittels der elektronischen Gesundheitskarte auch durch das Mitwirkungserfordernis des Versicherten im Einzelfall. Dieses wirkt sich auf die Angemessenheit des gesamten Verfahrens aus. Im Bereich der freiwillige Anwendungen nach § 291a Abs. 3 Satz 1 SGB V, bei denen regelmäßig sensiblere Daten verarbeitet werden als bei den verpflichtenden Anwendungen, ergibt sich sogar eine doppelte Mitwirkung des Versicherten. Zunächst ist nach § 291a Abs. 3 Satz 3 SGB V eine generelle Einwilligung in die Einrichtung des Verfahrens, darüber hinaus gemäß § 291a Abs. 5 Satz 1 und 2 SGB V eine technisch abgesicherte Autorisierung durch den Versicherten im Einzelfall erforderlich. Die Verfahren, die normalerweise § 10 BDSG unterfallen, werden dagegen ohne jede Mitwirkung des Betroffenen eingerichtet. Für den konkreten Übermittlungsvorgang ist zwar stets

1736 Simitis-*Ehmann*, § 10 Rn. 64, 66, 75.
1737 Simitis-*Ehmann*, § 10 Rn. 67.
1738 *Bergmann/Möhrle/Herb*, § 10 Rn. 14; Simitis-*Ehmann*, § 10 Rn. 72; *Gola/Schomerus*, § 10 Rn. 11; *Tinnefeld/Ehmann* 1998, 240; s.a. die Begründung des Regierungsentwurfs, BT-Drs. 11/4306, 43; Bsp. bei Roßnagel-*Duhr*, Kap. 7.5, Rn. 68.
1739 Simitis-*Ehmann*, § 10 Rn. 69, 73; *Bergmann/Möhrle/Herb*, § 10 Rn. 12; *Gola/Schomerus*, § 10 Rn. 11. Viel zu weitgehend deshalb Roßnagel-*Duhr*, Kap. 7.5, Rn. 68, wonach schutzwürdige Interessen dann nicht vorliegen sollen, wenn das Abrufverfahren dazu führt, dass die Betroffenen eine gewünschte Ware oder einen beantragten Kredit zügiger erhalten. Ein derartiges Kriterium würde jede sinnvolle Abwägung mit den Persönlichkeitsrechten der Betroffenen unmöglich machen.
1740 Simitis-*Ehmann*, § 10 Rn. 73.
1741 S. dazu oben 4.3.4.2.2.
1742 S. näher unten 4.3.8.

eine gesetzliche Ermächtigung oder eine Einwilligung des Betroffenen erforderlich.[1743] Bei der Gesundheitskarte findet jedoch darüber hinaus bei jedem Übermittlungsvorgang der freiwilligen Anwendungen eine aktive Mitwirkung des Versicherten (PIN-Eingabe) statt. Diese Mitwirkung sorgt für eine Kontrollmöglichkeit des Betroffenen und spricht entscheidend dafür, dass das automatisierte Abrufverfahren bei der Gesundheitskarte angemessen ist.

4.3.6.3.3 Anforderungen aus § 10 Abs. 2 und 4 BDSG

Weiter bestimmt § 10 Abs. 2 BDSG, dass Anlass und Zweck des Verfahrens, die Datenempfänger, die Art der zu übermittelnden Daten und die nach § 9 BDSG erforderlichen Maßnahmen schriftlich festzulegen sind.[1744] Bei der Gesundheitskarte steht diese Norm mit § 291b Abs. 1 SGB V im Zusammenhang, wonach die Gesellschaft für Telematik ein Sicherheitskonzept zu erstellen und Inhalt und Struktur der Datensätze für deren Bereitstellung und Nutzung festzulegen hat. Im Rahmen dieser Festlegungen sollten zweckmäßigerweise die nach § 10 Abs. 2 BDSG erforderlichen Punkte beschrieben werden.

§ 10 Abs. 4 BDSG regelt die Verantwortlichkeit für einzelne Datenabrufe. Diese liegt bei der abrufenden Stelle.[1745] Des Weiteren hat die speichernde Stelle eine stichprobenartige Überprüfung der Zulässigkeit der einzelnen Abrufe durchzuführen.[1746] § 10 Abs. 4 BDSG wird für die Gesundheitskarte jedoch durch die spezielleren Vorschriften in § 291a Abs. 4 und 5 SGB V verdrängt. Aufgrund der dort normierten technischen und rechtlichen Absicherung besteht kein Raum mehr für die Anwendung der allgemeinen Regelung in § 10 Abs. 4 BDSG und insbesondere keine Notwendigkeit für den Dienstleister, nach § 10 Abs. 4 Satz 3 BDSG die Zulässigkeit der Abrufe zu prüfen.

4.3.7 Besonderheiten der Betroffenenrechte

4.3.7.1 Die Rechte des Betroffenen

Der von der Datenverarbeitung Betroffene hat nach dem deutschen Datenschutzrecht die Rechte auf Auskunft, Widerspruch, Berichtigung, Löschung, Sperrung und Schadensersatz.[1747] Nach § 6 Abs. 1 BDSG kann auf das Auskunfts-, Berichtigungs-, Löschungs- und Sperrungsrecht nicht rechtsgeschäftlich verzichtet werden. Betroffenenrechte finden sich auch durchweg in internationalen Rechtsquellen. Die europäische Datenschutzrichtlinie umfasst dieselben Rechte wie das Bundesdatenschutzgesetz.[1748] Auskunft, Berichtigung und Löschung finden sich auch in Art. 8 des Übereinkommens des Europarats.[1749] Die Charta der Grundrechte der Europäischen Union (Art. 8 Abs. 2 Satz 2) beinhaltet nur Auskunfts- und Berichtigungsrechte, während die Richtlinien der Generalversammlung der Vereinten Nationen (Nr. 4) und die OECD-Richtlinien (Art. 13) lediglich ein Auskunfts-

1743 Nach § 10 Abs. 1 Satz 2 BDSG bleibt die Zulässigkeit des einzelnen Abrufs unberührt.
1744 Näher *Gola/Schomerus*, § 10 Rn. 12 ff.; Simitis-*Ehmann*, § 10 Rn. 83 f.
1745 Vgl. im Einzelnen Simitis-*Ehmann*, § 10 Rn. 90 ff.
1746 Näher *Auernhammer*, § 10 Rn. 15; *Bergmann/Möhrle/Herb*, § 10 Rn. 36 ff.; Roßnagel-*Duhr*, Kap. 7.5, Rn. 70 ff.; Simitis-*Ehmann*, § 10 Rn. 101 ff.
1747 S. allgemein Roßnagel-*Wedde*, Kap. 4.4, Rn. 12 ff.; *Gola/Klug* 2003, 52 ff.; *Tinnefeld/Ehmann* 1998, 336 ff., 385 ff.
1748 S. Art. 12 (Auskunft, Berichtigung, Löschung und Sperrung), Art. 14 (Widerspruch) und Art. 23 (Schadensersatz) DSRL.
1749 Vgl. *Henke* 1986, 127 ff.

recht vorsehen.[1750] Aus Art. 8 Abs. 1 EMRK lässt sich die Notwendigkeit von Auskunfts-, Berichtigungs- und Löschungsansprüchen ebenfalls ableiten, auch wenn der Europäische Gerichtshof für Menschenrechte sich bislang lediglich zu ersteren geäußert hat.[1751]

Das Auskunftsrecht nach §§ 19, 34 BDSG ist ein Instrument vorgelagerten Rechtsschutzes und dient dazu, durch individuelle Unterrichtung für den Betroffenen Transparenz hinsichtlich der über ihn erhobenen, verarbeiteten und genutzten Daten zu ermöglichen,[1752] beziehungsweise – in den Worten des Bundesverfassungsgerichts – sicherzustellen, dass die Bürger erfahren „wer was wann und bei welcher Gelegenheit über sie weiß".[1753]

Mit seinem Widerspruch gemäß §§ 20 Abs. 5, 28 Abs. 4, 35 Abs. 5 BDSG bringt der Betroffene zum Ausdruck, dass er Einwände gegen eine an sich rechtmäßige Datenverwendung hat. Er hat damit die Möglichkeit, schutzwürdige Interessen, die in seiner Person liegen, geltend zu machen. Sofern diese Interessen wegen der besonderen persönlichen Situation das Interesse an der Datenverwendung überwiegen, hat diese zu unterbleiben. Das gilt allerdings nicht, sofern eine Rechtsvorschrift zur Erhebung, Verarbeitung oder Nutzung verpflichtet.

Sind Daten unrichtig, so sind sie zu berichtigen (§§ 20 Abs. 1, 35 Abs. 1 BDSG). Wenn die Speicherung unzulässig oder die Kenntnis der Daten zur Aufgabenerfüllung nicht mehr erforderlich ist, besteht ein Anspruch auf Löschung (§§ 20 Abs. 2, 30 Abs. 3, 35 Abs. 2 BDSG). Dasselbe gilt nach § 35 Abs. 2 Nr. 2 BDSG im nichtöffentlichen Bereich, wenn besondere Arten personenbezogener Daten gespeichert werden und ihre Richtigkeit nicht bewiesen werden kann. An die Stelle der Löschung kann unter bestimmten Voraussetzungen die Sperrung treten (§§ 20 Abs. 3, 4 und 6, 28 Abs. 4 Satz 3, 35 Abs. 3 und 4 BDSG).

Schadensersatzansprüche des Betroffenen ergeben sich schließlich aus §§ 7, 8 BDSG. Nach der Grundnorm des § 7 BDSG besteht eine Ersatzpflicht, sofern durch unzulässige oder unrichtige Erhebung, Verarbeitung oder Nutzung ein Schaden entstanden ist. Die zuständige Stelle kann sich aber durch den Nachweis sorgsamen Verhaltens exkulpieren. § 8 BDSG sieht demgegenüber für den Bereich der automatisierten Datenverarbeitung durch öffentliche Stellen eine Gefährdungshaftung vor.

Bei Chipkartenausweisen ergeben sich bezogen auf die Mehrzahl der Transparenz- und Korrekturrechte keine Besonderheiten.[1754] Wenn allerdings wie beim digitalen Personalausweis und der elektronischen Gesundheitskarte die Erhebung, Verarbeitung und Nutzung der Daten durch Gesetz geregelt ist, bleibt ein eventueller Widerspruch hiergegen ohne Wirkung. Darüber hinaus sind sowohl für den digitalen Personalausweis als auch für die elektronische Gesundheitskarte spezielle Betroffenenrechte normiert, die den allgemeinen datenschutzrechtlichen Bestimmungen vorgehen. Für das JobCard-Verfahren bestehen bislang keine Sonderregeln.

4.3.7.2 Betroffenenrechte beim digitalen Personalausweis

§ 3 Abs. 5 Satz 2 PersAuswG gibt dem Personalausweisinhaber das Recht, Auskunft über „den Inhalt der verschlüsselten Merkmale und Angaben" auf dem Ausweis zu erhalten. Hier stellt sich – parallel zur Zweckbindung nach § 3 Abs. 5 Satz 1 PersAuswG – das

1750 Zumindest dieses Recht auf Auskunft oder Zugang zu den Daten ist im Grundsatz universell anerkannt, s. *Banisar/Davies*, J. Marshall J. Computer & Info. L. 1999, 1, 11.

1751 S. *Matz* 2003, 133 ff. m.w.N. zur Rspr. des EGMR.

1752 *Roßnagel/Pfitzmann/Garstka* 2001, 170 f.

1753 BVerfGE 65, 1 (43).

1754 Zur Anwendung der Betroffenenrechte auf Chipkarten s. insoweit Roßnagel-*Weichert*, Kap. 9.5, Rn. 47 ff.; *Bizer* 2002, 29 ff.

Problem der Auslegung des Tatbestandsmerkmals „verschlüsselt“.[1755] Da das Auskunftsrecht des Betroffenen ebenso wie die Zweckbindung der Daten zu den verfassungsrechtlichen Anforderungen des Grundrechts auf informationelle Selbstbestimmung gehört,[1756] müssen beide Sätze des § 3 Abs. 5 PersAuswG identisch interpretiert werden. Der Inhaber kann also über alle elektronisch gespeicherten Daten, die für ihn nicht visuell erkennbar sind, Auskunft verlangen.

§ 3 Abs. 5 Satz 2 PersAuswG verlangt nur die Auskunft selbst, ohne nähere Angaben über die Modalitäten zu machen. Die Umsetzung kann auf unterschiedlichen Wegen erfolgen. Für die biometrischen Daten ergeben sich Schwierigkeiten daraus, dass sie regelmäßig für eine Verkörperung in Papierform nicht geeignet sind. Zwar lassen sich Volldatensätze noch graphisch darstellen, bei der Iris kann der Betroffene aber bereits kaum noch kontrollieren, ob die Daten korrekt sind. Werden demgegenüber Templates gespeichert, ist eine Auskunft in Papier weder möglich noch sinnvoll. Die Daten sind deshalb in elektronischer Form zu übermitteln. Allerdings werden nur die wenigsten Betroffenen über die technischen Möglichkeiten verfügen, diese Daten zu prüfen. Für die Mehrheit der Betroffenen geht es aber auch weniger um die konkrete Datenstruktur, sondern um die Auskunft, welches biometrische Merkmal in welcher Form auf der Karte gespeichert ist, und insbesondere darum, ob es sich um ihr eigenes Merkmal handelt. Deshalb sind für die Auskunft grundsätzlich entsprechende Prüfgeräte in den Personalausweisbehörden oder an öffentlichen oder halböffentlichen Kiosken vorzuhalten.[1757]

Erfolgt eine derartige technische Umsetzung des Auskunftsrechts, so ist auch den grundrechtlichen Transparenzanforderungen Genüge getan. In diesem Fall kann keine Rede davon sein, dass die Verschlüsselung der Daten das Auskunftsrecht „entzieht“.[1758] Der ganz überwiegende Teil des staatlichen Datenbestandes ist zunächst für die Betroffenen intransparent und setzt staatliche Mitwirkung bei der Auskunftserteilung voraus. Es ist also aus verfassungsrechtlicher Sicht nicht notwendig, lediglich visuell erkennbare Merkmale auf den Ausweis aufzubringen.

4.3.7.3 Betroffenenrechte bei der elektronischen Gesundheitskarte

Patienten steht gegenüber Leistungserbringern ein generelles Einsichtsrecht in die gespeicherten Daten zu, das vom Bundesgerichtshof seit dem Jahre 1982 als Nebenpflicht aus dem Behandlungsvertrag abgeleitet wird[1759] und neben das datenschutzrechtliche Auskunftsrecht tritt. Es bezieht sich allerdings nur auf „naturwissenschaftlich objektivierbare Befunde“ und „Behandlungsfakten, die die Person des Patienten betreffen“ und wird deshalb von der Rechtsprechung dann eingeschränkt, wenn ein schützenswertes Interesse des Patienten selbst, eines Arztes oder Dritten entgegensteht. Solche Fälle können sich insbesondere im Bereich der Psychiatrie ergeben. Zwar besteht auch hier ein grundsätzliches Recht auf Einsicht in Krankenunterlagen.[1760] Ausgehend vom ärztlichen Auftrag des ’nihil nocere’ soll dies jedoch dann nicht gelten, wenn die Auskunft den Zustand des Pati-

1755 Vgl. bereits oben 4.2.2.3.
1756 S.o. 4.2.1.2.5.
1757 Wenn der digitale Personalausweis in seiner technischen Ausgestaltung von § 3 Abs. 10 BDSG erfasst wird, ist dies bereits nach § 6c Abs. 2 BDSG erforderlich, s.o. 4.3.3.4.
1758 So aber *Chaos Computer Club* 2001; *Koch* 2002, 24.
1759 BGHZ 85, 327 (331 ff.); 85, 339 ff.; ebenso BVerfG, MedR 1993, 232; 1999, 180; *Gola/Schomerus*, § 34 Rn. 15 m.w.N.; s. zur Herleitung auch *Meier* 2003, 105 f. m.w.N.
1760 BGH, NJW 1985, 674 ff.

enten verschlimmern würde.[1761] Auch die Regelung in § 10 Abs. 2 MBO-Ä 2004 schränkt das Auskunftsrecht ein: Danach wird auf Verlangen Einsicht in die Teile der Unterlagen gewährt, die den Patienten betreffen, nicht jedoch in diejenigen Abschnitte, die subjektive Eindrücke oder Wahrnehmungen des Arztes enthalten.[1762] Im Datenschutzrecht ermöglicht Art. 13 Abs. 1 lit. g DSRL eine Beschränkung des Auskunftsrechts, sofern dies zum Schutz der betroffenen Person notwendig ist.[1763]

Für die elektronische Gesundheitskarte normiert § 291a Abs. 4 Satz 2 SGB V ein Recht der Versicherten „auf die Daten nach Absatz 2 Satz 1 und Absatz 3 Satz 1 zuzugreifen". Diese Formulierung spricht zunächst für ein eigenes technisches Zugriffsrecht. Zu beachten ist jedoch das Zusammenspiel mit § 291a Abs. 5 Satz 3, 1. Halbsatz SGB V, der einen Zugriff nur unter Verwendung eines elektronischen Heilberufsausweises zulässt. Vertreten wird, dies betreffe nur Verarbeitungen durch andere als den Betroffenen, sodass eine Einbeziehung von Leistungserbringern bei der Wahrnehmung des Auskunftsrechts rechtlich nicht geboten sei.[1764] Dem kann jedoch nicht gefolgt werden. § 291a Abs. 5 Satz 3, 2. Halbsatz SGB V bestimmt nämlich, dass in Abweichung von der Regelung im 1. Halbsatz der Karteninhaber auf die selbst zur Verfügung gestellten Daten auch mit einer eigenen qualifizierten Signaturkarte zugreifen kann. Hieraus folgt im Umkehrschluss, dass für die Daten der übrigen Anwendungen kein eigener Zugriff eröffnet ist. § 291a Abs. 4 Satz 2 SGB V normiert deshalb im Ergebnis ein datenschutzrechtliches Auskunftsrecht,[1765] während eine Zugriffsmöglichkeit nur für die selbst zur Verfügung gestellte Daten sowie für das elektronische Rezept besteht, weil der Inhaber dieses nach § 291a Abs. 5 Satz 5 SGB V auch ohne Mitwirkung eines Leistungserbringers freischalten kann.

Das Auskunftsrecht in § 291a Abs. 4 Satz 2 SGB V sieht keine Beschränkungen entsprechend § 10 Abs. 2 MBO-Ä 2004 und den von der Rechtsprechung entwickelten Grundsätzen vor. Angesichts des deutlichen Wortlauts ist es auch nicht möglich, diese in die Bestimmung hineinzuinterpretieren, sodass über den gesamten Inhalt der auf oder mittels der elektronischen Gesundheitskarte gespeicherten Daten Auskunft zu erteilen ist. Auch das datenschutzrechtliche Transparenzprinzip fordert, dass auf Chipkarten keine Daten gespeichert werden, von denen der Inhaber keine Kenntnis hat.[1766] Das führt dazu, dass das ärztliche Standesrecht und die genannte Rechtsprechung – jenseits der Frage, ob die entwickelten Einschränkungen gerechtfertigt sind[1767] – in diesem Punkt obsolet sind.

1761 Sog. „therapeutisches Privileg", s. *Deutsch*, NJW 1980, 1305 ff.; *Hollmann* 1979, 45; *Menzel/Schläger*, DuD 1999, 70, 74; Laufs/Uhlenbruck-*Uhlenbruck/Schlund* 2002, 488 f.; Roßnagel-*Schirmer*, Kap. 7.12, Rn. 30; LG Saarbrücken, MedR 1995, 323 ff. (kritisch zur dortigen Begründung *Bäumler*, MedR 1998, 400, 401).

1762 Das ist allerdings nach den von den Ärztekammern beschlossenen Berufsordnungen tlw. anders geregelt.

1763 Dazu *Dammann/Simitis* 1997, Art. 13 Rn. 11; *Ehmann/Helfrich* 1999, Art. 13 Rn. 71 ff.

1764 So *Weichert*, DuD 2004, 391, 398.

1765 Perspektivisch wäre ein selbständiger Zugriff des Versicherten durchaus wünschenswert, s.o. 4.2.3.6.

1766 S. schon *Roßnagel* 1994b, 271; für das Gesundheitswesen vgl. *BSI* 1995, XIV, 56.

1767 Diese liegt außerhalb des Themas der Arbeit. Ein unbeschränktes Auskunftsrecht auch über subjektive Eindrücke und psychiatrische Befunde wird gefordert von *Beier* 1979, 102 f.; *Kilian* 1979, 127; *Giesen*, JZ 1982, 391, 392; *Kersten*, CR 1989, 1020, 1026; *Vahle*, DuD 1991, 614, 618; mit Kritik am BGH auch *Scheiwe*, KritV 1998, 313 ff.; anders demgegenüber *Hollmann* 1979, 44 f. (eine allgemeine Auskunft könne Angst „bis zur Beseitigung des Lebenswillens" herbeiführen); ähnlich *Auernhammer*, § 19 Rn. 19; *Schmidt-Beck* 1994, 222; Laufs/Uhlenbruck-*Uhlenbruck/Schlund* 2002, 490 f.; vermittelnd *GDD* 2002, 44; Simitis-*Mallmann*, § 33 Rn. 68, wonach Einschränkungen bei Gefahr für Leib und Leben, sowie für Genesung und Therapieprozess gerechtfertigt sind, dann aber eine Überprüfung in zeitlich vertretbaren Abständen zu erfolgen hat; s.a. die Richtlinien der *BÄK*, DÄ 1996, A-2809, 2811.

Es ist nicht möglich, mittels der Gesundheitskarte Daten zu transportieren, über die der Versicherte keine Auskunft verlangen kann.[1768] Dies könnte allerdings auch den Effekt haben, dass die jeweiligen Leistungserbringer an dieser Stelle keine vollständigen Angaben mehr machen, weil sie damit rechnen müssen, dass der Versicherte Kenntnis von ihren subjektiven Eindrücken erhält oder Informationen im therapeutischen Bereich erlangt, die seiner Gesundheit schädlich sein könnten. Ob diese Einschränkung wirklich zu unvollständigen Angaben führt und dies die Versorgung beeinträchtigen könnte, ist allerdings schwer abzuschätzen.

Zur Umsetzung des Auskunftsrechts bei der elektronischen Gesundheitskarte gibt es mehrere Möglichkeiten. Die Auskunft könnte durch einen (beliebigen) Leistungserbringer erteilt werden, der über einen elektronischen Heilberufsausweis verfügt. In diesem Fall muss sichergestellt werden, dass keine Übernahme von Fremddaten in die Dokumentation des Auskunft erteilenden Leistungserbringers erfolgt.[1769] Denkbar ist ein Ausdruck der Daten, die auf oder mittels der elektronischen Gesundheitskarte gespeichert sind.[1770] Da § 291a Abs. 2 Satz 2 und Abs. 3 Satz 5 SGB V auf § 6c Abs. 2 BDSG verweisen, hat der Gebrauch von Geräten und Einrichtungen zur Wahrnehmung des Auskunftsrechts unentgeltlich zu erfolgen. Das schließt auch eine Praxisgebühr (§ 28 Abs. 4 SGB V) aus. Allerdings könnte der Leistungserbringer durch die Krankenkasse eine Vergütung für die Auskunft erhalten. Überdies umfasst das unentgeltliche Auskunftsrecht keine umfassenden Erläuterungen und Interpretationen durch den Leistungserbringer, der den Zugriff auf die Karte ermöglicht. Wird dies vom Versicherten gewünscht, so handelt es sich vielmehr um eine normale Dienstleistung des Leistungserbringers, für die dieser eine Vergütung verlangen darf.

Neben dem speziellen Auskunftsrecht in § 291a Abs. 4 Satz 2 SGB V beinhaltet § 291a Abs. 6 Satz 1 SGB V ein besonderes Löschungsrecht für die Daten des elektronischen Rezepts und aller freiwilligen Anwendungen nach § 291a Abs. 3 Satz 1 SGB V.[1771] Fraglich ist, inwieweit dieses Löschungsrecht teilbar ist. Der Wortlaut ist insoweit offen. Bei den meisten Anwendungen bestehen keine Bedenken dagegen, auch einzelne Datensätze (etwa ein einzelnes Rezept) von der Karte zu löschen. Für die Daten zur Prüfung der Arzneimitteltherapiesicherheit und die elektronische Patientenakte gilt jedoch die Besonderheit, dass diese auf Vollständigkeit angelegt sind. Es würde den Sinn der Datenspeicherung vereiteln, wenn der Karteninhaber einzelne Datenteile löschen lassen könnte, der jeweilige Leistungserbringer jedoch von der Vollständigkeit der Dokumentation ausginge.[1772] Deshalb kann das Löschungsrecht nur insgesamt ausgeübt werden.

§ 291a Abs. 6 Satz 1 SGB V bezieht sich ausschließlich auf die auf oder mittels der elektronischen Gesundheitskarte gespeicherten Daten. Aus der Norm folgt keine Befugnis, eine Löschung von Daten zu verlangen, die bei dem jeweiligen Leistungserbringer gespei-

1768 S.a. *Weichert*, DuD 2004, 391, 396; *Iwansky* 1999, 107.

1769 *Weichert*, DuD 2004, 391, 398.

1770 Roßnagel-*Schirmer*, Kap. 7.12, Rn. 96. § 10 Abs. 2 Satz 2 MBO-Ä 2004 bestimmt, dass der Patient die Unterlagen nicht selbst kopieren darf, ihm jedoch gegen Kostenerstattung Kopien auszuhändigen sind; s. dazu *GDD* 2002, 44; *Klöcker/Meister* 2001, 60 f.

1771 Auch aus diesem Grund muss weiterhin eine Dokumentation bei dem jeweils behandelnden Leistungserbringer erfolgen (s.a. oben 4.2.3.3). Andernfalls wären die Daten insgesamt nicht mehr verfügbar.

1772 Ein ähnliches Problem stellt sich bei der Frage, ob es möglich ist, eine Pflicht zur Benutzung der Karte in jedem Einzelfall einzuführen, s.o. 4.2.3.1.

chert sind. Für diese gibt es vielmehr während der Mindestaufbewahrungsfristen keinen Löschungsanspruch.[1773]

Anders als in der Fassung des ersten Entwurfs[1774] besteht nach dem Gesetz kein Recht des Karteninhabers, die Protokolldaten nach § 291a Abs. 6 Satz 2 SGB V löschen zu lassen. Dies steht im Widerspruch dazu, dass die Daten zum Zweck der Datenschutzkontrolle, und damit im Interesse des Versicherten gespeichert werden. Je nach Verwendung der Karte kann es hier zu sensiblen Datensammlungen kommen. In Anbetracht der Befugnis des Karteninhabers, sowohl die Daten des elektronischen Rezepts als auch die der freiwilligen Anwendungen nach § 291a Abs. 3 Satz 1 SGB V löschen zu lassen, sollte eine Änderung erfolgen.

4.3.8 Anforderungen an die Datensicherheit

4.3.8.1 Hintergrund und Bedrohungen

Datenschutz und Datensicherheit sind insbesondere im Rahmen der elektronischen Datenverarbeitung kaum voneinander zu trennen, sondern eng miteinander verbunden und teilweise aufeinander bezogen.[1775] Entsprechend forderte das Bundesverfassungsgericht schon im Volkszählungsurteil für das Recht auf informationelle Selbstbestimmung die Ergänzung rechtlicher Schutzinstrumente durch technische Sicherungen.[1776]

Chipkartenausweise und die sie umgebende Infrastruktur stellen die hergebrachten Konzepte der Datensicherung vor neue Herausforderungen. Diese sind einerseits in der Sensibilität der verwendeten Daten, andererseits in deren erleichterter Zugänglichkeit und Veränderbarkeit begründet. So birgt beispielsweise eine elektronische Aufzeichnung von Daten im Gesundheitswesen insbesondere deshalb Risiken (für Patienten und Leistungserbringer), weil sie – ohne entsprechende Sicherungsmaßnahmen – leichter manipulierbar ist als die Karteikarten der herkömmlichen Dokumentation.[1777] Gleichzeitig ist das Gesundheitswesen ein Paradebeispiel für die Notwendigkeit mehrseitiger Sicherheit, weil die Interessen unterschiedlicher Beteiligter gleichzeitig berücksichtigt werden müssen.[1778]

Gerade an Chipkartenausweisen lassen sich die allgemeinen Grundbedrohungen für die Datensicherheit verdeutlichen. Dies sind der Verlust von Authentizität, Integrität, Vertraulichkeit, Verfügbarkeit und Kontrollierbarkeit.[1779] Authentizität und Kontrollierbarkeit der Daten sind zu gewährleisten, um jederzeit ihren Urheber und den Verantwortlichen eines Verarbeitungsvorgangs ermitteln zu können. Die Datenintegrität bezieht sich auf die Echtheit, Korrektheit und Vollständigkeit der Daten. Mit der Vertraulichkeit der Angaben wird sichergestellt, dass diese nur Berechtigten zur Verfügung stehen. Die Verfügbarkeit wird vor allem dann relevant, wenn vor Ort unter Zeitdruck gehandelt werden muss.

1773 Roßnagel-*Schirmer*, Kap. 7.12, Rn. 96. Unter Umständen kommt eine Sperrung in Betracht, s. *Kilian*, NJW 1992, 2313, 2315.

1774 § 291a Abs. 4 Satz 5 des ersten Entwurfs, s. BT-Drs. 15/1170, 39.

1775 Simitis-*Ernestus/Geiger*, § 9 Rn. 2 f.; s.a. *Steinmüller/Lutterbeck/Mallmann/Harbort/Kolb/Schneider* 1971, 71 ff.; *Steinmüller* 1993, 472 f.; *Gola/Schomerus*, § 9 Rn. 2; Roßnagel-*Heibey*, Kap. 4.5, Rn. 1 ff.; *Tinnefeld*/*Ehmann* 1998, 438.

1776 BVerfGE 65, 1 (44, 57, 59).

1777 Anschaulich *Schmidt-Beck*, NJW 1991, 2335, 2336.

1778 *Bäumler*, MedR 1998, 400, 404; s. zum Konzept der mehrseitigen Sicherheit allgemein die Beiträge in *Müller/Pfitzmann* (Hrsg.) 1997. Die Integrität der Gesundheitsdaten ist etwa im Sinne der Patienten (optimale Behandlung) und des behandelnden Arztes (Beweiswert in einem Haftungsprozess).

1779 Roßnagel-*Ernestus*, Kap. 3.2, Rn. 23; Roßnagel-*Heibey*, Kap. 4.5, Rn. 145; *Tinnefeld/Ehmann* 1998, 443 ff.; *Wehrmann/Wellbrock*, CR 1997, 754, 756.

Insbesondere in der schon weiter fortgeschrittenen Diskussion um die elektronische Gesundheitskarte besteht Einigkeit darüber, dass diesen Sicherheitszielen so weit wie möglich zu entsprechen ist.[1780] Das dient vor allem der Vermeidung von Behandlungsfehlern, die durch Produktmängel bei der Konstruktion und Herstellung der Chipkarte, die Unrichtigkeit von Daten aufgrund von Softwarefehlern oder eine mangelhafte Absicherung gegen Angriffe entstehen können.[1781] Wenn die Integrität und Verfügbarkeit der medizinischen Daten – aber auch ihre Validität (das heißt Aktualität und Qualität)[1782] – nicht jederzeit garantiert werden können, der jeweilige Leistungserbringer jedoch auf sie vertraut, bestehen erhebliche gesundheitliche Risiken für den Karteninhaber. Sollte es einmal zu Behandlungsfehlern kommen, muss zur Klärung der Verantwortlichkeiten beweiskräftig kontrollierbar sein, welche Beteiligten welche Daten zu welchem Zeitpunkt an welche Empfänger übermittelt haben.[1783]

Beim Personalausweis muss sich jede kontrollierende Stelle für eine ordnungsgemäße Identifizierung auf die Authentizität und Integrität der Daten, das heißt auf die ordnungsgemäße Produktion durch den Hersteller, die Ausstellung durch die Personalausweisbehörde und den Schutz gegen spätere Manipulationen verlassen können. Die Kontrollierbarkeit ist für den Personalausweis weniger wichtig, solange die Daten auf der Karte unveränderbar sind. Sie gilt jedoch auch hier für Auslese- und Weiterverarbeitungsvorgänge.

Im Rahmen der Verwendung biometrischer Daten ergibt sich eine Reihe von Besonderheiten hinsichtlich der Bedrohungsszenarien. Ein Angreifer kann dabei drei Ziele verfolgen, nämlich die Gewinnung von Daten zur missbräuchlichen Verwendung, das Absenden von Daten mit vorgetäuschter Authentizität und die Manipulation übertragener Daten.[1784] Ein möglicher Angriffspunkt ist zunächst der Sensor. Hier besteht die Gefahr einer Systemüberwindung durch Fake-Angriffe (Nachahmung des Merkmals)[1785] oder Datenakquisitions-Angriffe (Einspielen von Daten, die anderweitig beschafft wurden). Mit Angriffen auf den Sensor und frei zugängliche Datenleitungen wurden etwa in der Studie BioIS die Hälfte der Systeme überwunden.[1786] Bei der Verwendung von Chipkarten ist darüber hinaus die Schnittstelle ein Schwachpunkt. Werden Daten mitgeschnitten und danach erneut ins System eingespielt, so spricht man von einem Replay-Angriff.[1787] Daneben ist denkbar,

---

1780 S. u.a. *Bäumler*, MedR 1998, 400, 402, 404; *Bultmann/Wellbrock/Biermann/Engels/Ernestus/Höhn/Wehrmann/Schurig* 2002, 11 ff.; *Berger & Partner* 1997, 105 f.; *Der Landesbeauftragte für den Datenschutz Brandenburg* 2002, 99 f.; *Warda/Noelle* 2002, 188; *Jürgens* 2003, unter 4.1; *Menzel/Schläger*, DuD 1999, 70, 74; *Seidel*, DÄ 1997, A-1858; *Ulsenheimer/Heinemann*, MedR 1999, 197, 200.

1781 *Kilian*, NJW 1992, 2313, 2315.

1782 Validität beschränkt sich nicht auf die Unversehrtheit der Daten, sondern erfordert ihre inhaltliche Richtigkeit, s. *Goetz* 2001, 147.

1783 S. schon *BSI* 1995, 48 f., ferner *Ortner/Geis*, MedR 1997, 337, 339 f.; *Hermeler* 2000, 17. Die Nicht-Abstreitbarkeit von Datenübermittlungen beim Senden und Empfangen von Dokumenten ist im ärztlichen Haftungsfall von größter Wichtigkeit, s. *Goetz* 2001, 100.

1784 Für den Personalausweis s. *Struif/Scheuermann*, in: Reichl/Roßnagel/Müller 2005, 49 ff.; s.a. *Schneier*, C.ACM 8/1999, 136; *Daum* 2002, 189 ff.; *Dittmann/Mayerhöfer/Vielhauer* 2002, 192 ff.; *Thalheim/Krissler/Ziegler*, c't 11/2002, 114, 115 f.; *Woodward/Orlans/Higgins* 2003, 13 f.; *Bolle/Connell/Pankanti/Ratha/Senior* 2004, 211 ff.; *OECD* 2004, 13 f. m.w.N.; *Reid* 2004, 87 ff., 105 ff., 119 ff.

1785 Bsp. sind Silikonfinger, Tonbandaufnahmen, Photos, Kontaktlinsen mit fremden Irismustern oder Tippautomaten, vgl. Roßnagel-*Gundermann/Probst*, Kap. 9.6, Rn. 20; *Thalheim/Krissler/Ziegler*, c't 11/2002, 114 ff.; *Struif/Scheuermann/Köppen*, in: Reichl/Roßnagel/Müller 2005, 52 f. Insbesondere bei der Gesichtserkennung ist eine Überlistung per Photo ohne Lebenderkennungssystem regelmäßig sehr einfach, vgl. *Breitenstein* 2002, 45; *TAB* 2002, 17. Im Projekt BioP I wurden die Systeme selbst mit „zero effort attempts", d.h. durch schlichte Präsentation eines Ausweises durch eine visuell ähnlich aussehende Person, überwunden, vgl. *BSI/BKA/Secunet* 2004, 73; s.a. unten 6.2.2.

1786 S. *Busch/Daum/Finke/Funk* 2000, 44 (zitiert nach *Albrecht* 2003a, 55).

1787 Vgl. *Struif/Scheuermann*, in: Reichl/Roßnagel/Müller 2005, 51 f.

dass ein Angreifer übertragene Daten während der Kommunikation so verändert, dass beide Seiten die jeweils empfangenen Daten für authentisch halten. Dies wird als Man-in-the-middle-Angriff bezeichnet.[1788] In abgewandelter Form ist diese Attacke insbesondere bei kontaktlosen Chips von Bedeutung: Zur Täuschung mittels eines echten Ausweises zerstört der Angreifer dessen Chip, ohne dass dies äußerlich bemerkbar ist. Wird dann ein anderer Chip in die Reichweite des Lesegeräts gebracht, besteht die Gefahr, dass die Daten dieses Chips anstelle der Daten des zerstörten Chips akzeptiert werden. Weitere Angriffspunkte sind die gespeicherten Daten selbst, die verändert oder ausgelesen und später wieder ins System eingespielt werden können. Auch die Merkmalsextraktion und der Entscheidungsalgorithmus können manipuliert werden.

4.3.8.2 Normative Anforderungen und Anwendung auf Chipkartensysteme

4.3.8.2.1 Grundlagen

Normative Vorgaben für die Datensicherung finden sich in mehreren Rechtsquellen. Nr. 7 der Richtlinien der Generalversammlung der Vereinten Nationen fordert geeignete Maßnahmen gegen Naturgefahren, zufälligen Verlust und Zerstörung sowie gegen Gefahren durch menschliche Einwirkung. Nach Art. 7 des Übereinkommens des Europarats sind Vorkehrungen gegen zufällige oder unbefugte Zerstörung, zufälligen Verlust, unbefugten Zugang, unbefugte Veränderung und unbefugtes Bekanntgeben erforderlich.[1789] Art. 17 Abs. 1 DSRL verlangt geeignete technische und organisatorische Maßnahmen zum Schutz gegen die zufällige oder unrechtmäßige Zerstörung, den zufälligen Verlust, die unberechtigte Änderung, die unberechtigte Weitergabe oder den unberechtigten Zugang und gegen jede andere Form der unrechtmäßigen Verwendung personenbezogener Daten. Diese Maßnahmen stehen unter dem Vorbehalt der Verhältnismäßigkeit.

Im deutschen Recht finden sich die Anforderungen in § 9 BDSG und der entsprechenden Anlage. Daneben enthält die Signaturverordnung Sonderregeln für das Signaturverfahren. Im Gesundheitswesen wird die Datensicherheit vom Arzt auch als vertragliche Sorgfaltspflicht geschuldet;[1790] außerdem bestehen standesrechtliche Anforderungen nach § 10 Abs. 4 und 5 MBO-Ä 2004. Für den Bereich der elektronischen Datenverarbeitung hat der Arzt danach insbesondere die Empfehlungen der Bundesärztekammer zu beachten.[1791]

Verpflichtet werden nach § 9 Satz 1 BDSG „öffentliche und nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen". Bei Chipkartenausweisen sind das die Stellen, die die Ausweise ausgeben, auf ihnen Daten verarbeiten oder mit ihrer Hilfe Daten aus Netzwerken abrufen. Nicht verpflichtet wird der Inhaber der Karte. Die Auffassung, der Verfügungsbefugnis über die auf einer Patientenkarte gespeicherten Daten sei die Pflicht „immanent..., selber für die Datensicherheit der Patientenkarte zu sorgen"[1792] widerspricht dem Wortlaut von § 9 BDSG und der Grundkonzeption des Datenschutzrechts. Richtig ist zwar, dass der Karteninhaber dafür Sorge tragen sollte, die Sicherungsmechanismen Besitz (der Gesundheitskarte) und Wissen (der PIN) nicht aus der Hand zu geben. Das ist aber keine rechtliche Verpflichtung: Die Verfügungsbefugnis über die Daten beinhaltet vielmehr auch das Recht, sorglos mit ihnen um-

1788 S. *Struif/Scheuermann*, in: Reichl/Roßnagel/Müller 2005, 52.
1789 Zu den sich hieraus ergebenden Anforderungen vgl. *Henke* 1986, 121 ff.
1790 Roßnagel-*Schirmer*, Kap. 7.12, Rn. 100.
1791 S. *BÄK*, DÄ 1996, A-2809 ff. Die Landeskrankenhausgesetze enthalten keine Vorgaben oder verweisen auf die allgemeinen Verpflichtungen nach dem BDSG oder den LDSG, s. *Hermeler* 2000, 82.
1792 *Iwansky* 1999, 91.

zugehen. Erst recht besteht keine Verantwortung für die Datensicherheit „der Patientenkarte“. Deren technische Ausgestaltung ist vielmehr Aufgabe der ausgebenden Stelle. Der Karteninhaber nimmt also lediglich an den Prozessen der Datensicherheit teil und wird durch diese geschützt.

Die Regelungen in § 9 BDSG und der Anlage sollen vor allem präventiv wirken. Gefordert ist zunächst eine Bedrohungs- und Risikoanalyse vor Beginn des Verarbeitungsverfahrens, weil ansonsten die erforderlichen Schritte nicht abgeschätzt werden können.[1793] Auf der Basis der Ergebnisse müssen dann technische und organisatorische Maßnahmen ergriffen werden, die sicherstellen, dass der Verpflichtete seinen Pflichten aus dem Bundesdatenschutzgesetz nachkommen kann. Das gilt für den gesamten Geltungsbereich des Gesetzes.[1794] Seit der letzten Novelle des Bundesdatenschutzgesetzes im Jahre 2001 erfasst § 9 BDSG nicht nur die Verarbeitung, sondern auch die Erhebung und die Nutzung personenbezogener Daten.

Die nach § 9 Satz 1 BDSG zu treffenden Maßnahmen sind zunächst technischer Natur, wie etwa bauliche Strukturen, Einbruchs- und Brandschutzeinrichtungen oder die Virenabwehr. Daneben sind organisatorische Vorkehrungen erforderlich, zum Beispiel hinsichtlich der Einhaltung eines ordnungsgemäßen Betriebsablaufs, der Personalauswahl, der Einhaltung eines Vier-Augen-Prinzips, der Festlegung von Arbeitsabläufen in Arbeitsplatzbeschreibungen und Geschäftsverteilungsplänen, einer Trennung nach Funktionen und deren schriftliche Fixierung in Arbeitsanweisungen, der Registrierung des Datenträgerbestands und der Zugangskontrolle zu Gebäuden und Datenverarbeitungssystemen.[1795] Technische und organisatorische Maßnahmen sind nicht immer eindeutig gegeneinander abgrenzbar. Dies ist mit Blick auf ihre identische Zielrichtung aber auch nicht notwendig.

Die technische und organisatorische Gestaltung betrifft bei Chipkartenausweisen zunächst den Datenerhebungsvorgang, also beim Personalausweis die Aufnahme der bisher gespeicherten und eventueller biometrischer Daten sowie Angaben für das Signaturzertifikat, daneben die Übermittlung von der Daten erhebenden zur Ausweis herstellenden Stelle und zum Zertifizierungsdiensteanbieter. Ebenso müssen die weitere Aufbewahrung der Daten und die übrigen Verwendungsvorgänge so gestaltet werden, dass sie den Anforderungen des Datenschutzes gerecht werden. Gleiches gilt für die elektronische Gesundheitskarte. Hier sind insbesondere in größeren Behandlungseinheiten (beispielsweise in Krankenhäusern) organisatorische Vorkehrungen zur Datensicherheit zu ergreifen.

4.3.8.2.2 Anforderungen aus der Anlage zu § 9 Satz 1 BDSG

Die Anforderungen von § 9 Satz 1 BDSG werden in der Anlage weiter konkretisiert.[1796] Die dort aufgeführten Maßnahmen können aber auch bereits nach § 9 Satz 1 BDSG erforderlich sein, das heißt unabhängig von der Anlage und ihrer Anwendbarkeit. Ein Beispiel ist die effektive Protokollierung von Verarbeitungsvorgängen.[1797]

Kraft der ausdrücklicher Verweisung in § 9 Satz 1 BDSG hat die Anlage denselben Geltungsrang wie der Paragraph selbst. Sie gilt allerdings im Unterschied zu § 9 BDSG nicht

1793 Simitis-*Ernestus/Geiger*, § 9 Rn. 16; *Tinnefeld/Ehmann* 1998, 441; zur Methodik vgl. Roßnagel-*Ernestus*, Kap. 3.2, Rn. 29 ff.; *Rosenbaum/Sauerbrey*, DuD 1995, 28 ff.; ein (knappes) Bsp. für die Telematikstruktur im Gesundheitswesen findet sich bei *BITKOM/VDAP/VHitG/ZVEI* 2003, 38 ff.

1794 Simitis-*Ernestus/Geiger*, § 9 Rn. 4; *Gola/Schomerus*, § 9 Rn. 6.

1795 *Gola/Schomerus*, § 9 Rn. 5, 14 f.; ausführlich *GDD* 2002, 63 f.

1796 Vgl. zum Folgenden für den digitalen Personalausweis *Roßnagel/Hornung*, in: Reichl/Roßnagel/Müller 2005, 236 f.

1797 S. *Gola/Schomerus*, § 9 Rn. 10 f.; *Der Bundesbeauftragte für den Datenschutz*, 1993, 194.

für die Datenerhebung und für die Datenverarbeitung und -nutzung nur, wenn diese automatisiert erfolgt, also wesentliche Verfahrensschritte, insbesondere das Lesen und Vergleichen von Daten, in programmgesteuerten Einheiten ablaufen.[1798] Bei den hier behandelten Chipkartenausweisen ist das durchweg der Fall, weil diese bereits selbst programmgesteuert arbeiten. Auch dort, wo der Ausweis als reiner Datenspeicher verwendet wird (etwa bezüglich der biometrischen Daten beim Personalausweis), werden zum Auslesen automatisierte Verfahren benötigt. Nicht betroffen sind demgegenüber manuelle Überprüfungen der Oberfläche.

In der Anlage werden Anforderungen an die „innerbehördliche und innerbetriebliche Organisation" vorgegeben. Dieser Begriff ist weit zu verstehen; er umfasst die Aufbau- wie die Ablauforganisation, und damit auch technische und bauliche Aspekte.[1799] Die Bestimmungen der Anlage sind nicht abschließend. Deshalb sind bei hoher Sensibilität der Daten, besonderen Risiken der Verarbeitungssysteme oder bei anderen speziellen Gefährdungslagen zusätzliche Maßnahmen erforderlich.[1800]

Anders als in einigen Landesdatenschutzgesetzen[1801] wurden die sehr abstrakten Formulierungen der Anlage im Rahmen der Novelle des Jahres 2001 – trotz entsprechender Forderungen – nicht durch weltweit anerkannte Begriffe wie Vertraulichkeit, Verfügbarkeit und Integrität ersetzt. In der Abstraktheit der Begrifflichkeit liegt das Grundproblem bei der Auslegung.[1802]

Die *Zutrittskontrolle* nach Nr. 1 der Anlage regelt den körperlichen Zutritt zu Datenverarbeitungsanlagen und verlangt, durch entsprechende Maßnahmen sicherzustellen, dass nur hierzu befugte Personen in die Nähe der Geräte kommen.[1803] „Zutritt" kann aber auch das visuelle Wahrnehmen (etwa durch eine Glasscheibe) ohne physisches Betreten bedeuten.[1804] Besondere Herausforderungen ergeben sich insoweit für dezentrale, insbesondere vernetzte Anlagen wie PCs oder Terminals.[1805] Damit verschwimmen auch die Grenzen zu Nr. 2 und Nr. 3 der Anlage. Dies ist letztlich aber unerheblich, da alle Nummern gleichermaßen auf die Ausführung der Vorschriften des Bundesdatenschutzgesetzes abzielen.[1806] Zu den Verarbeitungsanlagen im Sinne der Nr. 1 zählen neben stationären Geräten auch tragbare PCs und Chipkartenlesegeräte, die gesamte Peripherie (Drucker, Scanner und andere Zusatzgeräte), sowie Leitungen.[1807]

Bei Chipkartenausweisen sind dementsprechend stationäre und mobile Lesegeräte so zu konstruieren und zu installieren, dass Unbefugte keinen Zutritt zu ihnen haben und nicht an

---

1798 Simitis-*Ernestus/Geiger*, § 9 Rn. 59; die Größe der Anlage ist ebenso unerheblich (ebd. Rn. 62 ff.; *Auernhammer*, § 9 Rn. 10; *Volle*, CR 1992, 500 ff.) wie einzelne manuelle Schritte (Simitis-*Ernestus/Geiger*, § 9 Rn. 61).

1799 Simitis-*Ernestus/Geiger*, § 9 Rn. 50.

1800 *Auernhammer*, § 9 Rn. 6; Simitis-*Ernestus/Geiger*, § 9 Rn. 17; *Schaffland/Wiltfang*, § 9 Rn. 38.

1801 Z.B. § 5 Abs. 2 BlnDSG, § 8 Abs. 2 HmbDSG, § 10 Abs. 2 DSG NW.

1802 S. Simitis-*Ernestus/Geiger*, § 9 Rn. 53 f.; Roßnagel-*Ernestus*, Kap. 3.2, Rn. 60; Roßnagel-*Heibey*, Kap. 4.5, Rn. 145; *Jacob*, DuD 2000, 5, 10.

1803 Zu den erforderlichen Maßnahmen vgl. z.B. das IT-Grundschutzhandbuch des *BSI*, Bauliche Maßnahmen; *Jürgens* 2003, unter 4.3.1; Simitis-*Ernestus/Geiger*, § 9 Rn 80 ff.; *Schaffland/Wiltfang*, § 9 Rn. 59 ff.

1804 Simitis-*Ernestus/Geiger*, § 9 Rn. 77.

1805 Hierzu bereits *Aufsichtsbehörde Baden-Württemberg*, StAnz BW 1986, 4 (unter 1); *Der Berliner Datenschutzbeauftragte* 1991, 35; *Der Landesbeauftragte für den Datenschutz Freie Hansestadt Bremen* 1993, 120; *Tinnefeld/Ehmann* 1998, 445; s.a. Roßnagel-*Heibey*, Kap. 4.5, Rn. 40 f.

1806 Simitis-*Ernestus/Geiger*, § 9 Rn. 69 f.

1807 DIN 44300 definiert eine Datenverarbeitungsanlage als „Gesamtheit der Baueinheiten, aus denen eine Funktionseinheit zur Verarbeitung von Daten aufgebaut ist". Damit ist etwa Software nicht erfasst; s.a. *Schaffland/Wiltfang*, § 9 Rn. 54 f.

ihnen manipulieren können. Anwendungsbeispiele sind Grenzanlagen und mobile Kontrollgeräte für den digitalen Personalausweis, Praxis- und Apothekencomputer für die elektronische Gesundheitskarte, sowie denkbare Selbstbedienungsterminals und die Elemente der Netzwerkinfrastruktur im Gesundheitswesen. Auch Chipkarten fallen an sich unter den Begriff der Datenverarbeitungsanlage, so es sich um Prozessorchips und nicht um reine Speicherkarten handelt. Allerdings muss Nr. 1 der Anlage einschränkend dahingehend ausgelegt werden, dass die verantwortliche Stelle nur soweit verpflichtet wird, wie ihre Kontroll- und Einflussmöglichkeiten gehen.[1808] Diese bestehen bei Chipkartenausweisen nicht, da sie ihrer Funktionsweise nach vom Betroffenen mit sich geführt werden und die verantwortliche Stelle deshalb keine Möglichkeit hat, Unbefugten den Zutritt zu verwehren.

Mit der *Zugangskontrolle* (Nr. 2 der Anlage) soll verhindert werden, dass Datenverarbeitungssysteme von Unbefugten genutzt werden. Damit ist der Schutz gegen das Eindringen in das System selbst gemeint.[1809] „Nutzen" der Daten ist hier nicht im Sinne der Definition in § 3 Abs. 5 BDSG, sondern im umgangssprachlichen Sinn zu verstehen[1810] und erfasst jeden unbefugten Umgang mit den Daten. Der Begriff des Datenverarbeitungssystems ist weiter als der der Datenverarbeitungsanlage und beinhaltet neben Geräten und Baueinheiten auch Software.[1811] Nach Nr. 2 der Anlage muss zum Beispiel sichergestellt werden, dass Unbefugte die Verarbeitungsanlagen bei der Datenerhebung, die Lesegeräte für Überprüfungsvorgänge, aber auch den Personalausweis und die Gesundheitskarte selbst nicht nutzen können.[1812] Dem können etwa geeignete Verschlüsselungsverfahren sowie eine Absicherung des Zugriffs auf die Karten durch eine PIN oder ein biometrisches Merkmal dienen. Im Unterschied zur Nr. 1 der Anlage ist hier keine Einschränkung für die Ausweise erforderlich, da es durchaus möglich ist, durch technische Sicherungen eine Nutzung durch Unbefugte zu verhindern oder zu erschweren.

Nr. 3 und Nr. 8 der Anlage stehen in engem sachlichem Zusammenhang. Wendet sich die Zugangskontrolle gegen die Benutzung durch Unbefugte, so richtet sich die *Zugriffskontrolle* (Nr. 3 der Anlage) an die zur Benutzung des Systems Berechtigten. Es muss sichergestellt werden, dass diese nur auf die Daten zugreifen können, für die sie eine Zugriffsberechtigung besitzen, und dass die verwendeten Daten nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.[1813] Zugriffsrechte sind dabei so zu organisieren, dass die an der Datenverarbeitung Beteiligten lediglich auf die zur Erfüllung ihrer Aufgaben erforderlichen Daten zugreifen und mit ihnen auch nur im Rahmen dieser Aufgaben Operationen durchführen können.[1814] Ebenso ist nach Nr. 8 der Anlage (*Funktionstrennung*) zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. Diese Regelung ist eine der wichtigsten der Anlage und verlangt, verschiedene Arbeitsbereiche der Datenverwendung grundsätzlich getrennt zu orga-

---

1808 Dieses Kriterium gilt etwa für gemietete Leitungen, s. Simitis-*Ernestus/Geiger*, § 9 Rn. 72 f.

1809 *Gola/Schomerus*, § 9 Rn. 24; Roßnagel-*Heibey*, Kap. 4.5, Rn. 42; zu Bsp. für Abwehrmaßnahmen s. Simitis-*Ernestus/Geiger*, § 9 Rn 97 f.; *Schaffland/Wiltfang*, § 9 Rn. 76 ff.

1810 Simitis-*Ernestus/Geiger*, § 9 Rn. 92.

1811 Vgl. DIN 44300 Nr. 99.

1812 Hier sind im Einzelfall Abstufungen je nach der Sensibilität der Daten möglich. So ist es etwa zulässig, die Daten des elektronischen Rezepts ohne PIN-Schutz des Karteninhabers zu speichern, weil dies dem bisherigen Schutz durch Besitz entspricht; s. näher oben 4.2.3.4.2.

1813 Näher *GDD* 2002, 65; *Gola/Schomerus*, § 9 Rn. 25; zu notwendigen Gegenmaßnahmen vgl. Simitis-*Ernestus/Geiger*, § 9 Rn. 108 f.; *Schaffland/Wiltfang*, § 9 Rn. 84 ff.; speziell für das Gesundheitswesen vgl. *Jürgens* 2003, unter 4.3.2.

1814 Simitis-*Ernestus/Geiger*, § 9 Rn. 104; *Tinnefeld/Ehmann* 1998, 452 (zu Nr. 5 der alten Anlage).

nisieren, um die Gefahr eines Missbrauchs zu verringern.[1815] Die getrennte Verarbeitung kann durch eine physische Trennung der Datenverarbeitungssysteme, aber auch durch eine logische Trennung innerhalb eines Systems erfolgen.[1816] Letztere muss dann in aller Regel mit der Ausdifferenzierung von Zugriffsrechten einhergehen. So können zum Beispiel Zugriffssysteme nach Funktionen getrennt, Datensätze je nach Zweckbindung unterschiedlich verschlüsselt oder bestimmte Rollen im Informationssystem festgelegt werden.

Die Bedeutung der Nr. 3 und 8 der Anlage zeigt sich bei den hier untersuchten Multiapplikationskarten. Sowohl bei der elektronischen Gesundheitskarte als auch beim digitalen Personalausweis bestehen wesentliche Elemente des verfassungsrechtlichen Erforderlichkeitsprinzips in einer strikten Datentrennung nach Applikationen und einem System von abgestuften Zugriffsberechtigungen für die Beteiligten.[1817] Diese Trennung des Zugriffs ist auf der Ebene der Datensicherheit auch technisch abzusichern.

Für die elektronische Gesundheitskarte bedeutet dies die technische Umsetzung der Anforderung eines ausdifferenzierten Zugriffsschutzes im Einzelfall.[1818] Es ist sicherzustellen, dass die Leistungserbringer immer nur auf die Daten zugreifen können, die sie entweder selbst gespeichert haben oder für deren Verwendung sie durch den Versicherten autorisiert wurden. Wenn bestimmte Gruppe von Leistungserbringern bestimmte Daten zur Erfüllung ihrer Funktion nicht benötigen (beispielsweise Apotheker in Bezug auf die komplette Krankengeschichte des Versicherten),[1819] so ist ihnen ein Zugriff auf die in diesen Datenfeldern gespeicherten Informationen beziehungsweise die hierzu auf Servern abgelegten Daten zu verwehren. Zur Umsetzung des abgestuften Zugriffsschutzes gibt es unterschiedliche technische Umsetzungsmöglichkeiten.[1820]

Beim Personalausweis besteht die Grundkonzeption in der Zusammenführung von zumindest zwei Funktionen, nämlich der hoheitlichen Identifizierungs- und der privaten Signaturfunktion (einschließlich des „elektronischen Ausweises“[1821]). Die Identifikationsdaten müssen vor dem Zugriff Unbefugter gesichert werden, wobei unbefugt hier alle Stellen und Personen außerhalb der Ermächtigungstatbestände von Identitätskontrollen sind. Konkret bedeutet das, dass die Identifikationsdaten vor Zertifizierungsdiensteanbietern, Stellen im privaten Bereich, Dritten, aber auch vor dem Inhaber selbst geschützt werden müssen. Schutz wiederum heißt unbedingten Schutz gegen Veränderung und relativen Schutz insoweit, als bei Berechtigung zum Zugriff nur die Daten ausgelesen werden dürfen, auf die sich die Berechtigung erstreckt. Es darf darüber hinaus keine Möglichkeit der Duplizierung der elektronischen Daten und ihrer Speicherung auf einem anderen Ausweis geben, der auf einen Dritten ausgestellt ist.

Die Herstellung einer exakten Kopie des digitalen Personalausweises ist demgegenüber an sich ein relativ geringes Sicherheitsrisiko. Eine Verwendung durch den Inhaber ist unproblematisch, da in diesem Fall keine Identitätstäuschung vorliegt. Allerdings eröffnet eine im Umlauf befindliche Kopie die Möglichkeit für Dritte, ungestört an dieser zu manipulieren oder (bei ähnlich aussehenden Personen) den Personalausweis als eigenen auszugeben. Dieses Risiko wird zwar durch die Aufnahme biometrischer Merkmale entschei-

1815 Die Norm bildet damit einen Einstieg in den Systemdatenschutz, s. Simitis-*Ernestus/Geiger*, § 9 Rn. 160; zu diesem Konzept s. bereits oben 4.3.2.2. Nicht nachvollziehbar ist die Auffassung von *Schaffland/Wiltfang*, § 9 Rn. 140, aus Nr. 8 der Anlage folge kein Handlungsbedarf.

1816 Simitis-*Ernestus/Geiger*, § 9 Rn. 161.

1817 S.o. 4.2.2.4.6 und 4.2.3.4.

1818 Vgl. ausführlich oben 4.2.3.4.2.

1819 S.o. 4.2.3.4.2.2.

1820 Vgl. unten 6.3.3.1.

1821 Dazu unten 5.2.1.

dend vermindert, kann jedoch nicht vollständig beseitigt werden. Eine entsprechende Risikobewertung hat auch Eingang in die Landespersonalausweisgesetze gefunden, wonach niemand mehr als einen Personalausweis besitzen darf,[1822] der Verlust und das Wiederauffinden anzuzeigen sind[1823] und ungültige und nach Verlust wieder aufgefundene Ausweise abgegeben werden müssen.[1824] Überdies ist das zentrale Register der Ausweisnummern bei der Bundesdruckerei GmbH nach § 3 Abs. 3 Satz 1 PersAuswG ausdrücklich zum Nachweis des Verbleibs der Ausweise zulässig. Im Ergebnis muss der Personalausweis damit auch gegen die Herstellung einer exakten Kopie geschützt werden.

Die Daten der Signatur-, Authentisierungs- und Verschlüsselungsfunktion (sowie die des elektronischen Ausweises) müssen für den Inhaber gegen den Zugriff anderer geschützt werden, wobei dies nunmehr auch den Schutz vor dem Zugriff staatlicher Stellen einschließt. Es ist also sicherzustellen, dass diese nicht auf den geheimen Schlüssel zugreifen und zum Beispiel gefälschte Willenserklärungen abgeben können. Diese Prinzipien der Datentrennung sind entsprechend auf mögliche Zusatzapplikationen anwendbar.

Die Umsetzung dieser Anforderungen hat durch organisatorische, vor allem aber durch technische Maßnahmen zu geschehen. Geschützt werden müssen Vertraulichkeit und Integrität der Daten. Da alle Funktionalitäten auf einer Karte vereint werden, käme hierfür zunächst die Verwendung getrennter Chips in Betracht. Sofern die Funktionsweise des verwendeten Mikroprozessors allerdings eine saubere Datentrennung garantiert, spricht nichts dagegen, diese innerhalb ein und desselben Chips vorzunehmen. In jedem Fall muss aber in technischer Hinsicht der Zugriff auf die Daten der Chipkarte so organisiert werden, dass immer nur die jeweils berechtigten Stellen die technische Möglichkeit des Auslesens haben.[1825]

Findet eine Weitergabe von Daten statt, so greifen die Anforderungen der *Weitergabekontrolle* nach Nr. 4 der Anlage. Danach ist zu gewährleisten, dass die Daten bei Übermittlungs-, Transport- und Speicherungsvorgängen nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. Die Übermittlungsmöglichkeiten sind außerdem zu dokumentieren. Nach dem eindeutigen Wortlaut und der Gesetzgebungsgeschichte ist lediglich eine Dokumentation darüber erforderlich, welche Übermittlungswege bestehen, nicht aber die Protokollierung jedes einzelnen Übermittlungsvorgangs.[1826] Eine Pflicht hierzu kann jedoch (zum Beispiel bei besonders sensiblen Daten) direkt aus § 9 Satz 1 BDSG folgen.[1827] Die Regelungen über die Protokollierung sollen zum einen den Nachweis von Missbrauch ermöglichen, gleichzeitig aber auch abschreckend wirken.

Beim Personalausweis sind danach insbesondere die Übermittlungsmöglichkeiten automatisiert ausgelesener Daten von Kontrollstellen an zentrale Datenbanken zu Abgleichszwecken (etwa mit einer Fahndungsdatenbank) zu dokumentieren.[1828] Die Anforderungen aus Nr. 4 der Anlage sind insbesondere im Gesundheitswesen wichtig, weil es hier durch den Einsatz der elektronischen Gesundheitskarte zu einer deutlich höheren Zahl von Da-

---

1822 S. z.B. § 1 Abs. 5 LPAuswG Bln., § 1 Abs. 4 LPAuswG Hess., § 1 Abs. 5 LPAuswG Bbg.

1823 Bspw. § 6 Abs. 1 Nr. 3 LPAuswG Bln., § 7 Nr. 3 LPAuswG Hess., § 6 Abs. 1 Nr. 4 LPAuswG Bbg.

1824 Vgl. z.B. § 6 Abs. 1 Nr. 4 LPAuswG Bln., §§ 7 Nr. 2, 9 Satz 1 LPAuswG Hess., § 6 Abs. 1 Nr. 3, 5 und 6 LPAuswG Bbg.

1825 Allgemein für Chipkarten *BT-Enquetekommission Zukunft der Medien* 1998, 54; Roßnagel-*Weichert*, Kap. 9.5, Rn. 43; *Bizer* 2002, 32.

1826 Simitis-*Ernestus/Geiger*, § 9 Rn. 116. Eine derartige Bestimmung wurde bei den Beratungen zum BDSG 1977 ausdrücklich gestrichen; zu den weiteren Anforderungen an die Dokumentation und Bsp. für mögliche Maßnahmen s. Simitis-*Ernestus/Geiger*, § 9 Rn. 119 ff.

1827 *GDD* 2002, 66; Simitis-*Ernestus/Geiger*, § 9 Rn. 118; s.a. *Jürgens* 2003, unter 4.3.3.

1828 Ein solches Vorgehen ist insbesondere für die elektronisch gespeicherten Ausweisdaten denkbar, die der bisherigen maschinenlesbaren Lesezone entsprechen.

tenübermittlungen kommen wird. Eine Pflicht, jede Übermittlung zu protokollieren, ergibt sich zwar nicht aus der Anlage, für die letzten 50 Zugriffe auf die Gesundheitskarte aber aus § 291a Abs. 6 Satz 2 SGB V.

Im Rahmen der Weitergabekontrolle müssen außerdem die Übertragungswege, also zum Beispiel zwischen der Daten erhebenden Stelle und dem Kartenproduzenten, gesichert werden.[1829] Es sind geeignete Verschlüsselungsverfahren zu verwenden. Bei der Gesundheitskarte sind die Daten darüber hinaus sowohl auf Servern und den sie verbindenden Übermittlungswegen als auch auf der Gesundheitskarte gegen unbefugte Lese-, Kopier-, Veränderungs- oder Entfernungsschritte zu schützen. Dies ist insbesondere im Verlustfall wichtig. So darf es nicht möglich sein, aus einer Gesundheitskarte Informationen auszulesen, wenn diese dort zum Zweck des Transports vom Hausarzt zum Facharzt gespeichert wurden.

Nach Nr. 5 der Anlage (*Eingabekontrolle*) sind auch die Eingabe, Veränderung und Entfernung von Daten zu dokumentieren.[1830] Diese Verpflichtung wirkt mit der Zugriffskontrolle nach Nr. 3 zusammen und erfordert neben dem Festhalten des Vorgangs auch die Protokollierung der einwirkenden Person.[1831] Sie greift zum einen bei der Eingabe der erhobenen Daten in das jeweilige Verarbeitungssystem zur Herstellung des Chipkartenausweises, zum anderen bei der Eingabe, Veränderung und Entfernung von Daten auf der Karte selbst, sofern diese möglich sind. Beim Personalausweis wird bei der Veränderung von Daten der Identifikationsfunktion allerdings regelmäßig ohnehin ein neuer Ausweis ausgestellt werden. Eine Änderung der elektronisch gespeicherten Daten – zum Beispiel bei Namensänderungen – wäre noch technisch durchführbar. Sofern diese Daten von der ausgebenden Stelle elektronisch signiert und mit einem Zeitstempel versehen würden, wäre auch eine Dokumentation möglich. Da die Daten (mit Ausnahme der biometrischen Merkmale) jedoch auch visuell aufgebracht werden, ist ein neuer Personalausweis unumgänglich, sobald sich die optisch erkennbaren Angaben ändern. Anders ist das bei einer eventuellen „Nachlademöglichkeit" der Signaturzertifikate und möglichen Zusatzapplikationen. Wenn hier eine Eingabe, Veränderung oder Entfernung personenbezogener Daten auf der Karte erfolgt, muss diese dokumentiert werden.[1832]

Im Gesundheitswesen ist die Kontrolle und Protokollierung von Dateneingaben ein noch wichtigerer Baustein der Datensicherung. Ohne eine Nachvollziehbarkeit von Datenänderungen könnte sich kein Leistungserbringer darauf verlassen, dass ihm die vorliegenden Daten ein zutreffendes Bild über den Gesundheitszustand des Versicherten liefern. Dies ist jedoch als Basis für die jeweilige Behandlung unabdingbar. Überdies muss im Haftungsfall zweifelsfrei bestimmbar sein, wer wann welche Daten bereitgestellt oder verändert hat. Dies kann durch die Verwendung von Attribut-Zertifikaten auf dem elektronischen Heilberufsausweis geschehen.[1833]

Nr. 6 der Anlage (*Auftragskontrolle*) verlangt die Gewähr, dass bei einer Auftragsdatenverarbeitung (§ 11 BDSG) die Daten ausschließlich entsprechend den Weisungen des Auftraggebers verarbeitet werden. Danach hat der Auftragnehmer für Sicherungsmaßnahmen zu sorgen, während der Auftraggeber klare Anweisungen geben und Kontrollabreden

1829 S. allgemein Simitis-*Ernestus/Geiger*, § 9 Rn. 112; Roßnagel-*Heibey*, Kap. 4.5, Rn. 53.

1830 *Gola/Schomerus*, § 9 Rn. 27; zum Umfang der Protokollpflicht Simitis-*Ernestus/Geiger*, § 9 Rn. 131 ff. Die Norm wurde gegenüber der alten Fassung abgeschwächt; kritisch dazu Roßnagel-*Heibey*, Kap. 4.5, Rn. 57 ff.

1831 *Tinnefeld/Ehmann* 1998, 453 (zu Nr. 7 der alten Anlage); einschränkend *Schaffland/Wiltfang*, § 9 Rn. 127; mögliche Maßnahmen bei Simitis-*Ernestus/Geiger*, § 9 Rn. 144 f.

1832 *Bizer* 2002, 32; Simitis-*Bizer*, § 6c Rn. 13.

1833 S.u. 6.3.3.1.

treffen muss.[1834] Insgesamt erfordert die Norm technische und organisatorische Maßnahmen, die die lückenlose Einhaltung des Weisungsprinzips gewährleisten.[1835] Bei der elektronischen Gesundheitskarte ist Nr. 6 der Anlage nicht einschlägig, weil es sich bei der Einschaltung von Dritten zum Betrieb der Serverarchitektur nicht um eine Datenverarbeitung im Auftrag handelt.[1836] Dagegen sind die Anforderungen der Anlage wie bisher bei abgegrenzten, untergeordneten Aufgaben (beispielsweise der Archivierung von Daten, die mit Hilfe der Gesundheitskarten von Patienten in das Datenverarbeitungssystem eines Krankenhauses übernommen wurden) zu beachten. Für den Personalausweis findet die Norm insbesondere Anwendung, wenn bestimmte Produktionsverfahren oder laufende Betreuungen an externe Stellen abgegeben werden. Eine denkbare Zusammenarbeit der Personalausweisbehörde im Rahmen eines Auftragsverhältnisses für einen oder mehrere Zertifizierungsdiensteanbieter im Rahmen der Registrierung, Ausgabe und Unterrichtung ist dagegen spezialgesetzlich zu regeln,[1837] sodass Nr. 6 nicht anwendbar sein wird.

Im Rahmen der *Verfügbarkeitskontrolle* nach Nr. 7 der Anlage haben Schutzmaßnahmen gegen zufällige Zerstörung oder Verlust wie etwa Wasserschäden, Brände, Blitzschlag und Stromausfall zu erfolgen.[1838] Sicherungsmittel können bauliche Maßnahmen, die Installation von Notstromaggregaten und die Erstellung von Sicherungskopien sein.[1839] Aus Nr. 7 der Anlage ergeben sich Anforderungen an den digitalen Personalausweis und die Gesundheitskarte selbst. Durch die normale mechanische Beanspruchung darf es nicht zu Funktionsuntauglichkeiten des Chips kommen. Für die Telematik im Gesundheitswesen gilt überdies, dass sie die benötigten medizinischen Daten schnell und sicher bereitstellen muss. Hierfür sind einerseits die verwendeten Systeme mit größter Sorgfalt gegen Störungen zu schützen, andererseits geeignete Rückfallsysteme für den Fall von Serverausfällen oder anderen Problemen zu implementieren. Beides wird in dem Maße wichtiger werden, in dem im Gesamtsystem die elektronische Verfügbarkeit essentieller Daten für die Akteure selbstverständlich werden wird.

Eine nicht gesetzlich geregelte Pflicht zur Datensicherung besteht schließlich dann, wenn man – wie hier vertreten – eine Anwendbarkeit des Datenschutzrechts auf anonyme, pseudonyme und verschlüsselte Daten ablehnt.[1840] Um eine nachträgliche Re-Personalisierung zu verhindern, müssen Maßnahmen zur Aufrechterhaltung der Anonymitäts- und Pseudonymitätseigenschaft und zur technischen und organisatorischen Sicherung getroffen werden.[1841]

4.3.8.2.3 Verhältnismäßigkeit

Sowohl die Pflichten aus § 9 BDSG als auch die aus der Anlage stehen nach § 9 Satz 1 BDSG unter dem Vorbehalt der Verhältnismäßigkeit. Die verantwortliche Stelle muss nur

---

1834 *Gola/Schomerus*, § 9 Rn. 28; Roßnagel-*Heibey*, Kap. 4.5, Rn. 64 f.; *GDD* 2002, 66; für Bsp. vgl. *Aufsichtsbehörde Baden-Württemberg*, StAnz BW 1980, 5 (unter 6.2); Simitis-*Ernestus/Geiger*, § 9 Rn. 155; *Jürgens* 2003, unter 4.4.1.2.

1835 Simitis-*Ernestus/Geiger*, § 9 Rn. 149; s.a. oben 4.3.6.2.1.

1836 S.o. 4.3.6.2.2.

1837 S.o. 4.3.6.2.2.2.

1838 *Gola/Schomerus*, § 9 Rn. 29; *Schaffland/Wiltfang*, § 9 Rn. 139; weitere Anwendungsfälle bei Simitis-*Ernestus/Geiger*, § 9 Rn. 159. Nr. 7 erfasst nicht den Schutz vor unrechtmäßigem Handeln Unbefugter. Dies ist Gegenstand der übrigen Nummern, s. Roßnagel-*Heibey*, Kap. 4.5, Rn. 68.

1839 Weitere Bsp. bei *GDD* 2002, 66 f.; Simitis-*Ernestus/Geiger*, § 9 Rn. 159.

1840 S.o. 4.1.2.1.

1841 S. näher *Roßnagel/Pfitzmann/Garstka* 2001, 108 ff.; *Roßnagel/Scholz*, MMR 2000, 721, 730 f.; *Scholz* 2003, 198 ff.

solche Maßnahmen ergreifen, deren Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht (§ 9 Satz 2 BDSG). Zu beachten ist, dass damit nicht etwa Pflichten, die sich aus den Normen des Bundesdatenschutzgesetzes ergeben, sondern lediglich eine konkrete Umsetzungsart gemeint ist. Daher stellt sich beispielsweise für die Pflicht zur Auskunftserteilung die Frage der Verhältnismäßigkeit nicht, während eine bestimmte Art der Auskunft unverhältnismäßig sein kann.[1842] Ist (in diesem Beispiel) der verarbeitenden Stelle die Auskunft insgesamt zu aufwendig, so muss sie auf die Datenverarbeitung verzichten.

Der vom Gesetz geforderte Aufwand der Maßnahmen ist umso größer, je stärker das Schutzbedürfnis des Betroffenen ist. Allgemeiner gesagt, geht es um den Grad der Gefährdung für das Recht auf informationelle Selbstbestimmung. Das gebotene Sicherheitsniveau hängt unter anderem von der Sensibilität der Daten, der Seriosität des Verwenders und der Art und Intensität der Datennutzung ab.[1843] Bei der Verarbeitung von Daten aus allgemein zugänglichen Quellen ist weniger Schutz erforderlich. Der Gefährdungsgrad ist andererseits dann höher, wenn Daten als Grundlage für Entscheidungen dienen, die sich auf den Betroffenen auswirken,[1844] oder wenn es um Daten geht, an denen Außenstehende ein starkes Interesse haben.

Bei der Abwägung sind auf der Seite der verantwortlichen Stelle sämtliche Kosten in Anschlag zu bringen, die die technischen und organisatorischen Maßnahmen verursachen. Dazu zählt allerdings nicht der Aufwand, der bei der Datenverarbeitung ohnehin entsteht oder aus eigenen wirtschaftlichen Interessen der verarbeitenden Stelle begründet wird.[1845] Wenn die Maßnahmen der Stelle auch wirtschaftliche Vorteile eintragen, so sind diese anzusetzen. Einerseits darf es nicht zu einer wirtschaftliche Überforderung der Daten verarbeitenden Stelle kommen, andererseits jedoch der Datenschutz auch nicht ökonomischen Gesichtspunkten zum Opfer fallen. Bei einem hohen Risiko für das Recht auf informationelle Selbstbestimmung müssen also auch teure Schutzmaßnahmen ergriffen werden. Die Alternative dazu besteht nur im Verzicht auf die konkrete Art der Verarbeitung.

Für den digitalen Personalausweis ist das Bild hinsichtlich der Sensibilität der verwendeten Identifikationsdaten uneinheitlich.[1846] Einige von ihnen (Größe, Augenfarbe) sind von geringer Relevanz. Die Adresse ist regelmäßig öffentlich verfügbar, auch wenn an der zunehmenden Ablehnung einer Aufnahme in das Telephonbuch ein Trend hin zu einem höheren Schutzbedürfnis erkennbar wird. Aus datenschutzrechtlicher Sicht ist zu beachten, dass die Kombination der unterschiedlichen, für sich genommen nicht sehr sensiblen Daten in ihrer Gesamtheit zu einem gesteigerten Schutzbedürfnis führen kann. Bei der Verwendung biometrischer Merkmale besteht grundsätzlich eine hohe Sensibilität, die in den Risiken der Profilbildung, der Unveränderbarkeit der Merkmale, der Möglichkeit von Rückverfolgbarkeiten und der Verwertung von Zusatzinformationen begründet liegt. Die Verwendung von Volldaten erfordert stärkere Sicherheitsvorkehrungen als die von Templates. Aber auch der Umgang mit den Templates ist insoweit sehr sensibel, als damit im Rahmen von Identifizierungsvorgängen Aussagen über die Identität des Inhabers getroffen werden und im Bereich der elektronischen Signatur in Zukunft möglicherweise rechtsverbindlich gehandelt werden wird.

1842 Simitis-*Ernestus/Geiger*, § 9 Rn. 24, 46; *Gola/Schomerus*, § 9 Rn. 8; s.a. Roßnagel-*Heibey*, Kap. 4.5, Rn. 25.

1843 Simitis-*Ernestus/Geiger*, § 9 Rn. 27; *Schaffland/Wiltfang*, § 9 Rn. 5, 17 f.

1844 Simitis-*Ernestus/Geiger*, § 9 Rn. 41.

1845 Simitis-*Ernestus/Geiger*, § 9 Rn. 34 ff.

1846 Vgl. bereits *Roßnagel/Hornung*, in: Reichl/Roßnagel/Müller 2005, 237.

Bei der elektronischen Gesundheitskarte ist an sich zwischen den Stammdaten des Versicherungsverhältnisses und den Gesundheitsinformationen zu differenzieren. Da erstere jedoch um die Angabe zum Zuzahlungsstatus erweitert werden sollen, aus der unter bestimmten Umständen auf die Gesundheit rückgeschlossen werden kann, handelt es sich auch hier um sensible Daten.[1847] Das Bundesverfassungsgericht hat bereits im Jahre 1972 betont, dass die Offenbarung von Krankheiten, Leiden oder Beschwerden dem Einzelnen unangenehm und peinlich oder seiner sozialen Geltung abträglich sein kann.[1848] Diese Gefahren erhöhen sich durch die moderne automatisierte Datenverarbeitung deutlich. Alle Gesundheitsdaten sind deshalb – bei Abstufungen im Detail – als so sensibel einzustufen, dass ein hohes Schutzbedürfnis besteht.[1849] Dieses wird überdies durch das Allgemeininteresse am Schutz des Vertrauensverhältnisses zwischen Patient und Arzt[1850] weiter erhöht.

Die Daten des privaten Signaturschlüssels der jeweiligen Karte sind extrem sensibel, da mit Hilfe des Schlüssels rechtsverbindliche Erklärungen abgegeben werden können. Dementsprechend stellt das Signaturgesetz an die Erstellung des Schlüssels und den Umgang mit ihm hohe Anforderungen, die auch bei den behandelten Karten beachtet werden müssen.[1851] Diese sind gegenüber der Anlage zu § 9 BDSG vorrangig.

Schließlich müssen die besonderen Bedingungen der Integration unterschiedlicher Funktionalitäten auf einem Medium und die sich daraus ergebenden Gefahren einer Sektorenüberschreitung auch auf der Verhältnismäßigkeitsebene berücksichtigt werden. Je mehr Applikationen auf einer Karte vereint werden, desto größer sind die Anforderungen an die Datensicherheit.

Aufgrund der genannten Gefahren für das Recht auf informationelle Selbstbestimmung muss für alle Daten der untersuchten Karten, vor allem aber für Gesundheitsangaben, biometrischen Daten und Signaturschlüssel ein hohes Sicherheitsniveau verlangt werden. Dem kann nicht das Argument zu hoher Kosten entgegengehalten werden. Will der Staat durch den Einsatz biometrischer Merkmale die Identifizierung per Ausweis verbessern und durch die Verwendung der elektronischen Gesundheitskarte die Effektivität der Gesundheitsversorgung erhöhen, so muss er im Gegenzug auch ein entsprechendes Schutzniveau für die sensiblen Daten garantieren. Da andernfalls die Identifikationsfunktion des digitalen Personalausweises und die Validität der Gesundheitsdaten nicht hinreichend sichergestellt wären, liegt dies auch in seinem eigenen Interesse. Das gilt noch stärker für die Signaturschlüsseldaten: Ein Schutzniveau, dass die Rechtssicherheit abgegebener Erklärungen in Frage stellen würde, würde den Erfolg der elektronischen Signatur im Rechtsverkehr gefährden.

Zur Erfüllung dieser Anforderungen an die Datensicherheit bei Chipkartensystemen besteht eine Reihe von technischen Möglichkeiten. Diese werden zusammen mit den anderen Fragen der Umsetzbarkeit später behandelt.[1852]

1847 S.o. 4.3.4.2.2.

1848 BVerfG, NJW 1972, 1123, 1124.

1849 *Jürgens* 2003, unter 4.2.2; *Dierks/Nitz/Grau* 2003, 231; s.a. *Goetz* 2001, 101.

1850 S. BVerfGE 32, 370 (380); EGMR, Z ./. Finnland, Urteil v. 25.2.1997 (abrufbar unter http://www.echr.coe.int/Eng/Judgments.htm), Abs. 95; s.a. *Ulsenheimer/Heinemann*, MedR 1999, 197, 202; *Lilie* 1980, 78 f.; *Beier* 1979, 55; *Schmidt*, NJW 1962, 1747, 1747; *Laufs*, NJW 1975, 1433, 1434; Roßnagel-*Schirmer*, Kap. 7.12, Rn. 23; näher oben 4.2.3.4.1 und 4.2.3.5.1.

1851 S. dazu unten 5.1.2. Es bestehen auch besondere Dokumentationspflichten (§ 10 SigG); dazu Roßnagel-*Roßnagel*, Kap. 7.7, Rn. 124 ff.

1852 S.u. 6.

5 Signaturrechtliche Fragestellungen

Chipkarten sind derzeit die einzigen Trägermedien, auf denen sichere elektronische Signaturen erstellt werden können. Sie verfügen über Speicher- und Verarbeitungsbereiche, in denen Daten ohne Zugriffsmöglichkeit von außen verwahrt und eingesetzt werden können.

Die Verwendung von Chipkartenausweisen als sichere Signaturerstellungseinheiten ist gegenüber sonstigen Signaturkarten von Vorteil, weil sie einen hohen Verbreitungsgrad in der Bevölkerung aufweisen. Nach § 1 Abs. 1 Satz 1, 1. Halbsatz PersAuswG ist jeder Deutsche verpflichtet, einen Personalausweis zu besitzen. Im 2. Halbsatz der Vorschrift wird zwar eine Ausnahme für Inhaber eines gültigen Reisepasses normiert.[1853] Dennoch dürfte der Personalausweis das Medium mit der größten Verbreitung in Deutschland sein. Die elektronische Gesundheitskarte wird an die Mitglieder der gesetzlichen Krankenversicherung und – im Unterschied zur bisherigen Krankenversichertenkarte – nach § 264 Abs. 4 Satz 2 SGB V auch an nicht versicherte Empfänger laufender Leistungen zum Lebensunterhalt und von Hilfe in besonderen Lebenslagen, nicht aber an privat Versicherte abgegeben werden.

Nach der am 9. März 2005 verabschiedeten „eCard-Strategie" der Bundesregierung sollen sowohl der digitale Personalausweis als auch die elektronische Gesundheitskarte „von vorneherein technisch so ausgestaltet sein, dass sie auf Wunsch der nutzenden Personen auch für qualifizierte Signaturen zu verwenden sind".[1854] Für den digitalen Personalausweis ist bislang keine gesetzgeberische Entscheidung über eine Signaturfunktion gefallen. Anderes gilt für die elektronische Gesundheitskarte. Diese muss gemäß § 291 Abs. 2a Satz 3 SGB V technisch geeignet sein, Authentisierung, Verschlüsselung und elektronische Signatur zu ermöglichen. Damit wird zwar weder die tatsächliche Implementierung dieser Funktionalitäten noch die Verwendung qualifizierter Signaturverfahren vorgeschrieben. Dies wird jedoch auch nicht ausgeschlossen, sodass die Gesundheitskarte als sichere Signaturerstellungseinheit in Frage kommt, wenn sie noch über hinreichende Speicher- und Verarbeitungskapazitäten neben den Anwendungen im Gesundheitswesen verfügt.[1855]

Der Ablauf elektronischer Signaturverfahren auf Chipkartenausweisen unterscheidet sich im Grundsatz nicht von dem auf anderen Signaturkarten. Die Verbindung mit anderen Applikationen auf derselben Karte und die Besonderheiten der Ausgabe- und Anwendungsprozesse verursachen jedoch eine Reihe von spezifischen Rechtsproblemen.

5.1 Das allgemeine Regelungssystem des Signaturgesetzes

5.1.1 Grundlagen und Unterschiede zwischen den Signaturstufen

Elektronische Signaturen dienen in tatsächlicher Hinsicht der Sicherung von Integrität und Authentizität einer Erklärung oder, allgemeiner, von elektronischen Daten.[1856] Derartige Sicherungsinstrumente sind der Rechtsordnung seit jeher geläufig; die bekanntesten Beispiele hierfür sind die Schriftform (§ 126 BGB) und die notarielle Beurkundung (§ 128 BGB). In aller Regel führt die Beachtung oder Nichtbeachtung der rechtlichen Erfordernisse eines solchen Sicherungsinstruments zu besonderen Rechtsfolgen für die Gültigkeit oder

1853 Soweit ersichtlich ist nicht bekannt, wie viele Bürger von dieser Möglichkeit Gebrauch machen.
1854 S. http://www.bundesregierung.de/-,413.799497/artikel/eCard-Strategie-der-Bundesregi.htm.
1855 Vgl. hierzu *Hornung* 2004a, 229 f.; *BITKOM/VDAP/VHitG/ZVEI* 2003, 46; s.a. *Krüger-Brand*, DÄ 2002, A 3304.
1856 Hierzu, und zur Funktionsweise der Signaturerstellung, s.o. 2.3.2.

den Beweiswert einer Erklärung. Rechtsgeschäfte, die der durch Gesetz vorgeschriebenen Form ermangeln, sind nach § 125 Satz 1 BGB nichtig; nach § 125 Satz 2 BGB gilt das im Zweifel auch für die gewillkürte Form. Für öffentliche und private Urkunden gelten die besonderen Beweisregeln der §§ 415 ff. ZPO.

Dementsprechend hat der Gesetzgeber in den letzten Jahren auch für die elektronische Signatur zunächst im Signaturgesetz und der Signaturverordnung rechtliche Voraussetzungen geschaffen und in einem zweiten Schritt an die Beachtung dieser Voraussetzungen Rechtsfolgen geknüpft.[1857] Im privaten Bereich ersetzt die elektronische Form nach §§ 126 Abs. 3, 126a BGB die gesetzliche Schriftform.[1858] Hierzu muss der Aussteller der Erklärung dieser seinen Namen hinzufügen und das Dokument mit einer qualifizierten elektronischen Signatur versehen. Für die gewillkürte Form bestimmt § 127 Abs. 3 BGB, dass im Zweifel auch eine nicht qualifizierte Signatur zur Formwahrung ausreicht. In diesem Fall kann jedoch eine nachträgliche qualifizierte Signatur oder, wenn einer der Parteien dies nicht möglich ist, eine § 126 BGB entsprechende Beurkundung verlangt werden.[1859] Liegt eine elektronische Willenserklärung nach § 126a BGB vor, so ordnet ein „vorgezogener Anscheinsbeweis" in § 371a Abs. 1 Satz 2 ZPO an, dass der Anschein ihrer Echtheit, der sich auf Grund der Prüfung nach dem Signaturgesetz ergibt, nur durch Tatsachen erschüttert werden kann, die ernstliche Zweifel daran begründen, dass die Erklärung mit dem Willen des Signaturschlüssel-Inhabers abgegeben worden ist.[1860]

Für die öffentliche Verwaltung wurden die entsprechenden Grundlagen im Dritten Gesetz zur Änderung verwaltungsrechtlicher Vorschriften[1861] gelegt. Dieses beinhaltet Spezialregelungen für 67 Gesetze und Verordnungen aus dem besonderen Verwaltungsrecht des Bundes und Generalklauseln für die allgemeinen Verfahrensgesetze. § 3a VwVfG, § 36a Abs. 2 SGB I und § 87a Abs. 2 und 3 AO ordnen die Gleichstellung der elektronischen Form mit der Schriftform an, wenn das Dokument mit einer qualifizierten elektronischen Signatur nach dem Signaturgesetz versehen wurde. Für das verwaltungsgerichtliche Beweisverfahren ist § 371a ZPO über die Verweisung in § 173 Satz 1 VwGO entsprechend anzuwenden. Derartige Verweisungsnormen sind auch in anderen speziellen Prozessordnungen enthalten, nämlich in § 46 Abs. 2 Satz 1 ArbGG, § 155 FGO und § 202 SGG.[1862] Eine eigenständige Regelung findet sich demgegenüber in § 87a Abs. 5 AO. Weitere Bestimmungen zur Verwendung elektronischer Signaturen im gerichtlichen Verfahren finden

---

1857 Das erste SigG trat 1997, das zweite 2001 in Kraft; zu Hintergrund und Gesetzgebungsgeschichte vgl. RMD-*Roßnagel*, Einl. SigG Rn. 146 ff.; s.a. *Bröhl/Tettenborn* 2001. Die Rechtsfolgen des Gesetzes von 2001 sind weitgehend durch die Bestimmungen in Art. 5 RLeS vorgegeben; zum europarechtlichen Hintergrund s. RMD-*Roßnagel*, Einl. SigG Rn. 105 ff. m.w.N.; *Rapp* 2002, 36 ff.

1858 S. hierzu *Boente*/*Riehm*, Jura 2001, 793; *GI*, DuD 2001, 38 ff.; *Malzer* 2000, 173 ff.; *Müglich*, MMR 2000, 7 ff.; *Oertel*, MMR 2001, 419 ff.; *Roßnagel*, NJW 2001, 1817 ff.; *Sieber/Nöding*, ZUM 2001, 199, 203 ff.; hierdurch werden Art. 5 Abs. 1 RleS, 9 RLeG umgesetzt, s. näher *Roßnagel*, K&R 2000, 313, 315 ff.

1859 S. näher *Vehslage*, DB 2000, 1801, 1802.

1860 S. hierzu (auf der Basis der wortgleichen Vorläufernorm des § 292a ZPO a.F.) und den Hintergründen *Roßnagel*, NJW 2001, 1817, 1826 m.w.N.; *Borges*, K&R 2001, 196 ff.; *Müglich*, MMR 2000, 7, 12 f.; *Scheffler*/*Dressel*, CR 2000, 378 ff.; *Dästner*, NJW 2001, 3469 ff.; *Fischer-Dieskau/Gitter/Paul/Steidle*, MMR 2002, 709. Bereits vor der Einführung von § 292a ZPO normierte § 1 Abs. 1 SigG 1997 eine Sicherheitsvermutung zugunsten elektronischer Signaturen, die entsprechend dem damaligen SigG erstellt wurden; s. näher *Roßnagel*, NJW 1998, 3312 ff.

1861 V. 21.8.2002, BGBl. I, 3322; s. *Roßnagel*, NJW 2003, 469 ff.; *Schmitz/Schlatmann*, NVwZ 2002, 1281 ff.; *Schlatmann*, LKV 2002, 489; *Geis*, K&R 2003, 21 ff.; Manssen-*Skrobotz*, § 1 SigG Rn. 97 ff. m.w.N.

1862 Zur Verwendung der Signatur im Gerichtsverfahren vgl. RMD-*Roßnagel*, Einl. SigG Rn. 281 ff.

sich im Gesetz über die Verwendung elektronischer Kommunikationsformen in der Justiz, das am 1. April 2005 in Kraft trat.[1863]

Aufgrund dieser weitgehenden rechtlichen Gleichstellung kann man die elektronische Signatur im Ergebnis als Funktionsäquivalent zur eigenhändigen Unterschrift bezeichnen.[1864] Das gilt jedoch nur mit zwei Einschränkungen. Zum einen schließen einige spezialgesetzliche Normen die Formäquivalenz aus.[1865] Zum anderen werden nur solche elektronische Signaturen gleichgestellt, die bestimmte, im Signaturgesetz normierte Anforderungen erfüllen. Das Signaturgesetz unterscheidet terminologisch zwischen einfachen, fortgeschrittenen, qualifizierten und akkreditierten elektronischen Signaturen,[1866] wobei sich daneben eine Tendenz zur Kreation weiterer spezialgesetzlicher Ausdifferenzierung beobachten lässt.[1867]

Einfache elektronische Signaturen sind nach § 2 Nr. 1 SigG Daten in elektronischer Form, die anderen elektronischen Daten beigefügt werden oder logisch mit ihnen verknüpft sind und zur Authentifizierung dienen. Ein Beispiel hierfür ist die eingescannte Unterschrift.[1868] Diese elektronischen Signaturen müssen nicht fälschungssicher sein.

§ 2 Nr. 2 SigG regelt fortgeschrittene elektronische Signaturen. Diese müssen ausschließlich dem Signaturschlüssel-Inhaber zugeordnet sein, seine Identifizierung ermöglichen, mit Mitteln erzeugt werden, die der Signaturschlüssel-Inhaber unter seiner alleinigen Kontrolle halten kann und mit den Daten, auf die sie sich beziehen, so verknüpft sein, dass eine nachträgliche Veränderung der Daten erkannt werden kann.[1869]

Qualifizierte elektronische Signaturen sind gemäß § 2 Nr. 3 SigG fortgeschrittene elektronische Signaturen im Sinne von § 2 Nr. 2 SigG, die überdies auf einem zum Zeitpunkt ihrer Erzeugung gültigen qualifizierten Zertifikat beruhen und mit einer sicheren Signaturerstellungseinheit erzeugt werden. Die Definition des qualifizierten Zertifikats findet sich in § 2 Nr. 7 SigG. Erforderlich ist die Ausstellung für eine natürliche Person, die Beachtung von § 7 SigG (Mindestangaben und qualifizierte Signatur des Zertifikats) und die Ausstellung durch einen Zertifizierungsdiensteanbieter, der mindestens den Erfordernissen nach §§ 4 bis 14 oder § 23 SigG und der sich darauf beziehenden Vorschriften der Signaturverordnung genügt. Sichere Signaturerstellungseinheiten sind nach § 2 Nr. 10 SigG Software- oder Hardwareeinheiten zur Speicherung und Anwendung des jeweiligen Signaturschlüssels, die für qualifizierte elektronische Signaturen bestimmt sind und die Anforderungen nach § 17 oder § 23 SigG und der Verordnung erfüllen.

„Akkreditierte Signaturen“[1870] entsprechen in technischer Hinsicht qualifizierten Signaturen. Der Unterschied besteht jedoch darin, dass sie von Zertifizierungsdiensteanbietern ausgestellt werden, deren technische und administrative Prozesse nach § 15 SigG zuvor auf

---

1863 „Justizkommunikationsgesetz“, BGBl. I, 837; s. dazu *Viefhues*, NJW 2005, 1009 ff.; *Fischer-Dieskau*, MMR 2003, 704 ff.

1864 RMD-*Roßnagel*, Einl. SigG Rn. 322, § 2 SigG 1997 Rn. 25; Manssen-*Skrobotz*, § 1 SigG Rn. 38 ff. m.w.N.

1865 S. etwa §§ 484, 492, 623, 761, 766, 780, 781 BGB.

1866 Ausführlich *Roßnagel* 2002, 31 ff.; RMD-*Roßnagel*, Einl. SigG Rn. 176 ff.; s.a. Manssen-*Demmel*, § 2 SigG Rn. 1 ff. Die Unterscheidung ist durch die Signaturrichtlinie bedingt.

1867 S. etwa die „qualifizierte elektronische Signatur mit Einschränkungen“ nach § 87a Abs. 6 AO und der Steuerdatenübermittlungsverordnung; hierzu *Roßnagel*, K&R 2003, 379 ff.; *ders.*, MMR 2002, 215 ff.

1868 RMD-*Roßnagel*, Einl. SigG Rn. 176.

1869 S. ausführlich *Roßnagel*, MMR 2003, 164 ff. Auch hier finden sich keine Anforderungen an die Fälschungssicherheit.

1870 Dieser Begriff wird vom Gesetz nicht verwendet, das in § 15 Abs. 1 Satz 4 SigG „qualifizierte elektronische Signaturen mit Anbieterakkreditierung“ legaldefiniert. Der Gesetzgeber hat damit von Art. 3 Abs. 2 RLeS Gebrauch gemacht.

ihre Sicherheit überprüft wurden. Zuständig für diese und die übrigen Aufgaben des Signaturgesetzes ist gemäß § 3 SigG die Regulierungsbehörde für Telekommunikation und Post.

Bezüglich der Rechtsfolgen lassen sich die fünf im Signaturgesetz definierten Signaturformen in drei Stufen unterteilen, nämlich akkreditierte, qualifizierte und sonstige Signaturen, wobei die letzte Gruppe alle verbleibenden Verfahren (einfache, fortgeschrittene, eingeschränkte und andere) einschließt. Die drei Stufen unterscheiden sich in einer Reihe von Punkten:[1871]

- Bezüglich der technischen und organisatorischen Prozesse verfügen akkreditierte Verfahren über eine nachgewiesene, qualifizierte über eine behauptete Sicherheit. Sonstige Signaturen unterliegen hier keinen gesetzlichen Anforderungen.
- Nur für akkreditierte Anbieter stellt die Regulierungsbehörde nach § 16 Abs. 1 SigG ein qualifiziertes (Wurzel-)Zertifikat aus; andere Anbieter müssen auf dieses verzichten.
- Akkreditierte wie qualifizierte elektronische Signaturen erfüllen die erwähnten Formvorschriften, sonstige Signaturen nicht.
- Gleiches gilt auch für die Vorschriften des Beweisrechts, wobei sonstige Verfahren im Wege der freien Beweiswürdigung herangezogen werden können und damit nicht vollständig wirkungslos sind.
- Zertifikate von akkreditierten Anbietern müssen gemäß § 4 Abs. 2 SigV nach Ablauf ihrer Gültigkeit noch mindestens 30 Jahre prüf- oder abrufbar gehalten werden. Außerdem übernimmt die Regulierungsbehörde nach § 15 Abs. 6 SigG bei einer Einstellung des Betriebs des Anbieters die Zertifikate. Bei qualifizierten Zertifikaten ist der Zeitraum der Pflichtaufbewahrung auf fünf Jahre reduziert, und es existiert kein Schutz für den Fall der Betriebseinstellung. Sonstige Signaturverfahren unterliegen den Anforderungen an die Langzeitprüfbarkeit nicht.
- Die Regelungen über die Aufbewahrung der Dokumentation der Sicherheitsmaßnahmen sowie über die Ausstellung und Sperrung von Zertifikaten weisen für die unterschiedlichen Signaturstufen nach § 8 Abs. 3 SigV dieselben Unterschiede wie bei der Langzeitprüfbarkeit auf.
- Für ausländische Signaturverfahren gilt, dass sie akkreditierten Verfahren nach § 23 Abs. 2 SigG nur dann gleichgestellt sind, wenn sie nachweislich gleichwertige Sicherheit aufweisen. Bei qualifizierten Verfahren müssen demgegenüber nach § 23 Abs. 1 SigG alle Signaturen anerkannt werden, die innerhalb der Europäischen Gemeinschaft und des Europäischen Wirtschaftsraums entsprechend der jeweiligen nationalen Regelungen über qualifizierte Verfahren erstellt werden. Dies kann dann problematisch sein, wenn die Sicherheitsanforderungen niedriger als die des deutschen Rechts sind.
- Auf der Ebene der Haftung besteht schließlich für akkreditierte und qualifizierte Verfahren eine Verschuldenshaftung mit Beweislastumkehr nach § 11 Abs. 1 SigG gegenüber Dritten, die auf die Gültigkeit der Zertifikate vertrauen. Sie erfasst auch reine Vermögensschäden und ist durch eine obligatorische Deckungsvorsorge (§ 12 SigG in Verbindung mit § 9 SigV) abgesichert. Demgegenüber greift bei sonstigen Verfahren nur die Haftung des § 823 Abs. 1 BGB ein.

Im Ergebnis weisen akkreditierte Verfahren eine Vielzahl von Vorteilen gegenüber qualifizierten und sonstigen Verfahren auf. Sie sind deshalb am besten für rechtsverbindliches

1871 S. zum Folgenden ausführlich RMD-*Roßnagel*, Einl. SigG Rn. 181 ff.; *ders.*, MMR 2002, 215 ff.; *ders.*, NJW 2001, 1817, 1819 ff.

Handeln im elektronischen Rechtsverkehr geeignet. Die Unterscheidung zwischen akkreditierten und qualifizierten Signaturverfahren und die Zurückhaltung des Gesetzgebers hinsichtlich einer Anordnung der Verwendung akkreditierter Signaturen ist nur vor dem Hintergrund der europäischen Signaturrichtlinie zu erklären, die in Art. 3 Abs. 1 eine allgemeine Pflicht zur Anbieterakkreditierung ausdrücklich untersagt und in Art. 3 Abs. 7 Vorschriften über die Verwendung akkreditierter Signaturen nur unter engen Voraussetzungen zulässt.[1872]

5.1.2 Allgemeine signaturrechtliche Anforderungen an qualifizierte Verfahren

Falls der digitale Personalausweis oder die elektronische Gesundheitskarte fähig sein werden, qualifizierte elektronische Signaturen zu erstellen, so folgt daraus eine Reihe von Anforderungen an die jeweilige Chipkarte und die Produktions-, Antrags-, Ausgabe- und sonstigen Verfahren. Diese Anforderungen lassen sich in zwei Gruppen unterscheiden: zum einen allgemeine Erfordernisse, die auch die bisherigen Signaturkarten und Zertifizierungsprozesse erfüllen, zum anderen Besonderheiten, die sich durch die Verbindung mit anderen Funktionalitäten der Karte oder sonstigen Besonderheiten von Chipkartenausweisen ergeben. Die erste Gruppe wird im Folgenden nur kurz zusammengefasst.[1873]

Die jeweilige Chipkarte ist zunächst so zu wählen, dass sie als sichere Signaturerstellungseinheit nach § 2 Nr. 10 SigG geeignet ist. Dazu muss sie nach § 17 Abs. 1 Satz 1 SigG „Fälschungen der Signaturen und Verfälschungen signierter Daten zuverlässig erkennbar machen und gegen unberechtigte Nutzung der Signaturschlüssel schützen“.[1874] § 17 Abs. 1 Satz 2 SigG ermöglicht optional die Schlüsselerzeugung in der Signaturerstellungseinheit selbst. In diesem Fall gelten die Anforderungen nach § 17 Abs. 3 Nr. 1 SigG entsprechend. Danach ist die Einmaligkeit und Geheimhaltung der Signaturschlüssel zu gewährleisten und eine Speicherung außerhalb der sicheren Signaturerstellungseinheit auszuschließen.[1875] Darüber hinaus bestehen weitere Anforderungen nach § 15 Abs. 1 SigV und der Anlage 1 zur Signaturverordnung. Die Karte muss danach gewährleisten, dass der Signaturschlüssel erst nach Identifikation durch Besitz (der sicheren Signaturerstellungseinheit) und Wissen (beispielsweise einer PIN) oder durch Besitz und ein oder mehrere biometrische Merkmale angewendet werden kann;[1876] der Signaturschlüssel darf nicht preisgegeben werden.[1877] Außerdem muss es unmöglich sein, aus dem öffentlichen Schlüssel oder einer Signatur den geheimen Schlüssel zu errechnen oder diesen zu dupli-

1872 In der Folge hatten sich alle 28 Zertifizierungsdiensteanbieter in Deutschland, die im Mai 2005 qualifizierte elektronische Signaturverfahren anboten, auch akkreditieren lassen. Nur der Anbieter D-Trust betreibt zusätzlich ein nur qualifiziertes Signaturverfahren.

1873 Die Prozesse der Akkreditierung bleiben dabei ausgeklammert, da sich hieraus keinerlei Änderungen hinsichtlich der Karte und der sie betreffenden Verfahren ergeben.

1874 Dabei handelt es sich allerdings um weitgehend technikneutrale und generische Anforderungen, s. näher *Bröhl/Tettenborn* 2001, 99; *Roßnagel*, BB 2002, 261, 263. Wie diese umzusetzen sind, bleibt dem Anbieter überlassen, s. RMD-*Roßnagel/Pordesch*, § 14 SigG 1997, Rn. 3.

1875 Bei einer Erzeugung außerhalb der Chipkarte gelten diese Anforderungen auch für den Vorgang der Übertragung auf die Karte. Nähere Ausformungen finden sich in § 5 Abs. 1 SigV.

1876 Wird zum Freischalten eine PIN verwendet, so darf diese nur für die Signatur einsetzbar sein. Für andere Kartenfunktionen wie Authentisierung oder Verschlüsselung ist eine separate PIN erforderlich; zur Verwendung von Biometrie vgl. unten 5.2.6.

1877 Das erfordert nicht nur die Speicherung, sondern auch die Verwendung des Schlüssels zur Signaturerstellung in einem gesicherten Bereich. Nur das Ergebnis des Vorgangs darf an die Umgebung mitgeteilt werden, s. RMD-*Roßnagel/Pordesch*, § 14 SigG 1997 Rn. 62.

zieren.[1878] Diese Eigenschaften werden nach § 17 Abs. 4 SigG in Verbindung mit § 18 SigG von einer Prüfstelle bestätigt.

Neben diesen Anforderungen an den Chipkartenausweis selbst enthält das Signaturrecht Bestimmungen für die Prozesse der Zertifizierungsdiensteanbieter. Diese haben zunächst die Person, die ein qualifiziertes Zertifikat beantragt, nach § 5 Abs. 1 Satz 1 SigG zuverlässig zu identifizieren.[1879] § 3 Abs. 1 Satz 1 SigV bestimmt, dass dies anhand eines Personalausweises, Reisepasses oder eines Dokumentes mit gleichwertiger Sicherheit zu erfolgen hat. Bis zum Inkrafttreten des Ersten Gesetzes zur Änderung des Signaturgesetzes am 11. Januar 2005[1880] musste die Identifizierung bei der Beantragung der Signaturkarte erfolgen; seitdem kann mit Einwilligung des Antragstellers auf bereits vorliegende Identifizierungsdaten zurückgegriffen werden.[1881] Nach § 5 Abs. 2 Satz 2 SigG müssen auch Attribute des Schlüsselinhabers nachgewiesen werden. Attribute sind nach § 5 Abs. 2 Satz 1 SigG Vertretungsmacht sowie berufsbezogene oder sonstige Angaben zur Person des Schlüsselinhabers. Ihr Nachweis erfolgt gemäß § 3 Abs. 2 SigG durch ein qualifiziert signiertes oder schriftliches Dokument.

Nach Identifizierung und Schlüsselerzeugung wird die Zuordnung des öffentlichen Schlüssels zu der identifizierten Person nach § 5 Abs. 1 Satz 2 SigG in einem qualifizierten Zertifikat bestätigt. Dessen Inhalt ergibt sich aus § 7 SigG. Es muss den Namen (oder ein Pseudonym) des Signaturschlüssel-Inhabers, den öffentlichen Signaturschlüssel, Prüfangaben, die Zertifikatsnummer, den Beginn und das Ende der Zertifikatsgültigkeit, den Namen und Sitz des Anbieters, Angaben zur Beschränkung des Zertifikats und die Angabe enthalten, dass es sich um ein qualifiziertes Zertifikat handelt.[1882] Darüber hinaus können bei Bedarf Attribute des Schlüsselinhabers hinzugefügt werden, die nach § 7 Abs. 2 SigG auch in ein gesondertes Attribut-Zertifikat aufgenommen werden können.[1883]

Im nächsten Schritt hat sich der Zertifizierungsdiensteanbieter nach § 5 Abs. 6 SigG davon zu überzeugen, dass der Antragssteller die zugehörige sichere Signaturerstellungseinheit besitzt. § 5 Abs. 2 Satz 1 SigV verlangt im Grundsatz eine persönliche Übergabe der Schlüssel und Identifikationsdaten auf der Chipkarte, es kann jedoch durch formfreie Vereinbarung eine andere Übergabeform bestimmt werden. Anders als nach der Rechtslage bis zum 11. Januar 2005 ist es auch nicht mehr erforderlich, dass der Signaturschlüssel-Inhaber die Übergabe schriftlich oder mittels eines qualifiziert signierten Dokuments bestätigt; hierzu reicht vielmehr die Textform aus.[1884] Nach der Bestätigung des Inhabers darf gemäß § 5 Abs. 2 Satz 2 SigV das Zertifikat nachprüfbar oder – mit Willen des Signaturschlüssel-Inhabers – abrufbar gehalten werden.[1885]

1878 S. RMD-*Roßnagel/Pordesch*, § 16 SigV 1997 Rn. 32 ff.; zu einzelnen Angriffen s. *dies*., § 14 SigG 1997 Rn. 68 ff. m.w.N.

1879 Näher RMD-*Roßnagel*, § 5 SigG 1997 Rn. 36 f.; Manssen-*Demmel*, § 5 SigG Rn. 2 ff.

1880 BGBl. I, 2; vgl. näher *Roßnagel*, NJW 2005, 385 ff.; *Bergfelder*, CR 2005, 148 ff.

1881 Kritisch dazu *Roßnagel*, NJW 2005, 385, 387 f.

1882 Zum Inhalt des Zertifikats s. RMD-*Roßnagel*, § 7 SigG 1997 Rn. 30 ff. Der Inhaber hat nach § 5 Abs. 3 Satz 1 SigG einen Anspruch auf Verwendung eines Pseudonyms, s. hierzu Roßnagel-*Roßnagel*, Kap. 7.7, Rn. 61 ff., 116 ff.; zur Frage der Beschränkung vgl. *Fischer-Dieskau/Gitter/Hornung*, MMR 2003, 384 ff.

1883 Dessen nähere Ausgestaltung richtet sich nach § 14 Abs. 2 SigV.

1884 S. dazu *Roßnagel*, NJW 2005, 385, 386; *Skrobotz*, DuD 2004, 410, 412.

1885 Wird das Zertifikat nur nachprüfbar gehalten, so sendet der Empfänger einer signierten Erklärung das mitübersandte Zertifikat zum Anbieter und erhält lediglich die Information, ob dieses gültig ist. Wird das Zertifikat dagegen abrufbar gehalten, so ist es jedermann möglich, es mit Hilfe der Zertifikatsnummer online abzufragen. Je nach Inhalt (v.a. von Attributen) kann dies datenschutzrechtliche Implikationen haben; s. näher *Roßnagel*, DuD 1995, 582, 584 ff.; Roßnagel-*Roßnagel*, Kap. 7.7, Rn. 82 ff.

Gemäß § 6 Abs. 1 Satz 1 SigG ist parallel zur Übergabe eine Unterrichtung über Sicherheitsmaßnahmen bei der Signaturerstellung und -prüfung erforderlich.[1886] Gleiches gilt nach § 6 Abs. 1 Satz 2 SigG für das Erfordernis, die Daten neu zu signieren, bevor der Sicherheitswert einer vorhandenen Signatur geringer wird, und nach § 6 Abs. 2 SigG für die Formäquivalenz einer qualifizierten elektronischen Signatur. Die nähere Ausgestaltung der Unterrichtung wird durch § 6 SigV geregelt. Auch sie kann gemäß § 6 Abs. 3 Satz 1 n.F. in Textform erfolgen.[1887] Im Ergebnis ist damit durch das Erste Gesetz zur Änderung des Signaturgesetzes die Möglichkeit einer Beantragung und Ausgabe von Signaturkarten ohne persönlichen Kontakt mit dem Karteninhaber geschaffen worden.[1888]

Schließlich hat der Zertifizierungsdiensteanbieter nach § 8 Abs. 1 SigG einen Sperrdienst einzurichten, der es ermöglicht, auf Verlangen des Signaturschlüssel-Inhabers oder seines Vertreters das Zertifikat zu sperren.[1889] § 7 Abs. 1 SigV verlangt hierzu die Einrichtung einer ständig erreichbaren Rufnummer. Gemäß § 7 Abs. 2 SigV muss vor der Sperrung die Identität des Berechtigten geprüft werden. Dies geschieht regelmäßig durch ein Sperrkennwort. Der Anbieter hat außerdem eine Sperrung vorzunehmen, wenn das Zertifikat aufgrund falscher Angaben ausgestellt wurde, der Anbieter seine Tätigkeit beendet und diese nicht von einem anderen Anbieter fortgeführt wird, ein sonstiger vertraglich vereinbarter Sperrgrund eintritt, sowie auf Anordnung der Regulierungsbehörde.

5.2 Spezifische Probleme bei Chipkartenausweisen

5.2.1 Das Konzept des „elektronischen Ausweises" als Mittel zur Authentisierung in Online-Verfahren

5.2.1.1 Problemstellung

Elektronische Signaturverfahren sind funktional ein Ersatz für die Unterschrift des Signaturschlüssel-Inhabers.[1890] Eine Unterschrift ermöglicht im herkömmlichen Rechtsverkehr die nachträgliche Zuordnung einer Erklärung zu einer Person (etwa mittels eines graphologischen Gutachtens), sie gibt jedoch selbst keinen Aufschluss über die Identität des Unterzeichnenden.[1891] Ähnliches gilt auch für die elektronische Signatur. Der Name des Schlüsselinhabers ist zwar nach § 7 Abs. 1 Nr. 1 SigG grundsätzlich im Zertifikat enthalten. Dieser kann aber stattdessen ein Pseudonym wählen. Auch im Fall der Namensgleichheit besteht keine Möglichkeit, aus dem Zertifikat selbst auf den Unterzeichnenden zu schließen.

Ermöglicht wird die Zuordnung erst durch die – weltweit einmalige – Zertifikatsnummer.[1892] In einem Streitfall kann so bestimmt werden, wer die elektronische Signatur er-

---

1886 S. zur alten Rechtslage RMD-*Roßnagel*, § 6 SigG 1997, Rn. 19 ff.; RMD-*ders*., § 6 SigV 1997 Rn. 20 ff.

1887 Dazu *Roßnagel*, NJW 2005, 385, 386; *Skrobotz*, DuD 2004, 410, 412; *Bergfelder*, CR 2005, 148, 149.

1888 Zu den daraus resultierenden Problemen für die Authentizität der Signatur vgl. *Roßnagel*, NJW 2005, 385, 387 f.; ohne Bedenken *Bergfelder*, CR 2005, 148, 149.

1889 Näher Roßnagel-*Roßnagel*, Kap. 7.7, Rn. 94 ff.; s.a. RMD-*ders*., § 8 SigG 1997 Rn. 30 ff.; RMD-*ders*., § 9 SigV 1997 Rn. 22 ff.

1890 S. bereits *Hammer* 1995, 265; ferner RMD-*Roßnagel*, § 2 SigG 1997 Rn. 25; *ders.*, NJW 2001, 1817, 1825.

1891 Selbst wenn der Name zu entziffern ist (was nach BGH, NJW 1997, 3380, 3381; NJW 1994, 55 bei der Unterschrift nicht erforderlich ist), besteht keine Möglichkeit zu bestimmen, ob eine zweite Person selben Namens existiert.

1892 Entsprechend dem Standard X-509 der ITU, s. *Roßnagel*, DuD 2002, 281, 282.

stellt hat, auch wenn sich die prozessuale Einführung und Durchsetzung des Aufdeckungsvorgangs schwierig gestalten dürfte. Für den Fall eines Zertifikatspseudonyms ist das Fehlen einer Regelung über die Aufdeckung zu Recht bemängelt worden.[1893] Das Problem stellt sich aber im Prinzip bei jeder Signatur eines nicht weltweit einmaligen Namens genauso, da auch durch einen Namenszusatz nach § 7 Abs. 1 Nr. 1 SigG für den Erklärungsempfänger die Identität nicht notwendigerweise bekannt wird.[1894]

Unabhängig von dieser verfahrensrechtlichen Frage war jedoch exakt diese Form der eingeschränkten Anonymität bei der Konzeption der Signatur gewollt; es sollte vermieden werden, dass der Bürger bei jeder Handlung im elektronischen Rechtsverkehr seine Identität preisgeben muss, obwohl dies bei den bisherigen Verfahren nicht der Fall ist.[1895]

In der überwiegenden Zahl der Anwendungen im privaten, aber auch im öffentlichen Bereich reicht diese Form der Sicherheit völlig aus. Bei manchen Verfahren genügt es jedoch nicht, erst nachträglich und im Streitfall die Identität einer handelnden Person zu bestimmen. Werden etwa – insbesondere bei einem elektronischen Erstkontakt – durch den Kommunikationspartner personenbezogene Daten übermittelt oder geheime Informationen bereitgestellt, so muss bereits vorher feststehen, wem die Informationen offenbart werden. Derartiges kann insbesondere bei vollautomatisierten Verfahren in der öffentlichen Verwaltung der Fall sein,[1896] ist jedoch grundsätzlich auch im privaten Umfeld denkbar.

In der körperlichen Welt wird dieses Problem mit amtlichen oder privaten Ausweisen gelöst. Diese Funktion kann die elektronische Signatur selbst nicht erfüllen, solange das Zertifikat keine eindeutige Angabe enthält, die auch der Empfänger der Signatur bereits als internes Ordnungskriterium verwendet. Deshalb besteht das Problem in den Ländern nicht, die über eine einheitliche Personenkennziffer verfügen und diese in das Zertifikat aufnehmen. Dies ist etwa in Skandinavien üblich.[1897] In Deutschland existiert dagegen kein derartiges System.[1898] Damit muss nach anderen Lösungen gesucht werden.

5.2.1.2 Lösungswege

Diese könnten etwa in der Aufnahme ergänzender Identifikationsdaten (Geburtsdatum und -ort, Wohnort, Personalausweisnummer) in das Schlüsselzertifikat bestehen. Aus Sicht des Schlüsselinhabers hätte das jedoch den gravierenden Nachteil, dass dann jeder Empfänger des Zertifikats diese Daten einsehen könnte.[1899] Dies wäre ein nicht erforderlicher Eingriff in das informationelle Selbstbestimmungsrecht des Schlüsselinhabers und würde die erläuterte Konzeption der elektronischen Signatur aushebeln. Das Problem wird zwar dann umgangen, wenn die weiteren Informationen in ein Attribut-Zertifikat aufgenommen

---

1893 S. Roßnagel-*Roßnagel*, Kap. 7.7, Rn. 121; *Roßnagel/Pfitzmann/Garstka* 2001, 151 f.; s. näher oben 4.3.1.

1894 Das ist nur dann der Fall, wenn dieser Zusatz selbst eine Zuordnung ermöglicht. Das ist bspw. bei der Adresse möglich, nicht aber bei einer Nummer, die einem mehrfach vorkommenden Namen beigefügt wird (Müller1, Müller2,...). Diese Möglichkeit wird in der Gesetzesbegründung zum SigG 1997 ausdrücklich genannt, s. BR-Drs. 966/96, 34; RMD-*Roßnagel*, § 7 SigG 1997, Rn. 33.

1895 Das wird übersehen von *Baum*, DuD 1999, 511 ff., wonach der „Name" i.S.v. § 7 Abs. 1 Nr. 1 SigG auch weitere Identifizierungsdaten umfassen soll. Dies widerspricht sowohl dem Sprachgebrauch als auch der gesetzgeberischen Konzeption; s. *Roßnagel*, DuD 2002, 281, 282; Roßnagel-*ders.*, Kap. 7.7, Rn. 51 ff.

1896 *Klinger*, V&M 2002, 76 ff.; *Roßnagel*, DuD 2002, 281, 282 f.; *ders*. 2002, 49 f.; *Meinel/Gollan*, JurPC Web-Dok. 223/2002, Abs. 10.

1897 Bspw. in Finnland, Estland und Schweden, s.o. 3.2.1.1, 3.2.1.2 und 3.5.1.3.

1898 Zum Problem der Kennziffer nach deutschen Recht vgl. oben 4.2.1.2.4 und 4.2.2.1.2.

1899 *Roßnagel*, DuD 2002, 281, 283 f.; s.a. *Meinel/Gollan*, JurPC Web-Dok. 223/2002, Abs. 11.

werden. Dann müsste jedoch der Inhaber – zumindest nach dem gegenwärtigen Geschäftsmodell der Zertifizierungsdiensteanbieter[1900] – hierfür die Ausstellungskosten und die jährliche Zertifikatsgebühr tragen, was angesichts der wenigen Anwendungsfälle des Attributs nicht zu rechtfertigen wäre.

Eine weitere Möglichkeit ist der Weg, der im JobCard-Verfahren beschritten wird.[1901] Der Arbeitnehmer meldet sich bei der „Registratur Fachverfahren" an, die seine Zertifikatsnummer mit der Sozialversicherungsnummer verknüpft. Damit besteht eine exakte Zuordnung zwischen dem qualifizierten Zertifikat und dem internen Ordnungskriterium der Zentralen Speicherstelle. Diese Zuordnung ermöglicht es, auf der Basis eines signierten Antrags auf Übermittlung der gespeicherten Bescheinigungen die Person des Antragsstellers sicher zu bestimmen, seine Daten im System der Zentralen Speicherstelle aufzufinden und an die Arbeitsagentur zu übermitteln. Da dieses Verfahren jedoch eine Anmeldung bei der jeweils Daten speichernden Stelle voraussetzt, bietet es keine generelle Lösung für das hier angesprochene Problem, denn eine universale Authentisierungslösung sollte unabhängig von einem solchen persönlichen Kontakt funktionieren. Außerdem müssten bei einer Vielzahl von Stellen derartige Zuordnungssysteme verwaltet werden. Das ist bei kleinen Anwendungen und im privaten Bereich unrealistisch.

Ein Ausweg könnte darin bestehen, eine gesonderte allgemeine Zuordnungsstelle einzurichten, in der die Zertifikatsnummern mit weiteren Identifizierungsdaten verknüpft würden und auf die öffentliche und private Stellen immer dann Zugriff hätten, wenn sie auf eine sichere Identifizierung nicht verzichten wollen. Denkbar wäre auch eine Ergänzung der Melderegister um die Zertifikatsnummer.[1902] Dies würde ein hochverfügbares interoperables Netz der ca. 6.500 Meldestellen in Deutschland erfordern. Durch die Reform des Melderechts-Rahmengesetzes aus dem Jahre 2002[1903] wird eine solche Vernetzung angestrebt, die auch eine gegenseitige Abfrage zuließe. Der Aufbau einer derartigen Identifizierungsinfrastruktur ist jedoch überflüssig, da das hier im Folgenden vorgeschlagene Modell die Zertifikatsprüfstruktur der Zertifizierungsdiensteanbieter nutzt, ohne weitere Abfragedienste zu benötigen. Darüber hinaus führt eine Vernetzung der Meldebehörden zu Intransparenz für die Betroffenen und enthält Gefahren der Profilbildung.[1904] Schließlich müsste das System allgemein offen stehen, weil auch private Anwendungen auf eine sichere Identifizierung angewiesen sein können. Damit würde das Verfahren jedoch funktional einer Erweiterung des Datensatzes des Hauptzertifikats entsprechen, da jedermann die Zertifikatsnummern und die weiteren Daten zusammenführen könnte. Die Argumente gegen diese Erweiterung sind deshalb auch auf die Einrichtung eines allgemeinen Zuordnungssystems anwendbar.

Der Signaturschlüssel-Inhaber hat in dieser Situation zwei Interessen: Er möchte einerseits nicht mehr Daten preisgeben, als für die jeweilige Anwendung erforderlich sind, andererseits jedoch über ein Instrument verfügen, sich sicher in Online-Anwendungen ausweisen zu können. Im Grundsatz ist eine Art Attribut-Zertifikat damit der richtige Weg.

1900 Diese berechnen derzeit zertifikatsabhängige Entgelte. Allerdings verursacht die Zertifikatsvergabe kaum Kosten. Denkbar (und betriebswirtschaftlich sinnvoll) wäre es deshalb auch, bei einem einmaligen Registrierungsvorgang eine Vielzahl von Zertifikaten auszustellen und eine Gesamtgebühr zu erheben. In diesem Fall wäre ein Attribut-Zertifikat eine sinnvolle Alternative zu der im Folgenden vorgeschlagenen Lösung.

1901 S.o. 4.2.4.1.

1902 *Roßnagel*, DuD 2002, 281, 284; *Roßnagel/Gitter/Hornung*, in: Reichl/Roßnagel/Müller 2005, 240.

1903 BGBl. I, 1342.

1904 *Roßnagel*, DuD 2002, 281, 284.

Es hätte jedoch Kosten-[1905] und Sicherheitsvorteile, statt der bisher gebräuchlichen Attribut-Zertifikate gemäß § 7 Abs. 2 SigG eine staatlich signierte Datei einzusetzen. An dieser Stelle setzt die Idee des so genannten „elektronischen Ausweises" an. Dabei handelt es sich um den Personalausweis- oder Melderegisterdatensatz des Signaturschlüssel-Inhabers, der durch die Personalausweis- oder Meldebehörde qualifiziert signiert wird.

Hierbei sind unterschiedliche Konzepte denkbar. Eine Möglichkeit besteht darin, den Datensatz nur durch die Behörde signieren zu lassen. So würde der Bürger nur eine Chipkarte, nicht jedoch ein Schlüsselpaar nebst qualifiziertem Zertifikat benötigen. Wenn beispielsweise beim digitalen Personalausweis die Signaturfunktion auf freiwilliger Basis verwirklicht würde, könnte die Ausweisbehörde den elektronischen Ausweis dennoch standardmäßig auf der Karte speichern. Der Idee nach würde dieser sodann zur Authentisierung von der Karte durch ein offenes Netz zum Gegenüber übermittelt. Eine derartige Authentisierungslösung wäre nicht identisch mit der Client-Server-Authentisierung, die bei den momentanen Signaturkarten als Lösung mitgeliefert wird und ein separates Schlüsselpaar verwendet.[1906]

Diese Form der Verwendung des elektronischen Ausweises stößt allerdings auf eine Reihe von Schwierigkeiten.[1907] Zunächst müsste dieser in einem geschützten Bereich auf der Karte gespeichert werden, der vom Inhaber zur Übermittlung im Authentisierungsvorgang freigeschaltet werden würde. Andernfalls könnte jedermann die Daten des Ausweises (etwa nach einem Diebstahl der Karte) übermitteln. Wird der Schutz der Daten allerdings durch eine PIN bewerkstelligt, besteht das Problem, dass diese in der Mehrzahl der Fälle über einen langen Zeitraum unverwendet bliebe. Damit ergibt sich das Risiko des Vergessens oder Verlierens der PIN. Des Weiteren besteht eine Reihe gravierender Sicherheitsprobleme. Die Daten des so konzipierten elektronischen Ausweises könnten nämlich bei der Übertragung in offenen Netzen abgefangen, mitkopiert und danach von Dritten missbraucht werden. Selbst wenn dies durch starke Verschlüsselungen erschwert wird, besteht stets die Gefahr, dass der Empfänger des Datensatzes (oder eine Person, die bei diesem Zugriff auf die Daten hat oder sich verschafft) diesen weiterverwendet. Wenn diese Form der Authentisierung allgemeiner Standard würde, hätte eine Vielzahl von staatlichen und privaten Stellen den Ausweisdatensatz gespeichert. Eine Stelle, die den Datensatz empfinge, könnte sich deshalb auch bei einer Speicherung im geschützten Bereich der Karte nicht darüber sicher sein, dass die Daten im konkreten Fall wirklich vom Inhaber selbst übermittelt wurden. Diese Variante ist deshalb zu einer sicheren Authentisierung nicht geeignet.

Aus diesem Grund bietet sich eine andere Form der Konzeption an.[1908] Sie setzt voraus, dass der Karteninhaber bereits über ein qualifiziertes Zertifikat verfügt. Der Ausweis- oder Meldedatensatz wird zunächst vom Signaturschlüssel-Inhaber selbst signiert. Die Behörde signiert danach Datensatz und Signatur des Inhabers in einem einheitlichen Vorgang. Hierdurch werden beide amtlich miteinander verknüpft. Das Ergebnis dieses Vorgangs kann nun auf der Signaturkarte gespeichert werden und – ähnlich wie ein Attribut-Zertifikat – immer dann durch den Signaturschlüssel-Inhaber übermittelt werden, wenn die zusätzlichen Daten in der konkreten Situation benötigt werden.[1909]

1905 Das gilt nach der gegenwärtigen Entgeltstruktur, s.o. Fn. 1900.

1906 S. näher oben 2.3.2.

1907 S. schon *Roßnagel/Gitter/Hornung*, in: Reichl/Roßnagel/Müller 2005, 239 f.

1908 S. zum folgenden Konzept *Roßnagel*, DuD 2002, 281, 284 f.; *ders*. 2002, 52 f.; *Roßnagel/Gitter/Hornung*, in: Reichl/Roßnagel/Müller 2005, 240.

1909 Eine ähnliche Lösung wird auch in Österreich verfolgt, s. Bundesgesetz über Regelungen zur Erleichterung des elektronischen Verkehrs mit öffentlichen Stellen (E-Government-Gesetz – E-GovG), BGBl. I Nr. 10/2004. Eine eindeutige Identifikation wird dort durch eine Personenbindung erzeugt.

Auf Seiten des Empfängers der Daten läuft die Authentisierung folgendermaßen ab: Er erhält einen qualifiziert signierten Antrag (regelmäßig unter Einschluss des Zertifikats) und den so erstellten elektronischen Ausweis. Nach der üblichen Prüfung der Signatur des Antrags, der etwa auf Datenübermittlung gerichtet sein kann, wird zunächst die Signatur des elektronischen Ausweises geprüft, die dessen Inhaber erstellt hat. Dies erfolgt mittels des öffentlichen Schlüssels, der im Zertifikat angegeben ist und mit dem auch der Antrag geprüft wurde. Ist die zweite Prüfung erfolgreich, so ist gesichert, dass ein und dieselbe Person sowohl den Antrag als auch den elektronischen Ausweis signiert hat. Im dritten Schritt kann jetzt die Signatur der Behörde geprüft werden. Ist auch diese Prüfung erfolgreich, so steht fest, wer die Person des Antragstellers tatsächlich ist: Seine Identität ergibt sich aus den Daten des elektronischen Ausweises.

Dieser Vorgang ist zwar relativ kompliziert, er kann jedoch vollständig automatisiert werden.[1910] Im Ergebnis eröffnet sich deshalb die Möglichkeit einer sicheren Online-Authentisierung ohne großen Kostenaufwand auf Seiten des hoheitlichen oder privaten Erklärungsempfängers. Gleichzeitig bleibt jedoch dem Karteninhaber die Option erhalten, ohne Übersenden des elektronischen Ausweises weiterhin unter einem Zertifikats-Pseudonym zu handeln oder zwar seinen Namen, nicht jedoch die weiteren Daten des elektronischen Ausweises preiszugeben.

Das System des elektronischen Ausweises ist nicht notwendig an einen digitalen Personalausweis mit Signaturfunktion gekoppelt. Denkbar ist auch, dass der Karteninhaber sich mit einer anderen signaturfähigen Karte in der Behörde seinen elektronischen Ausweis ausstellen lässt. Eine Umsetzung über den digitalen Personalausweis hat allerdings verfahrenstechnische Vorteile, weil der elektronische Ausweis bei der Aushändigung des Personalausweises ausgestellt werden kann.[1911] In diesem Fall verfügt der Inhaber noch nicht über eine sichere Signaturerstellungseinheit und ein qualifiziertes Zertifikat, sondern erhält beides zusammen mit dem elektronischen Ausweis. Die eigene Signatur des Ausweisinhabers würde gleichzeitig Testzwecken dienen und damit die Anforderung aus § 5 Abs. 6 SigG erfüllen. Überdies ist es nach § 1 Abs. 4 Satz 3 PersAuswG bereits zulässig, den Datensatz des Personalausweises auf dem Chip zu speichern.

5.2.2 Das Zusammenwirken unterschiedlicher Instanzen

Chipkartenausweise wie der digitale Personalausweis und die elektronische Gesundheitskarte können eine Alternative zu eigenen sicheren Signaturerstellungseinheiten der Zertifizierungsdiensteanbieter sein. Beide Karten haben den Vorteil eines hohen Verbreitungsgrads und eröffnen die Möglichkeit für die Anbieter, auf ein bestehendes Infrastrukturnetz zurückgreifen zu können, das zur Ausgabe des jeweiligen Ausweises bereits besteht. Zwar ist seit Anfang des Jahres 2005 auch eine Ausgabe ohne direkten Kontakt mit dem Signaturschlüssel-Inhaber möglich.[1912] Die persönliche Antragstellung und Übergabe

---

Diese ist eine behördlich signierte Bestätigung, dass ein bestimmter Karteninhaber einer bestimmten „Stammzahl“ zugeordnet wird. Diese Zahl wiederum wird aus der ZMR-Zahl (Ordnungsnummer des Zentralen Melderegisters) abgeleitet. Im Ergebnis arbeitet dieses Modell zwar mit einem Register; die Vertrauenswürdigkeit entspringt aber wie hier der Signatur der Behörde. Der elektronische Ausweis kommt jedoch im Unterschied zum österreichischen Konzept ohne eine zentrale Datenbank aus und stellt deshalb einen geringeren Eingriff in das Grundrecht auf informationelle Selbstbestimmung dar, s. *Roßnagel/Gitter/Hornung*, in: Reichl/Roßnagel/Müller 2005, 240.

1910 *Roßnagel*, DuD 2002, 281, 285.

1911 S. *Roßnagel/Gitter/Hornung/Strasser*, in: Reichl/Roßnagel/Müller 2005, 319 ff.

1912 S.o. 5.1.2; *Roßnagel*, NJW 2005, 385 ff.

hat jedoch enorme Vorteile für den Rechtsverkehr, weil das Vertrauen in die Authentizität der signierten Erklärung gesteigert wird.[1913]

§ 4 Abs. 5 SigG erlaubt dem Zertifizierungsdiensteanbieter, unter Einbeziehung in sein Sicherheitskonzept nach § 4 Abs. 2 Satz 4 SigG Aufgaben nach dem Signaturgesetz und der Signaturverordnung an Dritte zu übertragen.[1914] Der nähere Inhalt des Sicherheitskonzepts ist durch § 2 SigV vorgeschrieben.[1915] Bei akkreditierten Anbietern bestimmt § 15 Abs. 2 SigG, dass sich die erstmalige und laufende Kontrolle der Prüf- und Bestätigungsstelle nach § 18 SigG auch auf den Dritten zu erstrecken hat. Weitere Regelungen zur Zulässigkeit der Übertragung enthält das Signaturrecht nicht. Damit ist jede Form der Aufgabenteilung zwischen Anbieter und Dritten denkbar, bis hin zu „virtuellen" Zertifizierungsdiensteanbietern, die die bestehende Infrastruktur anderer Anbieter nutzen und durch diese Zertifikate im Namen des „virtuellen" Anbieters ausstellen lassen.

Wenn der Zertifizierungsdiensteanbieter Aufgaben auf Dritte überträgt, so greifen allerdings spezielle Haftungsregelungen.[1916] Für den Fall der Verletzung von Anforderungen des Signaturgesetzes und der Signaturverordnung oder des Versagens von Produktion oder technischen Sicherungseinrichtungen haftet der Anbieter nach § 11 Abs. 1 Satz 1 SigG auf den erlittenen Schaden gegenüber jedem, der auf die Angaben in einem qualifizierten Zertifikat, einem qualifizierten Zeitstempel oder einer Zertifikatsabfrage vertraut hat. Es handelt sich um eine Verschuldenshaftung, bei der der Anbieter sein fehlendes Verschulden nach § 11 Abs. 2 SigG zu beweisen hat. § 11 Abs. 4 SigG bestimmt, dass der Zertifizierungsdiensteanbieter für beauftragte Dritte wie für eigenes Handeln haftet.[1917] Die Exkulpationsmöglichkeit nach § 831 BGB ist ausdrücklich ausgeschlossen. Gegenüber dem Signaturschlüssel-Inhaber, der Vertragspartner des Anbieters ist, besteht eine Haftung über die Zurechnungsnorm des § 278 Satz 1 BGB. In beiden Fällen tritt keine Haftung ein, wenn der Anbieter nachweisen kann, dass der Dritte nicht schuldhaft gehandelt hat. Um die Sicherheit des Rechtsverkehrs zu gewährleisten, der auf das Handeln mittels der elektronischen Signatur vertraut, sind hohe Anforderungen an die Sorgfaltspflichten zu stellen.[1918]

Beim digitalen Personalausweis ist es danach für die Personalausweisbehörde signaturrechtlich[1919] zulässig, Aufgaben nach dem Signaturgesetz zu übernehmen.[1920] Hierzu gibt es bereits erste Pilotprojekte, etwa in Saarbrücken[1921] und Bremen.[1922] In Rheinland-Pfalz

---

1913 S. *Roßnagel*, NJW 2005, 385, 388 und weiter unten in diesem Abschnitt.

1914 S. BT-Drs. 14/4662, 20; *v. Harnier* 2000, 99 ff.; Hoeren/Sieber-*Brisch/Brisch*, Kap. 13.3, Rn. 179 ff.; zu den zulässigen Kooperationsformen beim Personalausweis vgl. *Roßnagel/Gitter*, in: Reichl/Roßnagel/Müller 2005, 97 ff.; 219 ff.; s.a. *Gitter/Strasser*, DuD 2005, 74, 75 f.

1915 Vgl. *Roßnagel*, BB 2002, 261; RMD-*Roßnagel/Hammer*, § 2 SigV Rn. 1 ff.

1916 Vgl. ausführlich *Thomale* 2003; zum europarechtlichen Hintergrund *Balboni*, Information & Communications Technology Law 2004, 211 ff.; zur Anwendung auf den digitalen Personalausweis *Roßnagel/Gitter*, in: Reichl/Roßnagel/Müller 2005, 152 ff.; *Gitter/Strasser*, DuD 2005, 74, 75 f.

1917 S. näher *Thomale* 2003, 197 ff.; ferner *ders*., MMR 2004, 80, 83 ff.; *Blum*, DuD 2001, 71, 75 ff.

1918 S. die Gesetzesbegründung (BT-Drs. 14/4662, 25) und *Roßnagel*, NJW 2001, 1817, 1823.

1919 Zur Frage der datenschutzrechtlichen Zulässigkeit von Datenübermittlungen s.o. 4.3.6.

1920 Auch nach der Gesetzesbegründung (BT-Drs. 14/4662, 20, s.a. *Thomale* 2003, 197) können Behörden Teilaufgaben eines Zertifizierungsdiensteanbieters übernehmen. Die denkbare Variante einer vollständigen Übernahme der Zertifizierungsdienste durch den Staat oder einen staatlichen Monopolisten ist zwar rechtlich zulässig (s. *Bundesministerium für Wirtschaft und Arbeit/Hans-Bredow-Institut* 2003, 20) und wird auch im Ausland überwiegend verfolgt (vgl. oben 3). Sie ist in Deutschland aufgrund der Grundentscheidung des Gesetzgebers für den privaten Wettbewerb zwischen Zertifizierungsdiensteanbietern aber nicht realistisch und wird deshalb hier nicht weiter betrachtet.

1921 S. *Schiff*, der städtetag 6/2002, 20 f.

1922 Auskunft von Herrn Dr. *Pelz* vom 1.9.2003.

nehmen seit dem 1. Januar 2005 212 Personalausweisbehörden die Registrierungsaufgaben für einen Zertifizierungsdiensteanbieter vor.[1923] Auch die Krankenkassen können bei der elektronischen Gesundheitskarte mit den Anbietern kooperieren. Gleiches gilt für die Berufskammern der Leistungserbringer. Es sind unterschiedliche Umsetzungsmodelle denkbar, wobei es sich anbietet, diejenigen Aufgaben auf die Behörde, Krankenkasse oder Kammer zu übertragen, die nach alter Rechtslage einen direkten Kontakt mit dem Ausweisinhaber erforderten.[1924] Dies sind die Registrierung, eine eventuelle Entgegennahme von Nachweisen über Attribute, die Aushändigung der Karte und des PIN-Briefs und die Unterrichtung. Diese Prozesse können zwar seit dem 11. Januar 2005 auch ohne persönlichen Kontakt abgewickelt werden. Ein solcher Kontakt erhöht jedoch die Sicherheit, dass die Karte tatsächlich dem Signaturschlüssel-Inhaber zugeordnet wird.

Im Grundsatz macht es keinen Unterschied, welche Stelle als Dritter fungiert. Die Personalausweisbehörde erscheint jedoch aus tatsächlichen und rechtlichen Gründen als besonders geeignet.[1925] Sie könnte einerseits die Aushändigung der sicheren Signaturerstellungseinheit mit dem Ausstellen des „elektronischen Ausweises“ verbinden,[1926] andererseits die Prozesse der Identifizierung und Prüfung von Nachweisen sicherer durchführen als andere Stellen. Soweit es sich bei diesen Nachweisen um amtliche Dokumente handelt, werden sie im normalen Geschäft der Behörde täglich in großer Zahl geprüft, sodass auf entsprechende Routine und Erfahrung zurückgegriffen werden könnte.

Derselbe faktische Vorteil besteht auch im Rahmen der Identifizierung. Hinzu kommt aus rechtlicher Perspektive, dass der Personalausweisbehörde durch die Ausführungsgesetze der Länder zum Personalausweisgesetz besondere Befugnisse zur Identifizierung eines Antragstellers zustehen. Sie darf danach regelmäßig weitere Erkundigungen einholen, Gegenüberstellungen vornehmen und als letztes Mittel sogar eine erkennungsdienstliche Behandlung anordnen.[1927] Diese Befugnisse gewährleisten ein deutlich höheres Maß an Identifizierungssicherheit als die Möglichkeiten der Zertifizierungsdiensteanbieter nach § 3 Abs. 1 SigV. Überdies besteht ein direkter Kontakt zum Antragsteller, während die überwiegende Zahl der Anbieter zur Identifizierung bislang auf das Postident-Verfahren zurückgreift. Dabei wird die Identifizierung durch einen Bediensteten der Deutschen Post AG am Wohnsitz oder in einer Filiale vorgenommen.[1928] Sollten in Zukunft Banken auf der Basis ihrer bereits erhobenen Kontodaten Signaturkarten in einem reinen Online-Verfahren ausgeben, würde die Identifizierungssicherheit weiter reduziert.[1929]

Für den Einsatz der elektronischen Signatur ist eine sichere Identifizierung jedoch unabdingbar, weil sich ein Erklärungsempfänger darauf verlassen muss, dass die Signatur tatsächlich von demjenigen erstellt wurde, der im Zertifikat als Schlüsselinhaber angege-

---

1923 S. näher http://www.signatur.rlp.de. Es erfolgt eine Zusammenarbeit mit nur einem Anbieter (T-Systems).

1924 Vgl. für die Zusammenarbeit zwischen Personalausweisbehörden und Zertifizierungsdiensteanbieter beim digitalen Personalausweis *Strasser/Müller/Roßnagel/Gitter*, in: Reichl/Roßnagel/Müller 2005, 260 ff., 268 ff.; näher unten 6.2.4.2; s.a. *Gitter/Strasser*, DuD 2005, 74, 75 f.

1925 S. *Roßnagel/Gitter/Hornung/Strasser*, in: Reichl/Roßnagel/Müller 2005, 319 ff. Weitere Besonderheiten bei einem Tätigwerden der Behörde (wie etwa mögliche Amtshaftungsansprüche im Fall von schuldhaften Pflichtverletzungen) bleiben im Folgenden unberücksichtigt; s. ausführlich *Roßnagel/Gitter*, ebd., 152 ff.; s.a. *Gitter/Strasser*, DuD 2005, 74, 75 f.

1926 S.o. 5.2.1.2.

1927 S. bspw. § 4 Abs. 5 LPersAuswG Rh.-Pf., § 4 Abs. 5 LPersAuswG Bln, § 5 Abs. 4 LPersAuswG Hess.

1928 Vgl. http://www.deutschepost.de/dpag?xmlFile=872.

1929 Vgl. dazu *Roßnagel*, NJW 2005, 385, 388; zur Sicht der Banken *Büger/Esslinger/Koy*, DuD 2004, 133 ff.; s.a. *Bergfelder*, CR 2005, 148 ff.

ben ist. Jeder Gewinn an Identifikationssicherheit stellt deshalb unmittelbar einen Zugewinn an Rechtssicherheit dar. Eine Registrierung durch die Personalausweisbehörde könnte ein Mittel zur flächendeckenden Verbreitung von Signaturverfahren sein, ohne auf eine persönliche Identifizierung im Rahmen der Beantragung der Signaturkarte zu verzichten. Diese Tätigkeit der Behörden ließe sich mit der Ausgabe eines digitalen Personalausweises verbinden, dies ist jedoch nicht zwingend. Ebenso denkbar ist ein Modell, in dem die Behörden Identifizierungsdienstleistungen im Rahmen der Ausgabe eigener Karten der Zertifizierungsdiensteanbieter übernehmen. Dies hat allerdings den Nachteil, dass dann nicht mehr auf die erweiterten Identifizierungsbefugnisse des Personalausweisrechts zurückgegriffen werden kann. Es verbleibt der Vorteil der Kompetenz der Behörde im Bereich der Identifizierung, die eine ihrer Hauptaufgaben im täglichen Betrieb ist.

In beiden Fällen ist bereits unter datenschutzrechtlichen Gesichtspunkten eine gesetzliche Regelung für die Übermittlung von Daten von der Behörde zum Zertifizierungsdiensteanbieter erforderlich.[1930] Dies wird durch die signaturrechtliche Perspektive bestätigt, weil es – selbst bei einer Verwendung standardisierter Vertragsklauseln – kaum vorstellbar ist, dass die verschiedenen Zertifizierungsdiensteanbieter mit den Trägern der Personalausweisbehörden einzelne Verträge abschließen. Sinnvoll wäre es deshalb, per Gesetz die Verbreitung qualifizierter Signaturverfahren durch die Personalausweisbehörden als Infrastrukturaufgaben zu regeln.[1931] Wird diese Dienstleistung allen Zertifizierungsdiensteanbietern gleichermaßen und gegen ein angemessenes Entgelt angeboten, so ist weder die Dienstleistungsfreiheit nach Art. 50 EGV verletzt, noch bestehen wettbewerbs- oder beihilferechtlichen Probleme.[1932]

Auch bei der Ausgabe des elektronischen Heilberufsausweises ist ein Modell denkbar, in dem die Landesärztekammern – ähnlich wie die Personalausweisbehörden – die Antragsbearbeitung, Registrierung, Identifizierung und Attributsbestätigung übernehmen und dann mit einem oder mehreren Zertifizierungsdiensteanbietern zusammenarbeiten.[1933] Das GKV-Modernisierungsgesetz selbst enthält für den elektronischen Heilberufsausweis lediglich Verwendungsbestimmungen. Nach § 291a Abs. 5 Satz 3 SGB V ist er als Zugriffsinstrument auf die Daten des elektronischen Rezepts und der freiwilligen Anwendungen der elektronischen Gesundheitskarte erforderlich. Außerdem muss er im Echtbetrieb[1934] in der Lage sein, qualifizierte elektronische Signaturen zu erzeugen.[1935] Es finden sich jedoch keine Aussagen über das Ausgabeverfahren und sonstige Funktionen im Gesetz; § 291a Abs. 5a SGB V n.F. überträgt die Regelungskompetenz hierfür auf die Bundesländer. Wenn kammergebundene Berufe betroffen sind, kann die Ausgestaltung und Funktion des Heilberufsausweises an sich auch durch die Satzungen der Kammern geregelt werden. Hierzu ist eine einheitliche Vorgabe, beispielsweise durch die Bundeskammern, erforderlich, weil andernfalls die im Gesundheitswesen unabdingbare Interoperabilität nicht gewährleistet wäre. Dies wiederum setzt voraus, dass zunächst durch die Gesellschaft

1930 S.o. 4.3.6.2.2.2.

1931 S. *Roßnagel/Gitter*, in: Reichl/Roßnagel/Müller 2005, 157 ff.

1932 S. näher *Roßnagel/Gitter*, in: Reichl/Roßnagel/Müller 2005, 160 ff.

1933 Vgl. ausführlich *Secartis/Secunet* 2004; s.a. *Brenner* 2004, 224 ff.; *Grätzel v. Grätz* 2004c, 128 f.

1934 Im Rahmen von Feldversuchen kann das BMGS im Einvernehmen mit dem Bundesbeauftragten für den Datenschutz gemäß § 291a Abs. 9 SGB V befristete Ausnahmen vom Erfordernis der qualifizierten Signatur für die Dauer von bis zu sechs Monaten zulassen.

1935 Das ist zum einen zur sicheren Identifizierung, zum anderen zur Erfüllung von Formvorschriften im Rahmen des ärztlichen Schriftverkehrs, der Dokumentation und Protokollierung erforderlich. Neben dem Zugriff auf die elektronische Gesundheitskarte wird der Heilberufsausweis als Sichtausweis, zur Signatur und Authentisierung (bspw. bei der Anmeldung zum Praxiscomputer) Verwendung finden, s. *BITKOM/VDAP/VHitG/ZVEI* 2003, 54, 57; s.a. *Warda/Noelle* 2002, 91 ff.

für Telematik die Informations-, Kommunikations- und Sicherheitsinfrastruktur („Telematikinfrastruktur“) nach § 291a Abs. 7 Satz 1 SGB V verabschiedet wird, die durch die Satzungen strikt eingehalten werden muss.

Bei der Zusammenarbeit zwischen den ausgebenden Berufskammern und den Zertifizierungsdiensteanbietern könnten erstere selbst als reale oder virtuelle Anbieter auftreten.[1936] Die Heilberufsgesetze der Bundesländer weisen den Landesärztekammern schon heute die Aufgabe der Ausstellung von Bescheinigungen über die Arzteigenschaft zu. Nach einigen dieser Gesetze beinhaltet dies bereits jetzt, für die Ärzte Zertifikate oder Attribut-Zertifikate auszugeben.[1937] Entsprechend könnte die Ausgabe des elektronischen Heilberufsausweises als gesetzliche Pflicht der Landesärztekammern normiert werden.[1938] Die Kammern könnten sich jedoch auch auf die Ausstellung der nach § 5 Abs. 2 Satz 2 SigG erforderlichen Nachweise über die Berufszugehörigkeit beschränken und in einem Kooperationsmodell mit einem oder mehreren Zertifizierungsdiensteanbietern zusammenarbeiten.[1939] Für nicht kammergebundene Berufe wie Hebammen und Krankengymnasten ist allerdings auf jeden Fall eine alternative Organisation erforderlich.[1940] Diskutiert wird auch, inwieweit weitere Berufsgruppen (insbesondere Pflegeberufe)[1941] ebenfalls einen Heilberufsausweis erhalten sollten. Die Ärztekammern haben angekündigt, die Ausweise bundesweit gemeinsam auszugeben[1942] und die im Januar des Jahres 2005 geschaffene Möglichkeit zu nutzen, die Antragsdaten im Online-Verfahren zu übermitteln.[1943]

5.2.3 Der kombinierte Einsatz mehrerer Karten

Der Einsatz qualifizierter Signaturverfahren ist dazu geeignet, handelnde Personen sicher zu identifizieren. Gleichzeitig ist es auch möglich, die Zugehörigkeit zu einer Gruppe von Personen festzustellen. Hierzu können entweder Hauptzertifikate mit Attribut (§ 7 Abs. 1 Nr. 1 SigG) oder Attribut-Zertifikate (§ 7 Abs. 2 SigG) verwendet werden. In ihnen können nach § 5 Abs. 2 Satz 1 SigG insbesondere berufsbezogene Angaben enthalten sein, sodass sie als Sicherungsmittel einsetzbar sind, wenn der Zugriff auf bestimmte Daten nur bestimmten Berufsgruppen eröffnet sein soll. Bei einer Reihe von Anwendungen geht es zusätzlich darum, dem Betroffenen die Möglichkeit zu verschaffen, selbst darüber zu entscheiden, wem er bestimmte Daten zukommen lassen möchte. In diesem Fall bieten sich Systeme an, die einen Zugriff nur mit einer individuellen Chipkarte des Betroffenen und einer beliebigen Karte eines Inhabers eines Attribut-Zertifikats zulassen.

Die Umsetzung kann unterschiedlich realisiert werden. Nach dem Konzept des Job-Card-Verfahrens signiert der Antragsteller in der Arbeitsagentur einen Antrag auf Daten-

---

1936 S. zu den unterschiedlichen Umsetzungsvarianten (vor der Änderung des Signaturgesetzes) *Secartis/Secunet* 2004, Teil II, 31 ff.; zusammenfassend zu den wahrscheinlichen Kosten ebd., 88. Danach ergeben sich je nach Modell jährliche Gebühren pro Heilberufsausweis von 27,72 bis 45,67 Euro.

1937 Z.B. § 5 Abs. 1 Nr. 7 HeilberufsG Hess., § 6 Abs. 1 Satz 1 Nr. 12 HeilberufsG NW, § 2 Abs. 1 Nr. 11 HeilberufsG Bbg; s. näher *Dierks/Nitz/Grau* 2003, 146 f.; *Secartis/Secunet* 2004, Teil I, 13.

1938 Entsprechende Gesetzesänderungen waren Ende 2004 in Arbeit, s. *TeleTrusT* 2004, Anhang B, 2; *Secartis*/*Secunet* 2004, Teil I, 13.

1939 *Brenner* 2004, 223 ff.; *Secartis/Secunet* 2004, 31 ff.

1940 *Goetz*, DÄ 2003, A756, 759.

1941 http://www.heise.de/newsticker/meldung/58391; http://www.aerztezeitung.de/docs/2005/04/15/068a1301.asp?cat=/computer/telemedizin.

1942 S.a. *Secartis/Secunet* 2004, 49 ff. Diese Vorgehensweise ist auch am wirtschaftlichsten, s. ebd., 99 ff. Sie wird durch § 291a Abs. 5a Satz 2 SGB V ausdrücklich zugelassen.

1943 S. *Krüger-Brand*, DÄ 2005, A 14.

übermittlung.[1944] Zuvor oder danach signiert auch der Mitarbeiter der Arbeitsagentur – der über ein entsprechendes Attribut-Zertifikat verfügt, welches ihn als solchen ausweist – den Antrag. In der Zentralen Speicherstelle wird anhand der Zertifikatsnummer des Antragstellers dessen Sozialversicherungsnummer ermittelt. Mit dieser werden die Daten aus dem Datenbestand abgerufen, zuvor wird jedoch die Signatur des Mitarbeiters einschließlich seines Attribut-Zertifikats geprüft. Mit letzterem wird nachgewiesen, dass die Daten von der berechtigten Arbeitsagentur angefragt werden. Anhand der eindeutigen Zertifikatsnummer kann überdies die genaue Identität des abrufenden Mitarbeiters festgestellt und so der Zugriff auch innerhalb der Arbeitsagentur auf einzelne Mitarbeiter (den zuständigen Sachbearbeiter und eventuelle Vertreter) beschränkt werden. Wird eine Protokollierungsfunktion eingerichtet, so erlaubt das Zertifikat des Mitarbeiters eine genaue Rückverfolgbarkeit der jeweiligen Zugriffe.

Eine weitere Möglichkeit besteht darin, den Zugriff auf die Daten, die auf einer Karte selbst gespeichert sind, nur unter Verwendung einer anderen Karte zuzulassen. Diese Variante findet sich im Verhältnis zwischen elektronischer Gesundheitskarte und elektronischem Heilberufsausweis. Die Mitwirkung des Versicherten wird bei den verschiedenen Applikationen der elektronischen Gesundheitskarte unterschiedlich umgesetzt.[1945] Beim elektronischen Rezept besteht der Schutz im Besitz der Karte, bei den freiwilligen Anwendungen ist mit Ausnahme der Notfalldaten eine PIN-Eingabe erforderlich. Durch beide Verfahren wird – wenn auch mit unterschiedlichen Sicherheitsrisiken – die Teilnahme des Versicherten geprüft. In einem zweiten Schritt findet sodann die Überprüfung der Berechtigung des zugreifenden Leistungserbringers statt. Dieser muss seinen elektronischen Heilberufsausweis ebenfalls mittels einer PIN freischalten. Dann erfolgt eine gegenseitige Authentisierung zwischen den beiden Karten. Erst danach wird der Zugriff auf die Daten der elektronischen Gesundheitskarte freigegeben, wobei es sich hierbei um vollständige Daten oder um Verweise (Pointer) auf Daten handeln kann, die in der Peripherie gespeichert sind.[1946]

Zu beachten ist, dass die elektronische Gesundheitskarte in diesem System keine Zertifikatsabfrage durchführt. Im Rahmen der gegenseitigen Authentisierung prüft die Gesundheitskarte die Rolleninformation des Attribut-Zertifikats auf dem elektronischen Heilberufsausweis. Um sicherzugehen, dass dieses Zertifikat (beispielsweise bei Verlust des Heilberufsausweises oder Abhandenkommen der PIN) noch gültig ist, müsste die Gesundheitskarte selbst darüber hinaus eine Abfrage beim Zertifizierungsdiensteanbieter durchführen (OCSP-Abfrage). Dies ist jedoch aufgrund der zu geringen Speicher- und Verarbeitungskapazitäten nicht möglich. Eine Sicherung der Gültigkeit des elektronischen Heilberufsausweises kann damit nur auf der Applikations-Ebene erfolgen.

5.2.4 Institutionskarten

Die Konzepte für den Einsatz von Telematik im Gesundheitswesen sehen vor, dass jede Institution, in der Leistungserbringer des Gesundheitswesens tätig sind, mit einer Institutionskarte ausgestattet wird.[1947] Die Version 2.0 der Spezifikation für den elektronischen Heilberufsausweis normiert hierzu eine Security Module Card (SMC).[1948] Dabei handelt es

1944 S. *Hornung/Roßnagel*, K&R 2004, 263, 264 f. und oben 4.2.4.1.
1945 S. ausführlich oben 4.2.3.4.2, dort auch zur Frage, in welchem Umfang das hier beschriebene System rechtmäßig eingesetzt werden darf.
1946 Zur näheren Umsetzung s.u. 6.3.3.1.
1947 *BITKOM/VDAP/VHitG/ZVEI* 2003, 27.
1948 S. *Struif* (Hrsg.) 2003, 24 ff.

sich um eine Chipkarte mit den normalen Funktionalitäten der elektronischen Signatur, Verschlüsselung und Authentifizierung. Das Schlüsselzertifikat enthält jedoch nicht den Namen einer natürlichen Person, sondern den einer Institution, beispielsweise eines Krankenhauses. Damit wird ein verschlüsselter Datenversand ermöglicht, der nicht an eine bestimmte Person, sondern an diese Institution gerichtet ist. Unabhängig von etwaigen Wechseln in den dortigen Beschäftigungsverhältnissen können alle Personen, die die Institutionskarte freischalten können (also etwa über die PIN verfügen), die Daten entschlüsseln. Gleiches gilt auch für das Versenden von Daten. Ein Beispiel hierfür ist das DIGANT-Verfahren der Bundesdruckerei GmbH,[1949] bei dem die Personalausweisbehörden eine Signaturkarte für den verschlüsselten Datenversand erhalten, die nicht auf einen Mitarbeiter ausgestellt ist. Auch im Rahmen der internen verschlüsselten Archivierung von Daten können mehrere Beschäftigte dieselbe Karte zum Ver- und Entschlüsseln nutzen.[1950] Daneben lässt sich mit Hilfe von Institutionskarten die Delegation von Befugnissen umsetzen.[1951] Schließlich werden Verfahren der automatisiert erzeugten elektronischen Signatur erleichtert.[1952]

Für die rechtliche Bewertung von Institutionskarten ist zwischen der signaturrechtlichen und der datenschutzrechtlichen Perspektive zu differenzieren. Erstere betrifft die rechtliche Einordnung der von Institutionskarten erstellten Signaturen, letztere die Zulässigkeit des Einsatzes der Karten zum verschlüsselten Empfang und zum Abruf von Daten.

Bei den von Institutionskarten erstellten Signaturen müssen wiederum zwei Fälle unterschieden werden. Möglich ist es, dass eine natürliche Person sich ein qualifiziertes Zertifikat auf ein Pseudonym ausstellen lässt, das mit dem Namen der Institution identisch ist.[1953] In aller Regel wird es sich dabei um die Person handeln, die für die Institution zeichnungsberechtigt ist. Mit solchen Signaturkarten können Arbeitsabläufe organisiert werden, etwa durch die Weitergabe von Karte und PIN an Mitarbeiter und die Ausgabe mehrerer Karten. Durch interne Haftungsfreistellungen kann die natürliche Person, für die die qualifizierten Zertifikate ausgestellt werden, von der Verantwortung entlastet werden. Mit dieser Methode ist es möglich, mit Institutionskarten qualifizierte elektronische Signaturen zu erstellen.

Anders ist die Rechtslage dann, wenn das Zertifikat für die Institution selbst ausgegeben wird. In diesem Fall kann die Institutionskarte dieselbe technische Sicherheit aufweisen wie Signaturkarten, die mit qualifizierten Signaturverfahren arbeiten. Die Institutionszertifikate sind jedoch keine qualifizierten Zertifikate im Sinne des Signaturrechts. Nach § 2 Nr. 7 SigG können diese nämlich nur für natürliche Personen ausgestellt werden. Signaturen, die von Institutionskarten erstellt werden, sind auch keine fortgeschrittenen elektronischen Signaturen, da diese nach § 2 Nr. 2 a) SigG ausschließlich dem Signaturschlüssel-Inhaber zugeordnet sein müssen, und es sich hierbei gemäß § 2 Nr. 9 SigG um eine natürliche Person handeln muss.[1954] Aus signaturrechtlicher Sicht erzeugt diese zweite Gruppe von Institutionskarten damit einfache elektronische Signaturen nach § 2 Nr. 1 SigG.

Dies ist allerdings unschädlich, weil die Funktion dieser Karten nicht darin liegt, die Rechtsfolgen einer qualifizierten Signatur herbeizuführen, sondern Datenzugriffe innerhalb einer Institution zu organisieren und Verantwortlichkeit und Haftung derselben anstelle

1949 S. http://www.bundesdruckerei.de/de/behoerde/3_1/index.html; *Yildirim* 2004, 25 f.
1950 *BITKOM/VDAP/VHitG/ZVEI* 2003, 48.
1951 S.a. *Bertsch/Fleisch/Michels*, DuD 2002, 69, 71.
1952 Dazu allgemein *Roßnagel/Fischer-Dieskau*, MMR 2004, 133 ff.
1953 Die Begründung zu § 3a Abs. 3 VwVfG nennt die Möglichkeit, ein qualifiziertes Zertifikat ohne Nennung des Bearbeiters auf „Stadt München, Dezernat Jugend" auszustellen, s. BT-Drs. 14/9000, 31; näher *Roßnagel*, NVwZ 2003, 469, 472.
1954 S.a. *Roßnagel/Fischer-Dieskau*, MMR 2004, 133, 134 f.

eines konkreten Mitarbeiters zu begründen. Je nach Art der Anwendung kann dies sinnvoll oder sogar erforderlich sein.

Der Einsatz von Institutionskarten ist jedoch immer dann datenschutzrechtlich unzulässig, wenn Zugriffe auf Daten nur durch eine bestimmte Person erfolgen dürfen oder im Nachhinein genau ermittelbar sein muss, wer Daten gespeichert, verändert und abgerufen hat. Gerade für das Gesundheitswesen folgt daraus, dass in den allermeisten Fällen individualisierte Karten einzusetzen sind.

5.2.5 Probleme unterschiedlicher Gültigkeitszeiträume

Die Gültigkeit des Ausweiskörpers im Rahmen der Sichtkontrolle, die Gültigkeit der kryptographischen Eignung der Algorithmen der Signatur- und Hash-Verfahren und die Gültigkeitsdauer eines qualifizierten Zertifikats sind im Grundsatz voneinander unabhängig.[1955] Dies kann dazu führen, dass Beginn und Ende der einzelnen Gültigkeitszeiträume auseinander fallen.

Der Personalausweis wird nach § 2 Abs. 1 PersAuswG bislang für eine Dauer von zehn Jahren ausgestellt. Bei Personen, die das 26. Lebensjahr noch nicht vollendet haben, beträgt die Dauer fünf Jahre.[1956] Eine Verlängerung ist unzulässig. Die bisherige Krankenversichertenkarte hat keine gesetzlich geregelte Gültigkeitsdauer. Auch die Europäische Kommission macht hierzu keine Vorgaben, sondern will die Regelung der Dauer den Mitgliedstaaten überlassen.[1957] Gemäß § 291 Abs. 1 Satz 6 SGB V kann die Krankenkasse jedoch die Gültigkeit der Krankenversichertenkarte befristen. Von dieser Möglichkeit wird in der Praxis durchweg Gebrauch gemacht. Auch bei Ende der Mitgliedschaft ist die Karte zurückzugeben (§ 291 Abs. 4 SGB). Hiervon kann in Zukunft nach § 291 Abs. 4 Satz 2 SGB V abgewichen werden, wenn sich die Krankenkassen auf eine Weiternutzung der elektronischen Gesundheitskarte bei Kassenwechsel einigen.

Die Algorithmen und Parameter, die zur Erzeugung von Signaturschlüsseln, zum Hashen zu signierender Daten oder zur Erzeugung und Prüfung qualifizierter elektronischer Signaturen verwendet werden, sind immer nur für einen gewissen Zeitraum hinreichend sicher und damit als geeignet anzusehen. Nach Nr. I 2. der Anlage 1 zur Signaturverordnung wird dieser Zeitraum nach Angaben des Bundesamtes für Sicherheit in der Informationstechnik unter Beteiligung von Experten festgestellt und von der Regulierungsbehörde im Bundesanzeiger veröffentlicht. Er soll mindestens sechs Jahre betragen und wird jährlich neu bestimmt. Aufgrund des nicht exakt prognostizierbaren technischen Fortschritts handelt es sich bei dem Zeitraum der Eignung der Algorithmen und Parameter um eine variable Größe. Sofern sich die technischen Weiterentwicklungen auf die Rechenleistung beschränken, stellt dies kein grundsätzliches Problem dar. Hierdurch wird zwar der Zeitraum verkürzt, der für einen Angriff durch schlichtes Ausprobieren (Brute-Force-Attack) benötigt wird. Diese Verkürzung kann jedoch zumindest ungefähr abgeschätzt werden. Sofern dagegen das dem Algorithmus zugrundeliegende mathematische Problem gelöst wird, ist das Verfahren unmittelbar nicht mehr zur Signaturerzeugung geeignet.

Die Gültigkeitsdauer eines qualifizierten Zertifikats darf nach § 14 Abs. 3 Satz 1 SigV höchstens fünf Jahre betragen. Allerdings besteht die Möglichkeit, mittels Sperrung des

---

1955 Zur Abhängigkeit der Gültigkeit des Zertifikats von der der Eignung der Algorithmen s. weiter unten in diesem Abschnitt; vgl. zum Problem der verschiedenen Gültigkeitszeiträume von Personalausweisen und Zertifikaten *Roßnagel/Gitter*, in: Reichl/Roßnagel/Müller 2005, 100 f.; 221 f.

1956 Die Sonderfall des § 2 Abs. 1a PersAuswG (Beschränkung bis zur Vollendung des 23. Lebensjahres im Fall der doppelten Staatsangehörigkeit nach § 29 StAG) bleibt im Folgenden außer Betracht.

1957 S. *Europäische Kommission*, KOM(2003) 73, 10.

Zertifikats seine Gültigkeit jederzeit abrupt zu beenden. Der Zertifizierungsdiensteanbieter hat nach § 8 Abs. 1 Satz 1 SigG das Zertifikat auf Verlangen des Signaturschlüssel-Inhabers[1958] oder dessen Vertreters sowie dann zu sperren, wenn es aufgrund falscher Angaben ausgestellt wurde, der Anbieter seine Tätigkeit beendet und diese nicht von einem anderen Anbieter fortgeführt wird, ein vertraglich vereinbarter Sperrgrund eintritt oder wenn die zuständige Behörde dies anordnet.

Die in § 14 Abs. 3 Satz 1 SigV genannte Gültigkeitsdauer von fünf Jahren stellt des Weiteren nur eine Obergrenze dar; der Zertifizierungsdiensteanbieter kann also auch einen kürzeren Zeitraum festlegen. Dieser darf den festgelegten Zeitraum der Eignung der eingesetzten Algorithmen und zugehörigen Parameter nicht überschreiten. Das gilt zwar nur für den Zeitpunkt der Erstellung des Zertifikats, sodass eine spätere Änderung der Bewertung der Eignung die Gültigkeit zunächst unberührt lässt. Die zuständige Behörde kann jedoch nach § 19 Abs. 4 Satz 1 SigG die Sperrung von qualifizierten Zertifikaten unter anderem dann verlangen, wenn Tatsachen die Annahme rechtfertigen, dass diese nicht hinreichend fälschungssicher sind.

Damit ist auch die Gültigkeitsdauer des Zertifikats eine variable Größe und von der Eignung der eingesetzten Algorithmen und Parameter direkt abhängig. Es ist dennoch sinnvoll, zwischen diesen und dem Zertifikat zu unterscheiden, weil umgekehrt das Ende der Gültigkeit des Zertifikats die Eignung des Signaturschlüssels nicht beeinträchtigt. Läuft das Zertifikat ab oder wird es aus Gründen gesperrt, die nicht in der Eignung der Algorithmen und Parameter liegen, so kann es vorkommen, dass der im Chipkartenausweis gespeicherte Signaturschlüssel von der zuständigen Behörde nach wie vor als für die nächsten sechs Jahre zur Erstellung qualifizierter Signaturen geeignet bestimmt wird. Da die Sperrung das Zertifikat, nicht jedoch den Signaturschlüssel betrifft, kann für diesen grundsätzlich ein neues Zertifikat ausgestellt werden, allerdings dann nicht, wenn sich der Sperrgrund auf eine befürchtete Kompromittierung des Signaturschlüssels bezieht.

Im Ergebnis sind damit drei Fälle zu unterscheiden:

- Der Ablauf des Gültigkeitszeitraums des Ausweises. Dies beeinträchtigt die Signaturfunktion der Karte nicht. Der Signaturschlüssel ist nach wie vor zur Signaturerstellung geeignet, das Zertifikat gültig. Denkbar ist aber, dass der Ausweisinhaber den Chipkartenausweis nach Ablauf seiner Gültigkeit zurückgeben muss.[1959] Kommt der Inhaber dem nach, so benötigt er nicht nur eine neue Karte, sondern auch ein neues Schlüsselpaar nebst Zertifikat, da eine Übertragung des geheimen Schlüssels auf eine andere Chipkarte technisch nicht möglich ist. Aus signaturrechtlicher Sicht ist für die Rückgabe überdies die für den Schlüsselinhaber nachprüfbare Zerstörung der Karte zu verlangen. Der Schutz des Schlüssels erfolgt durch Besitz und Wissen. Besteht eine Pflicht zur Besitzübertragung auf die ausgebende Stelle, so muss der Chip unbrauchbar gemacht werden, um einen Missbrauch zu verhindern. Gibt der Karteninhaber die Karte andererseits nicht (oder nicht sofort) zurück und erzeugt er mit dieser nach Ablauf der Gültigkeit des Ausweises Signaturen, so sind diese ebenso rechtswirksam wie vor diesem Zeitpunkt. Sie erfüllen

1958 Das wird regelmäßig im Fall des Verlusts der Signaturkarte oder des Ausspähens der PIN der Fall sein, ist nach der Gesetzesbegründung aber auch möglich, wenn der Karteninhaber sich „nach eigenem Ermessen jederzeit aus dem ‚elektronischen Rechtsverkehr' zurückziehen" möchte, s. BR-Drs. 966/96, 35.

1959 Dies ist für den Personalausweis in den Ausführungsgesetzen der Länder bestimmt, s. etwa § 6 Abs. 1 Nr. 2 LPersAuswG Bln., § 6 Nr. 1 LPersAuswG Rh.-Pf., § 7 Nr. 2 LPersAuswG Hess. Auch die Krankenkassen schreiben eine solche Rückgabepflicht vor.

alle Anforderungen des Signaturgesetzes. Überdies ist für einen Erklärungsempfänger nicht erkennbar, dass der Ausweis selbst nicht mehr gültig ist.

- Das Ende der Gültigkeit des qualifizierten Zertifikats. Die Funktion der Karte als Ausweis oder Legitimationsdokument wird davon nicht berührt.[1960] Abgesehen davon, dass das Ende der Gültigkeit bei einer Verwendung als Sichtausweis nicht erkennbar ist, handelt es sich um eine grundsätzlich andere Funktionalität. Wenn der Signaturschlüssel noch hinreichend sicher ist, kann sich der Ausweisinhaber darüber hinaus für diesen ein neues qualifiziertes Zertifikat ausstellen lassen und danach die Karte erneut als sichere Signaturerstellungseinheit verwenden. Schwierigkeiten könnten sich allerdings für den elektronischen Ausweis ergeben, sofern dieser sich auf das alte Zertifikat bezieht. Mit diesem ist das oben beschriebene Modell einer sicheren Authentifizierung nicht mehr durchführbar. Das Problem stellt sich allerdings nur dann, wenn das Zertifikat des Ausweisinhabers (durch die eigene Signatur oder die der Personalausweisbehörde) in den elektronischen Ausweis eingeschlossen würde. Im Regelfall ist dies aus Gründen der Rechtssicherheit geboten.[1961] Für eine sichere Identifizierung nach dem beschriebenen System kommt es jedoch nur darauf an, dass der Ausweisdatensatz mit dem Signaturschlüssel und der Signaturschlüssel mit der Person des Karteninhabers verknüpft werden. Ersteres wird durch den elektronischen Ausweis bewirkt; hierzu ist kein Zertifikat des Karteninhabers erforderlich. Letzteres ergibt sich aus einem qualifizierten Zertifikat, setzt jedoch nicht ein spezifisches, sondern lediglich ein beliebiges Zertifikat voraus. Ein Zertifikatswechsel lässt damit die Funktionsfähigkeit des elektronischen Ausweises unberührt.[1962]
- Der Ablauf der Eignung der eingesetzten Algorithmen und zugehörigen Parameter. Schlüssel und Zertifikat sind dadurch zur Signaturerstellung ungeeignet. Falls (biometrische und andere) Identifikationsdaten unter Verwendung derselben Algorithmen und Parameter verschlüsselt und/oder signiert wurden, wird der Ausweis ungültig.[1963] Für die Sichtfunktion gilt im Übrigen dasselbe wie im Fall des Gültigkeitsablaufs des Zertifikats. Eine Nachlademöglichkeit des Signaturschlüssels – die technisch denkbar wäre – brächte im Unterschied zum Zertifikat massive Sicherheitsprobleme mit sich. Während letzteres nicht sicherheitsrelevant und deshalb aus signaturrechtlicher Sicht nicht schutzbedürftig ist, ist der Schlüssel nach § 15 Abs. 1 Satz 1 SigV durch geeignete Identifikationsmechanismen zu schützen und darf nach § 15 Abs. 1 Satz 2 SigV nicht preisgegeben werden. Für einen nachträglichen Austausch des Schlüssels müssten Löschungs- und Schreibrechte auf den Speicherbereich vergeben werden, in dem dieser abgelegt ist. Das widerspricht den Sicherheitsanforderungen und ist deshalb nicht zulässig. Ein Einsatz als sichere Signaturerstellungseinheit ist deshalb nicht mehr möglich.

In welchem Maße die Gültigkeitszeiträume auseinander fallen, wird entscheidend durch ihre unterschiedliche Dauer bestimmt. So würde ein digitaler Personalausweis, der – wie das bisherige Modell – zehn Jahre gültig wäre, mindestens zwei Zertifikate nacheinander erfordern, um über die gesamte Laufzeit signaturfähig zu sein. Eine Verkürzung des Gül-

1960 Das wird etwa in Estland in § 20 Abs. 3 des Gesetzes über Identitätsdokumente angeordnet.

1961 S. z.B. *Roßnagel*, NJW 2001, 1817, 1825; *GI*, DuD 2001, 38; *Fischer-Dieskau/Gitter/Hornung*, MMR 2003, 384, 386.

1962 S. *Roßnagel/Gitter*, in: Reichl/Roßnagel/Müller 2005, 222; zur Frage des Zertifikatswechsels s.a. *dies*., ebd., 106.

1963 Vgl. ausführlich unten 6.2.1.4; zur Umsetzung der kryptographischen Sicherung unten 6.2.1.

tigkeitszeitraums des Ausweises hebt das Problem nicht auf, weil die Gültigkeit der Schlüssel und Zertifikate stets abrupt enden kann. Nichtsdestotrotz kann es sinnvoll sein, die Laufzeit eines Chipkartenausweises nicht zu lang zu bemessen. Eine lange Gültigkeit behindert einen Technologiewechsel. Da im Bereich der Informationstechnologie alle zwei bis drei Jahre eine neue Technologie-Generation entsteht, ist es sinnvoll, den Ausweis in regelmäßigen Abständen anzupassen. In diesem Fall wird normalerweise kein sofortiger Austausch aller im Umlauf befindlicher Ausweise vorgenommen. Deshalb muss an allen Kontrollstellen die Ausrüstung zum Prüfen der alten Modelle solange vorgehalten werden, wie diese noch im Umlauf sind. Aufgrund der Geschwindigkeit der Entwicklung der Chipkartentechnologie rät auch die ICAO von einer Laufzeit über zehn Jahre ab und empfiehlt den Staaten, eine fünfjährige Gültigkeit aller maschinenlesbaren Reisedokumente mit Chip zu erwägen.[1964]

Bei der Verwendung biometrischer Daten auf dem Chipkartenausweis ergeben sich zwei Besonderheiten. Die eine besteht in der Gefahr der Kompromittierung der Algorithmen und Parameter, die zu ihrer technischen Sicherung verwendet werden,[1965] die andere in der mangelnden Langzeitstabilität einiger biometrischer Merkmale, insbesondere des Gesichts.[1966] Wenn ein Austausch des Referenzdatensatzes möglich ist, stellt beides kein grundsätzliches Problem dar. Es sind nur die Zugriffsorganisation logistisch zu lösen und die entsprechenden Schreibrechte kartenseitig abzusichern. Bei Hochsicherheitskarten wie dem digitalen Personalausweis, die den Referenzdatensatz unveränderbar auf dem Chip ablegen, kann eine Merkmalsänderung über die Zeit jedoch zu Problemen führen, weil sie eine höhere FRR verursacht. Dem Ausweisinhaber ist es nicht möglich, dies zu erkennen. Er wird vielmehr erst bei einem Kontrollvorgang die Veränderung dadurch bemerken, dass er nicht als der wahre Inhaber erkannt wird. Um dem vorzubeugen, empfiehlt es sich, die Laufzeit von Hochsicherheitskarten nicht zu lang zu wählen.

5.2.6 Kartenaktivierung mittels Biometrie?

Elektronische Signaturen dienen der Sicherung von Integrität und Authentizität elektronischer Daten. Werden die den Daten beigefügte Signatur und das zugehörige Zertifikat erfolgreich geprüft, so ist der Nachweis der Integrität der Daten erbracht. Für die Authentizität beweist die Prüfung jedoch nur, dass mit einem bestimmten Signaturschlüssel signiert wurde. Es ist nicht möglich zu erkennen, von welcher Person der Signiervorgang vorgenommen wurde. Um die signierte Erklärung dennoch einer Person zuordnen zu können, wird ein zweistufiges Verfahren angewendet. Der Prozess der Zertifikatsvergabe sichert die ursprüngliche Zuordnung des Schlüssel zu einer Person; das Erfordernis der Eingabe einer PIN, die nur dieser Person bekannt ist, soll die Zuordnung des einzelnen Signiervorgangs ermöglichen.

Die Sicherung mittels einer PIN kann jedoch die Signaturerstellung durch eine dritte Person nicht verhindern, die diese missbräuchlich ausspäht oder mit Wissen des Signaturschlüssel-Inhabers (in einer Art verdeckter Stellvertretung) verwendet.[1967] Dies verursacht Schwierigkeiten hinsichtlich der Authentizität der Erklärung und ihres Beweiswerts im

1964 *ICAO* 2004a, 40, 47; s. zu den Faktoren, die bei der Wahl der Laufzeit zu berücksichtigen sind, auch *Struif/Scheuermann*, in: Reichl/Roßnagel/Müller 2005, 178 f.
1965 S. bereits den dritten Fall oben und näher unten 6.2.1.4.
1966 S.o. 4.2.2.4.1.1.
1967 Vgl. hierzu schon *provet/GMD* 1994, 205 f.

Rechtsverkehr.[1968] Es lässt auch die gesetzgeberische Entscheidung für einen „vorgezogenen Anscheinsbeweis“ in § 371a ZPO fragwürdig erscheinen.[1969]

Da biometrische Merkmale untrennbar mit einer Person verbunden sind, könnte der Einsatz biometrischer Systeme – die technische Sicherheit der Verfahren unterstellt – den Problemen der Weitergabe und des Missbrauchs der PIN abhelfen.[1970] Durch biometrische Systeme wird eine echten Authentizität im Sinne einer Bindung an die Person des Erklärenden selbst hergestellt, auch wenn es zu weitgehend ist, einer Erklärung, die unter Verwendung einer PIN zustande kommt, jede Authentizität abzusprechen.[1971] In jedem Fall würde eine technische Grundlage geschaffen, die die Regelung in § 371a ZPO (zusätzlich) legitimieren würde.[1972]

Die Verwendung biometrischer Daten erfordert immer einen direkten Kontakt mit dem Signaturschlüssel-Inhaber zur Erhebung der Referenzdaten. Dies ist dann unproblematisch, wenn der Registrierungsprozess in einem dezentralen Vertriebssystem erfolgt. Effizienzgewinne ergeben sich, wenn die Registrierungsstellen (wie beim digitalen Personalausweis die Personalausweisbehörden) ohnehin aus anderen Gründen mit den technischen Möglichkeiten zum Enrolment ausgerüstet sind. Kaum zu überwindende Schwierigkeiten bestehen allerdings dann, wenn der Antrag und die Ausgabe der Signaturerstellungseinheit auf dem Postwege erfolgen sollen.

Rechtlich ist der Einsatz biometrischer Merkmale zur Anwendung des Signaturschlüssels in Deutschland bereits zulässig.[1973] Nach § 15 Abs. 1 Satz 1 SigV muss die Signaturkarte gewährleisten, dass der Signaturschlüssel erst nach Identifikation des Inhabers durch Besitz und Wissen oder durch Besitz und ein oder mehrere biometrische Merkmale angewendet werden kann.[1974] Letzteres ist allerdings nach § 15 Abs. 1 Satz 3 SigV nur zulässig, wenn das biometrische Verfahren hinreichend sicherstellt, dass eine unbefugte Nutzung des Signaturschlüssels ausgeschlossen und eine dem wissensbasierten Verfahren gleichwertige Sicherheit gegeben ist.[1975] Die näheren Anforderungen an die Prüftiefen, Schwachstellenbewertungen und Mechanismenstärken ergeben sich aus der Nr. I 1.1 und 1.2 der Anlage zur Signaturverordnung. Geringere Anforderungen gelten nach der Anlage dann, wenn biometrische Merkmale nicht an Stelle, sondern zusätzlich zur Identifikation durch Wissensdaten genutzt werden.

Bislang existiert allerdings kein biometrisches Verfahren, dem eine hinreichende Sicherheit zum Ersatz wissensbasierter Verfahren attestiert worden wäre. Gleichzeitig er-

1968 Ausführlich *Albrecht* 2003a, 64 ff.; 104 ff.; s.a. *dies*. 2002b, 100 ff.; *Schmidt/Lenz* 2002, 266, 272 ff.

1969 S. zu § 371a ZPO bereits die Nachweise in Fn. 1860 (S. 314).

1970 *Albrecht* 2003a, 50; *dies.* 2002b, 100 f.; *Albrecht/Probst* 2001, 40 ff.; *Laßmann*, DuD 1999, 135 f.; *Boente/Riehm*, Jura 2001, 793, 797; *Rapp*, 2002, 20; *Scheuermann/Schwiderski-Grosche/Struif* 2000, 36 f.

1971 So aber *Albrecht* 2003a, 68, 92, 107. Das impliziert, dass die Authentizität einer Handlung ausschließlich mittels Biometrie hergestellt werden kann. Angesichts der massiven technischen Probleme bei der Verwendung zur Signaturerstellung (s. dazu im Folgenden) würde diese Auffassung den elektronischen Rechtsverkehr in seiner gegenwärtigen technischen Ausprägung lähmen, weil keine rechtsverbindlichen elektronischen Erklärungen möglich wären.

1972 Nach *Albrecht* 2003a, 138 ff.; *dies*. 2002b, 108 darf der Gesetzgeber keinen Anscheinsbeweis einrichten, solange die technische Sicherheit des zugrundeliegenden Verfahrens nicht gewährleistet ist.

1973 Zur Diskussion in den USA vgl. *Woodward/Orlans/Higgins* 2003, 260 ff.

1974 Das ist eine Erweiterung gegenüber § 16 Abs. 2 Satz 3 SigV 1997, wonach biometrische Merkmale lediglich zusätzlich zur Identifikation durch Besitz und Wissen angewendet werden durften.

1975 S. *Roßnagel*, BB 2002, 261, 263; *Albrecht* 2003a, 81 f. m.w.N.

scheint es sehr fraglich, ob dies in absehbarer Zukunft erreichbar ist.[1976] Denn von sonstigen Problemen biometrischer Verfahren (insbesondere ihrer Fehleranfälligkeit) abgesehen, findet der Prozess der Signaturerstellung regelmäßig in der unbeobachteten Umgebung eines heimischen PCs statt, oder die Signaturkarte muss dies zumindest ermöglichen. Dies stellt ein erhebliches Sicherheitsrisiko dar. Ein Angreifer kann entweder die Signierumgebung des Karteninhabers manipulieren oder sich selbst die Karte verschaffen, um deren Sicherheitsmechanismen mit Hilfe von eigenen, manipulierten Signaturerstellungskomponenten zu überwinden. Zwar könnte die Signaturkarte mit einem Fingerabdrucksscanner oder einer Kamera zur Erfassung von Gesichts- oder Irisbildern geliefert werden, die über ein System zur Lebenderkennung verfügen. Auch dann hätte der Mechanismus in der Karte jedoch kaum eine Möglichkeit zu prüfen, ob an diesen manipuliert oder ein anderes Gerät verwendet wurde.[1977]

Zwar stellt sich auch bei der PIN das parallele Problem der Verwendung unsicherer Komponenten. Wie bei der Übertragung biometrischer Daten ist es möglich, die PIN mitzuschneiden, solange diese am PC über die Tastatur eingegeben wird. Dazu ist jedoch ein Abhören eines solchen Vorgangs erforderlich (bei dem der Nutzer zumindest anwesend ist und so eine gewisse Kontrolle ausüben kann), während biometrische Daten in einer Vielzahl von Alltagssituationen in einer Art und Weise hinterlassen werden, die eine Verwendung zu Fake-Angriffen möglich macht.

Auch gegen Replay-Attacken[1978] gibt es kaum einen Schutz. Zwar bestimmt § 15 Abs. 2 Nr. 1 a) SigV, dass die Identifikationsdaten nicht preisgegeben und nur auf der sicheren Signaturerstellungseinheit gespeichert werden dürfen. Hieraus folgt, dass die biometrischen Referenzdaten niemals die Signaturkarte verlassen dürfen und somit Matching-On-Card zu erfolgen hat.[1979] Dies bietet jedoch nur begrenzten Schutz, da biometrische Daten des Schlüsselinhabers auch durch Datenakquisitions-Angriffe beschafft oder an ungesicherten Datenleitungen in der heimischen Peripherie mitgeschnitten werden können. Die Verwundbarkeit durch Replay-Angriffe ist umso stärker, als das gängigste Verfahren hiergegen bei Chipkarten nicht praktikabel ist. Dabei wird der Zugriff immer dann verweigert, wenn zum Abgleich Daten an die Matching-Einheit gesendet werden, die in exakt dieser Form bereits zum Matching verwendet wurden.[1980] Dies spricht in hohem Maße für einen Replay-Angriff, weil es aufgrund der verschiedenen Ungenauigkeiten biometrischer Systeme[1981] praktisch ausgeschlossen ist, dass zwei Erhebungen eines biometrischen Merkmals zu exakt denselben Datensätzen führen. Ein solcher Schutzmechanismus setzt jedoch die Speicherung aller jemals zum Matching verwendeten Datensätze voraus. Dies ist wegen der begrenzten Speicherkapazität der Signaturkarte undurchführbar.

Aufgrund dieser prinzipiellen Probleme der Endgerätesicherheit greifen Ansätze zu kurz, die lediglich die – unbestreitbaren – technischen Probleme wissensbasierter Systeme betonen, die zum gegenwärtigen Zeitpunkt noch größeren Schwierigkeiten biometrischer Verfahren zur Sicherung des Signaturschlüssels jedoch als lösbar voraussetzen.[1982] Die im

1976 Vgl. zur Verwendbarkeit von Biometrie zur Signatur aus technischer Sicht *Struif/Scheuermann/Ullrich/Kraas*, in: Reichl/Roßnagel/Müller 2005, 190 und ausführlich für den Stand des Jahres 2000 *Scheuermann/Schwiderski-Grosche/Struif* 2000, 38 ff., 43 ff.

1977 S. zur Frage der Lebenderkennung auch unten 6.2.2.

1978 S. zu den Angriffen auf biometrische Systeme oben 4.3.8.1.

1979 RMD-*Roßnagel/Pordesch*, § 16 SigV 1997, Rn. 62, 66.

1980 So etwa im online-Banking System TOCA von ekey biometric systems (http://www.ekey.at) aus Österreich.

1981 Vgl. oben 2.3.3.2.

1982 So insbesondere durchgängig *Albrecht* 2003a; vgl. ebd., 27, wonach „bei der hier angestellten Untersuchung...stets solche biometrischen Systeme vorausgesetzt [sind], die den im technischen Kapitel

Grundsatz richtigen Überlegungen zur Herstellung von Authentizität bleiben notwendigerweise theoretisch, solange keine Konzepte zur Erfüllung essentieller Sicherheitsanforderungen erkennbar sind. Hinreichend wäre wohl nur eine technische Lösung, die einen zur Lebenderkennung fähigen Sensor in die sichere Signaturerstellungseinheit integriert und beide durch ein Hochsicherheitsgehäuse miteinander verbindet.[1983]

Ein gangbarer Weg dürfte demgegenüber die Verwendung biometrischer Identifikationssysteme als Ergänzung zu wissensbasierten Verfahren sein. Durch diese Kombination könnte ein deutlich höheres Sicherheitsniveau gegenüber der heutigen PIN-Absicherung erreicht und so die Authentizität einer abgegebenen Erklärung verstärkt werden. Ein alleiniger Schutz des Signaturschlüssels mittels biometrischer Daten ist dagegen in absehbarer Zeit nur beim Einsatz in kontrollierten Umgebungen denkbar. Wird sichergestellt, dass die Signaturkarte ausschließlich in einer solchen Umgebung verwendet wird, die etwa am Arbeitsplatz eingerichtet werden könnte, so könnte bei entsprechendem technischem Fortschritt eine der PIN vergleichbare Sicherheit gewährleistet werden.

Diskutiert werden schließlich – insbesondere im Gesundheitswesen – Ansätze einer anderen Form der Kombination von PIN und Biometrie. Beim Einsatz von Signaturkarten in Apotheken ergibt sich das Problem, dass deren Angestellte an ständig wechselnden Arbeitsplätzen im Ladenbereich und hinteren Räumlichkeiten tätig sind. Im herkömmlichen Verfahren müsste die Karte nach jedem Signiervorgang aus einer Signierstation gezogen und in eine neue eingesteckt werden. Außerdem wäre die erneute Eingabe der PIN erforderlich. Das VERSA-Konzept der Apotheker schlägt demgegenüber ein stationäres Kartenlesegerät vor, in dem die Karte verbleibt.[1984] Der Karteninhaber soll lediglich einmal täglich seine PIN eingeben und danach am jeweiligen Arbeitsplatz unter Verwendung seines Fingerabdrucks seinen Signaturschlüssel freigeben. Die genaue Untersuchung der Sicherheit dieses Verfahrens steht noch aus.

Eine Besonderheit ergibt sich schließlich dann, wenn die sichere Signaturerstellungseinheit auch in anderen Bereichen zur biometrischen Authentifizierung eingesetzt werden soll. Das könnte beim digitalen Personalausweis (in hoheitlichen und privaten[1985] Anwendungen), aber auch bei anderen Chipkartenausweisen der Fall sein. Hier ist eine Differenzierung erforderlich, weil bei der Absicherung der Signaturerstellung die Sicherheit des Verfahrens durch die Karte selbst prüfbar sein muss, während dies bei einer Ausweisfunktion in der Prüfumgebung der kontrollierenden Instanz gewährleistet werden sollte. Ersteres bedingt ein Matching auf der Karte, letzteres ein solches in der Prüfumgebung. Um einen minimalen Schutz gegen Replay-Attacken zu gewährleisten, sind unterschiedliche Datensätze zu verwenden und die jeweiligen Verfahren wirksam gegeneinander abzuschotten.

Im Ergebnis bietet der Einsatz von Biometrie perspektivisch Vorteile für die Nutzerfreundlichkeit der Signaturerstellung und die Authentizität der signierten Erklärung. Die Einsatzumgebungen sind jedoch genau auf die jeweiligen Sicherheitsdefizite zu untersuchen, weil sonst der umgekehrte Effekt eintreten könnte. Das würde nicht nur das Ansehen der Biometrie-Anbieter, sondern auch das Vertrauen in den elektronischen Rechtsverkehr beschädigen.

---

aufgestellten Sicherheitsanforderungen in hinreichendem Maße genügen". Die technischen Probleme (v.a. von Datenakquisitions-Angriffen) werden auch von *Aufreiter* 2002 (insbes. 253 f.) ignoriert, wonach es schwieriger sein soll, sich ein biometrisches Merkmal zu beschaffen, als eine PIN auszuspähen. Kritisch gegenüber dem Potential biometrischer Verfahren auch *Fox*, DuD 2002, 450.

1983 S.a. *Scheuermann/Schwiderski-Grosche/Struif* 2000, 52.

1984 Vgl. *ABDA* 2002.

1985 S. dazu oben 4.2.2.5.

6 Aspekte der technischen und organisatorischen Umsetzung

Die erörterten Bestimmungen des Datenschutz-, Signatur- und Ordnungsrechts haben Einfluss auf die technische und organisatorische Gestaltung von Chipkartenprojekten. Einige der aus technischer Sicht denkbaren Umsetzungsvarianten haben sich als rechtlich unzulässig herausgestellt. Im Folgenden werden – im Sinne rechtswissenschaftlicher Technikgestaltung[1986] – einzelne Aspekte erörtert und bewertet, die die gefundenen Gestaltungsanforderungen berücksichtigen, ohne dass dabei der Anspruch einer vollständigen Behandlung der technischen Umsetzung erhoben wird.[1987]

6.1 Allgemeine Umsetzungsstrategien

6.1.1 Mechanismen der Datensicherung

Trotz der unterschiedlichen Funktionsweise der betrachteten Chipkartensysteme sind die grundsätzlichen Strategien zur Datensicherung auf der technischen Ebene weitgehend identisch.[1988] Es handelt sich vor allem um Verfahren der Abschottung, des Back-Ups und der elektronischen Signatur, Authentisierung und Verschlüsselung.[1989] Mit diesen kann den angesprochenen Risiken adäquat begegnet werden. Als Grundlage ist stets eine verbindliche Festlegung von organisatorischen Verantwortlichkeiten, Befugnissen und Abläufen des Umgangs mit den Daten erforderlich.[1990] Diese hat sich an der Bedrohungs- und Risikoanalyse zu orientieren.

Die Vertraulichkeit der Daten ist durch die Verwendung starker kryptographischer Verfahren sicherzustellen. Dies gilt für die Angaben auf den Karten selbst, wenn sie vor dem Zugriff Dritter sicher zu schützen sind. Ergibt die Bedrohungsanalyse, dass – wie beim elektronischen Rezept – eine Sicherung durch den Besitz der Karte ausreichend ist, so kann die Sicherheit auf die Applikationsebene verlagert werden. Wird ein Verschlüsselungsmechanismus eingesetzt, so ist es erforderlich, dass der Inhaber diesen freischaltet. Dazu muss er sich gegenüber dem Ausweis authentisieren. Unter Datensicherheitsgesichtspunkten muss das diesem Vorgang zugrundeliegende Verfahren hochsicher sein, weil ansonsten Gefahren für die Integrität, Vertraulichkeit und Kontrollierbarkeit der Daten entstehen. PIN-Verfahren sind hierfür anerkannt und – bei allen Schwächen – auch geeignet. Der Einsatz biometrischer Verfahren kommt dann in Betracht, wenn diese hinreichend sicher sind. Die Überlegungen zur Verwendung von Biometrie im Rahmen qualifizierter Signaturverfahren[1991] sind insoweit auf Anwendungen übertragbar, die eine ähnlich hohe Sicherheit voraussetzen und in ähnlich schwer kontrollierbaren Umgebungen ablaufen. Be-

1986 S. zum Verhältnis von Recht und Technik oben 2.4.

1987 Allein die Rahmen- und Lösungsarchitekturen für die Telematik im Gesundheitswesen umfassen jeweils mehr als 1.000 Seiten. Eine Erläuterung der Gesamtkonzepte würde den Rahmen dieser Arbeit sprengen; s. ausführlich zum digitalen Personalausweis die Beiträge in Reichl/Roßnagel/Müller 2005, 63 ff., 75 ff., 167 ff., 181-218 und für die elektronische Gesundheitskarte die jeweils aktuellen Entwicklungen unter http://www.dimdi.de/.

1988 Aufgrund der im Gesundheitswesen – im Unterschied zum Personalausweis – schon länger existierenden Diskussion (s. z.B. bereits *v. Heydwolff/Anderson*, DuD 1997, 569 ff.; *Rienhoff*, DuD 1997, 579 ff.) befassen sich die Belege in den folgenden Fußnoten überwiegend mit diesem Bereich. Die Konzepte sind jedoch weitgehend verallgemeinerbar.

1989 S. allgemein Roßnagel-*Heibey*, Kap. 4.5, Rn. 96 ff.

1990 Roßnagel-*Heibey*, Kap. 4.5, Rn. 89 f.; s.a. *Jürgens* 2003, unter 2.2. Das schließt sich an die rechtlichen Anforderungen aus § 9 BDSG und der Anlage zu dieser Norm an, s.o. 4.3.8.2.

1991 S.o. 5.2.6.

sonderheiten ergeben sich schließlich dann, wenn wie beim digitalen Personalausweis ein Zugriff auch ohne Mitwirkung des Inhabers erfolgen soll.[1992]

Neben der Vertraulichkeit der auf der Chipkarte gespeicherten Daten ist auch die Vertraulichkeit der Übermittlungswege mittels Kryptographie zu gewährleisten. Das ist umso wichtiger, je mehr Daten in Serversystemen gespeichert werden, zu denen die Chipkarte den Zugang vermittelt.

Zu den Übermittlungswegen zählt auch die Datenübertragung zwischen der Chipkarte und dem Lesegerät. Chipkartenlesegeräte mit kontaktorientierter Schnittstelle werden in verschiedene Sicherheitsklassen unterteilt; für die Absicherung der Kommunikation stehen eine Reihe mechanischer Schutzvorkehrungen zur Verfügung.[1993] Diese Mechanismen sind aber technisch aufwendig und entsprechend teuer. Sie kommen deshalb lediglich für öffentliche Kartenterminals, nicht jedoch für Anwendungen am privaten PC in Betracht.

Bei kontaktlosen Systemen ist ein Mitschneiden der Daten an der Luftschnittstelle relativ problemlos möglich. Um dem vorzubeugen, werden Secure Messaging (SM)-Verfahren gemäß ISO/IEC 7816-4 eingesetzt.[1994] Diese entsprechen im Wesentlichen den allgemeinen Verschlüsselungsverfahren, setzen also die Verwendung eines symmetrischen Schlüssels, der auf der Karte und im Lesegerät gespeichert ist, oder den sicheren Austausch eines Session-Keys voraus. Ein weiterer Sicherheitsmechanismus ist die gegenseitige Authentisierung zwischen Karte und Lesegerät im Challenge-Response-Verfahren.[1995] Trotz dieser Verfahren sind kontaktlose Schnittstellen zu anfällig für einen Einsatz in Anwendungen, die höchsten Sicherheitsansprüchen genügen müssen. Eine Verwendung im Rahmen der qualifizierten Signatur ist deshalb abzulehnen.

Diese ist ihrerseits ein effektives Mittel zur Gewährleistung von Integrität und Authentizität der verwendeten Daten.[1996] Die qualifizierte Signatur gewährleistet die Zuordnung von Daten zur ausstellenden Instanz (etwa der Ausweisdaten zur Personalausweisbehörde oder der Untersuchungsergebnisse zum behandelnden Arzt), wie auch eine Überprüfbarkeit hinsichtlich nachträglicher Veränderungen. Sie ist damit auch ein Instrument zur Gewährleistung der Revisionsfähigkeit der Datenverarbeitungen. Hier müssen allerdings ergänzende Verfahren angewendet werden.[1997] So kann ein Zertifizierungsdiensteanbieter mittels elektronischer Zeitstempel, die den exakten Zeitpunkt der Erstellung oder Veränderung von Daten nachprüfbar festhalten, nach § 2 Nr. 14 SigG bescheinigen, dass ihm bestimmte elektronische Daten zu einem bestimmten Zeitpunkt vorgelegen haben.[1998] Über Protokollierungsverfahren können der Versand und der Erhalt von Daten nachträglich bewiesen werden.

1992 S.u. 6.2.1.3.

1993 S. *Bittlinger*, in: Reichl/Roßnagel/Müller 2005, 209; s.a. oben 2.3.1.

1994 S. näher *Rankl/Effing* 2002, 433 ff.; *Struif/Scheuermann/Ullrich/Kraas*, in: Reichl/Roßnagel/Müller 2005, 189 f. Um den unbemerkten Verlust eines abgesendeten Kommandos zu unterbinden, wird zusätzlich ein Zahlenwert (Send Sequence Counter, SSC) eingesetzt, der bei der ersten Kommunikation zwischen Sender und Empfänger auf einen nach außen unbekannten Initialwert gesetzt und bei jeder Datenübermittlung hochgezählt wird. Damit werden Manipulationen zwar nicht verhindert, aber bemerkt; vgl. zum sicheren Datentransfer zwischen Karte und Leser auch *Struif/Scheuermann/Ullrich/Kraas*, in: ebd., 190 f.; *Scheuermann/Schwiderski-Grosche/Struif* 2000, 43 ff.

1995 Diese kann allerdings je nach Einsatzumgebung schwierig umsetzbar sein, s.u. 6.2.1.2.

1996 *BITKOM/VDAP/VHitG/ZVEI* 2003, 54 f.; *Bultmann/Wellbrock/Biermann/Engels/Ernestus/Höhn/Wehrmann/Schurig* 2002, 21; *Hermeler* 2000, 105; Roßnagel-*Schirmer*, Kap. 7.12, Rn. 103 ff.; zur Funktionsweise vgl. oben 2.3.2.

1997 Näher *Bultmann/Wellbrock/Biermann/Engels/Ernestus/Höhn/Wehrmann/Schurig* 2002, 23 f.; s.a. Roßnagel-*Heibey*, Kap. 4.5, Rn. 107 ff.

1998 Zum Zeitstempel vgl. RMD-Roßnagel, § 2 SigG 1997 Rn. 75 ff. m.w.N.; *Gassen* 2003, 60 f.

Sind an einem Chipkartensystem mehrere Zugriffsberechtigte beteiligt, so ist zur Herstellung von Vertraulichkeit und organisatorischer Sicherheit die Bereitstellung abgestufter Zugriffssysteme erforderlich. Hierbei werden ausdifferenzierte Rollenkonzepte erstellt, die danach auf der technischen Ebene in entsprechenden Zugriffsbefugnissen abgebildet werden müssen. Das ist durch PKI-basierte Authentisierungsverfahren[1999] oder entsprechende Attribut-Zertifikate[2000] möglich. Die Applikationen sind dann nur denjenigen Teilnehmern zugänglich, die über ein entsprechendes Attribut verfügen.

Bei der Sicherung der Verfügbarkeit ist zwischen den Karten selbst und der Peripherie zu differenzieren. Besteht wie bei der elektronischen Gesundheitskarte eine fortlaufende Interaktion mit einer hochentwickelten Telematikstruktur, so müssen die Daten von der Peripherie schnell und sicher verfügbar sein. Die Chipkarten selbst müssen den üblichen Standards hinsichtlich Haltbarkeit, Abnutzung und Resistenz gegen zufällige Überbeanspruchung genügen.[2001] Der Chip ist auch gegen Angriffe zu schützen.[2002]

Die Forderung nach geeigneten Rückfallsystemen für den Fall eines Systemausfalls oder der Unbenutzbarkeit der Chipkarte hängt eng mit der Frage der Verfügbarkeit der Daten zusammen. Da der Karteninhaber die Funktionstüchtigkeit der Karte kaum kontrollieren kann, muss zumindest im Notfall eine Möglichkeit bestehen, allein auf der Basis der Sichtausweisfunktion der Karte akzeptiert zu werden. Aus dieser Anforderung folgt einerseits, dass die Sicherheit der Chipkarte nicht allein in der Sicherheit der elektronisch gespeicherten Daten liegen darf, andererseits, dass alternative Verfahrensabläufe ohne diese Daten vorhanden sein müssen.

Soll eine Chipkarte als Sichtausweis einsetzbar sein, so muss sie – wie der bisherige Personalausweis[2003] – über eine Reihe von Sicherheitsmerkmalen gegen Verfälschungen verfügen. Die Anforderungen an diese Merkmale richten sich nach dem Risiko und den Gefahren eines Missbrauchs. Sie werden deshalb beim digitalen Personalausweis höher sein als bei der elektronischen Gesundheitskarte. Übliche Sicherheitsmerkmale für Chipkarten sind beispielsweise Guillochen, Positiv-Negativ-Prägungen, Irisverläufe, Sicherheitsdruck, Spezialtinte, kopierresistente Druckfarben, optisch variable Merkmale und Farben, Laser-Kippbild, Kinegramm, UV-Druck und Hologramm.[2004] Die Fälschungssicherheit wird dabei nach dem Kostenwettbewerbsprinzip angestrebt: Ziel ist es, das Fälschen teuer, schwierig oder extrem zeitaufwendig zu machen. Das so erreichbare Sicher-

---

1999 *BITKOM/VDAP/VHitG/ZVEI* 2003, 56 ff.; Roßnagel-*Heibey*, Kap. 4.5, Rn. 103. Dabei wird der Authentisierungsschlüssel der Karte eingesetzt, der vom Signaturschlüssel verschieden ist; s. näher oben 2.3.2.

2000 Vgl. für das Gesundheitswesen *BITKOM/VDAP/VHitG/ZVEI* 2003, 42 ff.

2001 Die hierfür relevanten internationalen Normen sind EN ISO/IEC 10373, ISO/IEC 7816 und EN 27816. Danach sind bestimmte Zuverlässigkeitstests vorgeschrieben, die das Verhalten der Karte unter widrigen Bedingungen testen; s. näher *Rankl/Effing* 2002, 578 ff.; *Kallmeyer/Bittlinger/Struif/Scheuermann/Köppen*, in: Reichl/Roßnagel/Müller 2005, 73 ff.

2002 S. dazu *Kallmeyer/Bittlinger/Struif/Scheuermann/Köppen*, in: Reichl/Roßnagel/Müller 2005, 63 ff.; *Rankl/Effing* 2002, 535 ff. Bei kontaktorientierten Schnittstellen wird z.B. das Kontaktmodul verkapselt, um seine Entfernung zu erschweren, die einen direkten Zugang zum Chip eröffnen würde. Gegen Versuche, den Inhalt des Chips auszulesen, können auf ihm Metallflächen angebracht werden, die nicht abgetragen werden können, ohne die darunter liegenden Funktionsstrukturen zu beschädigen (Tresorfunktion). Bei kontaktlosen Schnittstellen erfolgt die Verbindung mit dem Kartenkörper meist in der Flip-Chip-Technik mit anisotrop leitfähigem Klebstoff. Die Entnahme solcher Chips ist grundsätzlich nur durch Zerstörung des Kartenkörpers möglich.

2003 Vgl. oben 4.2.2.2.

2004 S. zur Funktionsweise *Kallmeyer/Bittlinger/Struif/Scheuermann/Köppen*, in: Reichl/Roßnagel/Müller 2005, 68 ff.

heitsniveau ist nicht für die Zukunft quantifizierbar, da es durch technologische Entwicklungen beeinflusst wird.[2005]

Alternative Verfahrensabläufe kommen dann zum Einsatz, wenn ein Systemausfall vorliegt, ein Beteiligter seine Chipkarte nicht verfügbar oder vergessen hat oder diese nicht funktionstüchtig ist. Bei der elektronischen Gesundheitskarte sind effektive Rückfallsysteme zu implementieren, die eine ärztliche Versorgung auch beim Ausfall einzelner Komponenten garantieren.[2006] Der digitale Personalausweis muss auch im Fall der Funktionsuntüchtigkeit als Sichtausweis verwendbar sein.[2007]

Bei Chipkarten, die wie die elektronische Gesundheitskarte ein Zugangsinstrument zu Daten sind, ist es für den Fall des zufälligen Kartenverlusts oder Diebstahls wichtig, eine unmittelbare Sperrmöglichkeit einzurichten, um eine missbräuchliche Verwendung zu verhindern. Das kann zum Beispiel durch die Einrichtung einer Hotline mit 24-stündiger Erreichbarkeit realisiert werden.[2008] Verfügt der Chipkartenausweis über eine Signaturfunktion, so ist dieses Verfahren bereits nach § 7 Abs. 1 SigV vorgeschrieben.

Eine sichere Datentrennung zwischen den auf der Chipkarte implementierten Applikationen ist technisch machbar und entspricht dem Standard zertifizierter Karten und der auf ihnen ablaufenden Betriebssysteme, die die Möglichkeit bereitstellen, für neu angelegte Dateien oder Applikationen individuelle Zugriffsrechte festzulegen. Das Betriebssystem sorgt dann dafür, dass auf diese nur mit den jeweils zugelassenen Kommandos beziehungsweise nach dem Setzen des individuell geforderten Sicherheitsstatus zugegriffen werden kann.[2009] Damit ist es beispielsweise möglich, beim digitalen Personalausweis die Identifikations- und Signaturfunktionen ohne gegenseitige Zugriffsmöglichkeiten auf demselben Chip zu implementieren und bei der elektronischen Gesundheitskarte unterschiedliche Datenfelder, etwa für die verschiedenen Funktionen (§ 291a Abs. 2 Satz 1 und Abs. 3 Satz 1 SGB V), einzurichten.[2010]

6.1.2 Standardisierung

Jedes Chipkartenprojekt, welches nicht vollständig autark und ohne technische Weiterentwicklung arbeitet, ist auf Interoperabilität angewiesen. Das Mittel zu ihrer Ereichung ist die Standardisierung.[2011] Diese ist aus rechtswissenschaftlicher Sicht bedeutsam, weil nur hinreichend interoperable Systeme die erforderliche Eignung für den Einsatz aufweisen. Insbesondere internationale Standards können auf diese Weise auch die deutsche verfassungsrechtliche Bewertung beeinflussen.[2012]

Die Relevanz von Interoperabilität lässt sich am Beispiel des digitalen Personalausweises verdeutlichen. Da dieser in Europa als Reisedokument anerkannt sein wird, müssen nicht nur alle deutschen, sondern alle europäischen Kontrollstellen in der Lage sein, seine Echtheit zu überprüfen und Daten aus ihm auszulesen. Dabei ist es nicht hinreichend, die in Deutschland verwendeten Parameter zu veröffentlichen, weil kein Staat für die Ausweise jedes anderen Staates unterschiedliche Prüfgeräte vorhalten kann. Vielmehr muss ein

2005 *Köppen/Schneider*, in: Reichl/Roßnagel/Müller 2005, 55.
2006 S.u. 6.3.1.
2007 Das gilt allerdings nur für den ersten Kontrollvorgang; vgl. unten 6.2.1.4.
2008 Vgl. für die Gesundheitskarte *BITKOM/VDAP/VHitG/ZVEI* 2003, 49.
2009 S. *Struif/Scheuermann*, in: Reichl/Roßnagel/Müller 2005, 172; s.a. *Scheuermann*, DuD 2005, 66, 67 f.
2010 Zur Frage der abgestuften Zugriffsrechte vgl. unten 6.3.3.1.
2011 S. allgemein *Wende* 2002, 1101 ff. (dort auch zur tlw. uneinheitlichen Verwendung der Termini Norm, Spezifikation und Standard).
2012 Vgl. z.B. für die Frage des (datenschutzrechtlich wünschenswerten, aber durch mangelnde Interoperabilität behinderten) Einsatzes von Templates beim digitalen Personalausweis oben 4.2.2.4.2.

einziges Gerät zur Kontrolle sämtlicher Ausweise geeignet sein. Das Gleiche gilt auch für die elektronische Gesundheitskarte. Je mehr medizinische Dienstleistungen im Ausland in Anspruch genommen werden, desto wichtiger wird die Interoperabilität mit den dortigen Datenverarbeitungssystemen.

Interoperabilität hat eine räumliche, eine anwendungsbezogene und eine zeitliche Komponente. In räumlicher Hinsicht ist die technische Zusammenarbeit auf der regionalen, nationalen und internationalen Ebene anzustreben, auf der Anwendungsebene die Interaktionsmöglichkeit der Systeme, die unterschiedliche gesellschaftliche Funktionen (beispielsweise im Electronic Commerce und Electronic Government) erfüllen. Bei der Migration zu künftigen Technologiegenerationen muss schließlich die Abwärtskompatibilität gewährleistet werden, solange kein vollständiger Austausch aller Komponenten erfolgt ist.

Interoperabilität ist nicht mit einem schrankenlosen Datentransfer zwischen den beteiligten Datenverarbeitungssystemen zu verwechseln. Angestrebt wird lediglich, dass die verschiedenen Komponenten eines Systems und die Systeme selbst miteinander elektronisch interagieren können. Welche Daten letztlich tatsächlich kommuniziert werden, ist eine Frage der technischen Konfiguration des einzelnen Systems.

Standardisierungsverfahren werden in Deutschland überwiegend durch das Deutsche Institut für Normung (DIN) durchgeführt. Im Zuge der Globalisierung agiert das Institut kaum noch national, sondern konzentriert seine Arbeit auf die europäischen und internationalen Normungsgremien, die mittlerweile mehr als 85 Prozent seiner Aktivitäten ausmachen.[2013] In Europa werden einheitliche Standards durch die gemeinsame europäische Normungsorganisation aus European Committee for Standardization und European Committee for Electrotechnical Standardization (CEN/CENELEC) durchgeführt, deren Ergebnisse von allen Mitgliedstaaten der Europäischen Union unverändert als nationale Normen übernommen werden müssen. Weltweite Standards werden durch die International Organization for Standardization (ISO) festgelegt. Die Mitgliedsländer sind nicht verpflichtet, ISO-Standards in ihr nationales Normenwerk zu übernehmen. Die Welthandelsorganisation strebt jedoch eine stärkere Verpflichtung zur Übernahme der ISO-Normen an. Neben diesen übergreifenden Organisationen ist auf dem elektrotechnischen Sektor die International Electrotechnical Commission (IEC) tätig. Sie arbeitet analog zur ISO. Für die Normung im Bereich der Telekommunikation sind auf internationaler Ebene die International Telecommunication Union (ITU) und in Europa das European Telecommunications Standards Institute (ETSI) zuständig.

Es existieren mittlerweile eine Reihe von Standards, die Chipkartenausweise selbst oder die mit ihnen interagierenden Anwendungen betreffen. Wo dies noch nicht der Fall ist, wird die Standardisierung meist mit Nachdruck vorangetrieben. Das beinhaltet auch die Verbesserung bereits bestehender Normen, da sich bisweilen erst in der Praxis herausstellt, dass auch Komponenten, die denselben Standard einhalten, nicht immer miteinander kompatibel sind.[2014]

Standards für die Spezifikation der Schnittstelle zu kontaktbehafteten und kontaktlosen Chipkarten werden bei der ISO durch das Sub-Committee (SC) 17 erstellt.[2015] Die Standards der Reihe ISO/IEC 7816 wurden zwar ursprünglich für kontaktbehaftete Chipkarten

2013 S. zum Folgenden http://www.normung.din.de/ → Normungsverfahren → Auf dem Weg zu globalen Standards.

2014 So ergaben Tests der US-Regierung mit kontaktlosen Chipkarten zu Beginn des Jahres 2004, dass nicht alle Geräte miteinander interagieren konnten, obwohl alle den Standard ISO/IEC 14443 einhielten. S. http://www.cardtechnology.com/cgi-bin/readstory.pl?story=20040317IDNN784.xml.

2015 Vgl. zu den folgenden Standards *Struif/Scheuermann*, in: Reichl/Roßnagel/Müller 2005, 38 ff.; s.a. *Vedder/Weikmann* 1998, 2 ff., 8 f.; zu Standards für Identifikationskarten auch *Wende* 2002, 1127 ff.

konzipiert, weite Teile davon gelten nunmehr jedoch auch für kontaktlose Schnittstellen. Standardisiert sind die physikalische Schnittstelle (beispielsweise die Lage der Kontakte), die Übertragungsprotokolle, die Kommandos und Datenobjekte, die Organisations-Struktur der Datenfelder und die Sicherheitsarchitektur. Der neue Teil 11 befasst sich (aus Kartensicht) mit der Biometrie. Für kontaktlose Schnittstellen sind je nach Abstand zum Lesegerät die Standards ISO/IEC 10536 („close-coupled", Abstand bis 1 cm), ISO/IEC 14443 („proximity", bis 10 cm) oder ISO/IEC 15693 („vicinity", bis 1 m) einschlägig.

Der digitale Personalausweis hat die Vorgaben der ICAO einzuhalten.[2016] Das dreiteilige ICAO DOC 9303[2017] beschäftigt sich mit maschinenlesbaren Reisedokumenten, nämlich Reisepässen, Visa und anderen Dokumenten, die entweder das Chipkarten-Format oder das des jetzigen deutschen Personalausweises haben können. Zwei grundlegende Bestandteile eines jeden ICAO-konformen Reisedokumentes sind die „Visual Inspection Zone" mit aufgetragenen Daten zum manuellen Lesen durch eine Person und die „Machine Readable Zone" mit maschinenlesbaren Daten. Bei der letzteren handelt es sich jedoch nicht um einen elektronischen Datenspeicher, sondern lediglich um ein Feld mit aufgedruckten alphanumerischen Informationen, welche dann opto-elektronisch eingescannt werden. Das neue DOC 9303 enthält nunmehr auch Anforderungen an kontaktorientierte und kontaktlose Chips, übernimmt dabei aber die gängigen ISO/IEC Standards. Erste Überlegungen bestehen zur Verwendung von PKI.[2018] Daneben existieren Vorgaben der ICAO zu Sicherheitsmerkmalen, beispielsweise den mechanischen Eigenschaften aufgedruckter Merkmale, des zu verwendenden Papiers oder der Versiegelungen.

Die Standardisierungsaktivitäten für biometrische Datenformate werden bei der ISO von verschiedenen Arbeitsgruppen des SC 37 durchgeführt.[2019] Als übergreifende Spezifikationen existieren das Common Biometric Exchange Formats Framework (CBEFF) nach ISO/IEC 19785, das für unterschiedliche biometrische Merkmale und Verfahren anwendbar ist, und als Schnittstelle die so genannte „BioAPI" gemäß ISO/IEC 19784.[2020] Die ISO/IEC 19794-Serie (Biometric Data Interchange Formats) umfasst ein generelles, generisches Rahmenwerk und Festlegungen für unterschiedliche Verfahren, nämlich Fingerminutien, Fingerlinien, Fingervollbild, Gesichtsvollbild, Irisvollbild, Unterschriftsbild, Handgeometrie und Venenmuster. Die Normierung des Rahmenwerks und der Verfahren ist unterschiedlich weit fortschritten, einige Normen haben jedoch bereits die Industrietauglichkeit erreicht. Des Weiteren befassen sich Arbeitsgruppen des SC 37 mit der Vereinheitlichung biometrischer Termini, Evaluationskriterien und juristischen Aspekten.

Für Funktionen im Bereich von Public-Key-Infrastrukturen, also der elektronischen Signatur, Authentisierung und Verschlüsselung bauen die meisten Standards auf die Formate X.509 (Zertifikate und Zertifikats-Widerrufungs-Listen) und PKCS (weitere PKI-Funktionen) auf.[2021] Die aus den Standards MTT (TeleTrusT e.V.) und ISIS (T7-Gruppe) zusammengefügte Spezifikation ISIS-MTT enthält auf dieser Basis Festlegungen für einen

2016 Zur ICAO vgl. oben 3.1.1.
2017 *ICAO* 2003a, 1994, 2002.
2018 S.u. 6.2.1.1.
2019 S. näher *Struif/Scheuermann*, in: Reichl/Roßnagel/Müller 2005, 41 ff.; *Rejman-Greene* 2003b, 142 ff.; *OECD* 2004, 38 f.; *Sietmann*, c't 23/2002, 54 ff.; zu amerikanischen Aktivitäten vgl. *Woodward/Orlans/Higgins* 2003, 167 ff.; s.a. *Bolle/Connell/Pankanti/Ratha/Senior* 2004, 231 ff.
2020 S. *Bolle/Connell/Pankanti/Ratha/Senior* 2004, 229 ff. m.w.N.; zum Hintergrund *Schröter*, DuD 1999, 160. API steht für Application Programming Interface und bezeichnet eine detailliert spezifizierte Softwareschnittstelle für den Zugriff auf bestimmte Funktionen eines (in diesem Fall biometrischen) Programms.
2021 Vgl. *Struif/Scheuermann*, in: Reichl/Roßnagel/Müller 2005, 44 f.

gesicherten Austausch von Emails und andere interoperable Sicherheitslösungen.[2022] Weitere Standards im PKI-Bereich sind XML (für die Signierung beliebiger Dokumente und Teile davon), SSL/TLS (Verschlüsselung von Internet-Transaktionen) und DIN V66291 (Schnittstellen zu Chipkarten mit Signaturanwendungen).

Im Bereich des Gesundheitswesens existieren bislang mehrere Standards für Einzelanwendungen.[2023] Auf europäischer Ebene gibt es Vorschriften für die einheitliche Gestaltung der Daten des Berechtigungsnachweises, die auf die elektronische Gesundheitskarte aufgebracht werden sollen.[2024] Das gilt jedoch vorerst nur für eine drucktechnische Gestaltung, da die Gesundheitskarten in Europa in der ersten Stufe der Einführung die Daten in sichtbarer Form enthalten werden. Die erste Spezifikation für den deutschen elektronischen Heilberufsausweis stammt aus dem Jahre 1999.[2025] Sie beinhaltet fünf Funktionen, nämlich den Sichtausweis, die Speicherung der Ausweisdaten in elektronischer Form, sowie drei separate Schlüsselpaare zur elektronischen Signatur, Authentisierung (zum Beispiel am Praxiscomputer oder im Krankenhaus-Netz), und Verschlüsselung. Die Spezifikation ist mittlerweile in der zweiten Version vom 31. Juli 2003 verfügbar.[2026] Sie enthält bislang sechs Rollen-Definitionen, nämlich je zwei für Ärzte und Apotheker sowie zwei Security Module Cards (SMC). Seit dem 9. Juli 2004 gibt es auch eine Spezifikation für die elektronische Gesundheitskarte. Sie definiert in der zur CeBIT 2005 vorgestellten Version[2027] Kartenkommandos, Algorithmen und Funktionen der COS-Plattform (Teil 1), Basis-Anwendungen und Funktionen der Karte (Teil 2) und den Ablauf des elektronischen Rezepts (Teil 3). Die Standardisierung der gesamten Telematik-Infrastruktur ist seit Beginn des Jahres 2003 in Arbeit. Anlässlich der Messe CeBIT wurde der zuständigen Ministerin *Schmidt* im Frühjahr des Jahres 2004 die Rahmen-[2028] und im Frühjahr des Jahres 2005 die Lösungsarchitektur[2029] übergeben. Die Koordination der Arbeiten liegt seit Beginn des Jahres 2005 bei der neu gegründeten „gematik Gesellschaft für Telematikanwendungen der Gesundheitskarte GmbH", deren Rechtsgrundlage der neue § 291b SGB V bildet.[2030]

2022 Die aktuelle Entwicklung der ISIS-MTT Spezifikation kann unter http://www.teletrust.de/anwend.asp?id=30410&Sprache=E_&HomePG=0 verfolgt werden; s.a. *Fiedler/Bickenbach*, DuD 2005, 149 ff.

2023 Diese sind für eine Reihe von Telematik-Anwendungen noch nicht vereinheitlicht. *Schug/Schramm-Wölk* (2004, 15) sprechen von einem „Wildwuchs von nicht interoperablen Technologien"; s. etwa die Bestandsaufnahme für die elektronische Patientenakte im Sommer des Jahres 2003 bei *ATG/GVG* 2005, 8 ff.; allgemeiner http://www.telematik.biz; eine Übersicht über relevante Normen und Standards für eine Sicherheitsinfrastruktur im Gesundheitswesen (Stand 2001) bietet *ATG/GVG* 2001b, 46 ff.; zu den verschiedenen Aktivitäten vgl. auch *Schug/Schramm-Wölk* 2004, 11 ff.; zum jeweiligen Stand der Lösungsarchitektur s. http://www.dmdi.de.

2024 Auch die *Europäischen Kommission*, KOM(2003) 73, 8 f., fordert ein einheitliches Muster.

2025 Vgl. *Goetz* 2001, 107 ff.; *Warda/Noelle* 2002, 91 ff.; *Reichow/Hartlep/Schmidt*, MedR 1998, 162, 163 ff.

2026 S. *Struif* (Ed.) 2003. Gleichzeitig gibt es Aktivitäten zur Ausarbeitung eines Ausgabemodells, das die Zusammenarbeit zwischen Landesärztekammern und Zertifizierungsdiensteanbietern regeln wird, s. *Secartis/Secunet* 2004; s.a. oben 5.2.2.

2027 S. *Struif* (Ed.) 2005.

2028 Vgl. http://www.heise.de/newsticker/meldung/45879; die Architektur ist unter http://www.dimdi.de/de/ehealth/karte/technik/rahmenarchitektur/index.htm verfügbar.

2029 S. http://www.heise.de/newsticker/meldung/57490; die Ergebnisse sind unter http://www.dimdi.de/static/de/ehealth/karte/technik/loesungsarchitektur/ergebnisse/index.htm abrufbar.

2030 S.a. unten 6.3.4.

6.1.3 Evaluierung und Zertifizierung

Chipkarten und die mit ihnen interagierenden Datenverarbeitungssysteme werden künftig in großem Stil in sensiblen Bereichen eingesetzt werden. Hierfür bestehen technische und rechtliche Anforderungen, die die verwendeten Komponenten erfüllen müssen. Um die Funktionsfähigkeit zu sichern, Fehlinvestitionen zu vermeiden und Datenmissbrauch zu verhindern, ist es erforderlich, die eingesetzte Technik im Vorhinein auf ihre Leistungsmerkmale zu untersuchen. Das gilt umso mehr, als manche Produkte – beispielsweise im Bereich der Biometrie[2031] – die entsprechenden Herstellerangaben nicht immer einhalten.

In dieser Situation ist eine Evaluierung der Eigenschaften und Leistungsmerkmale der Komponenten erforderlich. Diese ist nach Möglichkeit durch unabhängige Institutionen durchzuführen. Das Ergebnis eines solchen Prozesses kann ein Zertifikat sein, welches die gefundenen Ergebnisse bestätigt und aus Herstellersicht ein Mittel der Werbung und Selbstdarstellung sein kann. Eine derartige Bestätigung dient dem Schutz und der Orientierung des Anwenders. Eine Grundbedingung für den Einsatz von Informationstechnologie in sensiblen Datenverarbeitungsbereichen ist deshalb, ausschließlich zertifizierte Komponenten einzusetzen.[2032]

Evaluierungsmaßnahmen können Laboruntersuchungen, Praxistests, groß angelegte Feldversuche und Simulationsstudien[2033] sein. Bei Chipkarten sind Evaluierung und Tests der Kartenkörper, der Mikroprozessoren und der Software erforderlich.[2034] Für biometrische Systeme gibt es mittlerweile eine Reihe von unabhängigen Untersuchungen. Das Bundesamt für Sicherheit in der Informationstechnik hat aus dem Projekt BioIS technische Evaluierungskriterien entwickelt[2035] und die Leistungsfähigkeit von Fingerabdrucksystemen in der Studie BioFinger,[2036] sowie die von Gesichtserkennungssystemen in den Studien BioFace[2037] und BioP I[2038] getestet. Die Folgestudie BioP II behandelt Gesichts-, Fingerabdrucks- und Iriserkennung und wurde im Frühjahr des Jahres 2004 gestartet. Die Arbeitsgruppe 6 des TeleTrusT e.V. hat einen „Kriterienkatalog zur Bewertung der Vergleichbarkeit biometrischer Verfahren“ erstellt.[2039] Das ISO/IES SC 27 beschäftigt sich mit Sicherheitskriterien für biometrische Verfahren, und seine Arbeitsgruppe 3 entwickelt derzeit ein Rahmenwerk zu ihrer standardisierten Prüfung. Insbesondere die US-amerikanische Regierung und das von ihr beauftragte National Institute for Standards and Technology (NIST) führen eine Reihe von Praxistests durch. Einige Vergleichsreihen finden mittlerweile jährlich statt und ermöglichen so eine Beurteilung des technischen

2031 S.o. 4.2.2.4.1.1.

2032 Für den Bereich des Gesundheitswesen s. bereits *BSI* 1995, XIX, 70, 97 f.; s.a. *Struif* (Ed.) 2004, 13; *Konferenz der Datenschutzbeauftragten* 2005.

2033 S. zu diesen ausführlich *Roßnagel/Sarbinowski*, GMD-Spiegel 2/1993, 30 ff., daneben *Pordesch/Roßnagel/Schneider*, DuD 1993, 491 ff.; *Roßnagel/Bizer/Hammer/Kumbruck/Pordesch/Sarbinowski/Schneider* 1994; *Bludau/Buchauer/Roßnagel/Schneider* 1999, 79 ff.; *Roßnagel* 1999, 65 ff.

2034 Näher *Rother* 1998, 251 ff.; *Rankl/Effing* 2002, 577 ff.

2035 *BSI* 2000 (vgl. *Albrecht* 2003a, 60 f.).

2036 *BSI/BKA/IGD* 2004.

2037 *BSI* 2003.

2038 *BSI/BKA/Secunet* 2004.

2039 *TeleTrusT* 2002; zu einem Bsp. für „Best Practices“ beim Testen der Leistungsfähigkeit eines biometrischen Systems vgl. *Biometric Working Group* 2000.

Fortschritts der Systeme.[2040] Problematisch ist allerdings, dass bisher immer noch weltweit einheitliche Testkriterien für biometrische Verfahren fehlen.[2041]

Im Gesundheitswesen wurden im Frühjahr des Jahres 2004 verschiedene Feldtests gestartet. Mehrere Städte und Regionen bewerben sich um den Status als offizielle Testregion.[2042] Sie sollen unterschiedliche Umsetzungsmodelle für die künftige Telematikstruktur erproben. Im Bereich des Einsatzes von Biometrie in Identitätspapieren fehlt dagegen bislang ein groß angelegter Feldversuch. In Anbetracht der beträchtlichen Unsicherheiten über die Leistungsfähigkeit biometrischer Verfahren beim Einsatz mit großen Teilnehmerzahlen ist ein solcher Feldversuch unbedingt erforderlich.[2043] Darin müssten die Fehlerraten, die Handhabbarkeit und die Überwindungssicherheit verschiedener Systeme unter realistischen Bedingungen, das heißt insbesondere mit einem repräsentativen und untrainierten Querschnitt aus der Bevölkerung untersucht werden.[2044]

Als Maßstab für eine unabhängige Zertifizierung können die „Common Criteria for Information Technology Security Evaluation" (CC) nach ISO/IEC 15408 dienen.[2045] Die Common Criteria gliedern sich in drei Teile. Teil 1 führt in das allgemeine Modell und die Vorgehensweise ein. In Teil 2 wird dem Entwickler einen Baukasten mit funktionalen Sicherheitskomponenten zur Verfügung gestellt, die er zur Common Criteria-konformen Modellierung seines Produkts verwenden kann. Teil 3 definiert schließlich Vertrauenswürdigkeitsstufen, die Anforderungen an die Prüfung des Produkts festlegen. Die sieben Stufen (EAL1 bis EAL7)[2046] stellen jeweils eine Vorauswahl an bestimmten Klassen aus Teil 3 der Common Criteria dar. Je höher die Klasse, desto höher sind die Ansprüche an die Prüfung, und desto mehr kann der Anwender in die Korrektheit der implementierten Sicherheitsmaßnahmen vertrauen.

Speziell im Bereich des Datenschutzes besteht die Möglichkeit einer Zertifizierung im Rahmen eines so genannten Datenschutz-Audits.[2047] Im Unterschied zum Bundesrecht, das in § 9a BDSG lediglich dessen Zulässigkeit erwähnt und die näheren Anforderungen einem besonderen Gesetz vorbehält, gibt es auf Länderebene mit dem Datenschutz-Gütesiegel des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein ein erfolgreiches Beispiel für diese Form der Zertifizierung.[2048]

2040 Weitere Bsp. bei *Woodward/Orlans/Higgins* 2003, 184 f.; *Albrecht* 2003a, 61; s.a. oben 4.2.2.4.1.1.

2041 *TAB* 2002, 20; *Albrecht* 2003a, 60 f.; zu Ansätzen vgl. *TAB* 2002, 23 ff.; *Woodward/Orlans/Higgins* 2003, 186 ff.; *Albrecht* 2003a, 60 f.; *Munde* 2002, 145 ff.; *Bolle/Connell/Pankanti/Ratha/Senior* 2004, 105 ff. m.w.N.

2042 Z.B. Flensburg, Trier, Bochum/Essen, Löbau/Zittau, Bremen, Wolfsburg, Ingolstadt sowie das Land Baden-Württemberg (Heilbronn, Zollern-Alb, Tübingen, Rhein-Neckar), s. http://www.aerztezeitung.de/docs/2004/12/13/227a0502.asp; zur Notwendigkeit von Feldversuchen vor dem Einsatz von Telematik im Gesundheitswesen s. *BSI* 1995, 64 f.

2043 S.o. 4.2.2.4.1.1.

2044 Dabei wird nicht übersehen, dass bei groß dimensionierten Tests bis zu einem gewissen Grad die Kontrollierbarkeit der relevanten Faktoren und damit die Vergleichbarkeit der Ergebnisse verloren gehen. Dennoch sind größere Tests als Ergänzung der bisher erfolgten – besser kontrollierbaren – kleineren Studien unbedingt erforderlich.

2045 Zu ersten Ansätzen der Anwendung auf biometrische Systeme vgl. *TeleTrusT* 2002, 21 f.; *Weghaus* 2002, 169 ff.; *Albrecht* 2003a, 62; allgemeine Sicherheitsstandards für den Umgang mit Daten finden sich auch in der ISO/IEC 17799, s. näher *Lincke/Vázques*, K&R 2003, 337 ff.

2046 Die Stufen sind: „funktionell getestet" (EAL1), „strukturell getestet" (EAL2), „methodisch getestet und überprüft" (EAL3), „methodisch entwickelt, getestet und überprüft" (EAL4), „semiformal entworfen und getestet" (EAL5), „semiformal verifizierter Entwurf und getestet" (EAL6), „formal verifizierter Entwurf und getestet" (EAL7).

2047 S. ausführlich *Roßnagel* 2000a; Roßnagel-*ders.*, Kap. 3.7; Simitis-*Bizer*, § 9a Rn. 2 ff.; *Roßnagel/Pfitzmann/Garstka* 2001, 132 ff.

2048 S. http://www.datenschutzzentrum.de/guetesiegel/index.htm; Roßnagel-*Roßnagel*, Kap. 3.7, Rn. 59 ff.

6.2 Besonderheiten des digitalen Personalausweises

Bei der technischen Ausgestaltung des digitalen Personalausweises ist die effektive Umsetzung der datenschutzrechtlichen Anforderungen von großer Bedeutung. Während einige von ihnen (wie das Verbot einer Speicherung biometrischer Daten außerhalb des Ausweises)[2049] keine technischen Probleme aufwerfen, müssen insbesondere für die Sicherung der Daten rechtskonforme Lösungen entwickelt werden. Außerdem ist die organisatorische Zusammenarbeit zwischen Personalausweisbehörden, Ausweishersteller und Zertifizierungsdiensteanbietern zu bewerten.

6.2.1 Sicherung der Daten durch Signatur, Verschlüsselung und Authentisierung

Wenn auf dem digitalen Personalausweis die bisherigen Ausweisdaten und biometrische Merkmale in elektronischer Form gespeichert werden, müssen diese Daten in geeigneter Form gesichert werden.[2050] Das ist im Grundsatz im Interesse von Staat und Bürgern, jedoch mit unterschiedlichen Schwerpunkten. Die kontrollierende Instanz muss sich auf die Integrität und die Authentizität der Daten verlassen können, also sichergehen, dass diese von der ausgebenden Stelle gespeichert und seitdem nicht verfälscht wurden. Das ist auch für den Inhaber wichtig, weil er sich sonst nicht sicher ausweisen kann. Darüber hinaus geht es für ihn um die Vertraulichkeit der Daten, also die Verhinderung des Mitschneidens beim Kontrollvorgang und des Auslesens durch Unberechtigte.

Als Mittel zur Sicherung der Daten kommen die elektronische Signatur, Verschlüsselung und Authentisierung in Betracht, die alle auf asymmetrischen Verschlüsselungsverfahren aufbauen. Sie stoßen beim digitalen Personalausweis aufgrund seines Einsatzes als Reisedokument auf Schwierigkeiten. Da es sich bei der Frage des Zugriffsschutzes jedoch um eine verfassungsrechtliche Anforderung handelt, müssen hier adäquate Lösungen gefunden werden.

6.2.1.1 Signatur der elektronischen Ausweisdaten

Es ist möglich, die Integrität und Authentizität des elektronischen Datensatzes, der biometrische und andere Daten umfassen kann, durch eine elektronische Signatur der ausgebenden Instanz zu schützen.[2051] Dies ist im Rahmen des Herstellungsprozesses technisch unproblematisch. Wenn der Hersteller, beispielsweise die Bundesdruckerei GmbH, den Datensatz im Chip speichert, so kann er ihn auch zuvor hashen, signieren und dann die Signatur ebenfalls im Chip speichern. Hierzu kann eine Institutionskarte des Herstellers in einem automatisierten Verfahren verwendet werden.

Schwieriger ist dagegen die Signaturprüfung. Solange der Personalausweis im rein nationalen Umfeld eingesetzt wird, können die Prüfgeräte auf die Prüfung eines Schlüssels, den des Herstellers, beschränkt werden. Hierfür ist noch nicht einmal eine Online-Abfrage über die Gültigkeit des Zertifikats erforderlich, weil alle Datensätze im gesamten System mit einem einzigen Signaturschlüssel signiert werden. Dieser basiert auf einem einzigen Zertifikat, sodass im Fall der Sperrung eine Mitteilung des Herstellers an die staatlichen

2049 Vgl. oben 4.2.2.4.3.

2050 S.o. 4.2.2.4.6.

2051 S. *Roßnagel/Hornung*, in: Reichl/Roßnagel/Müller 2005, 232 f.; *dies*., DuD 2005, 69, 71. Eine Alternative könnten sog. „digitale Wasserzeichen" sein, s. *Köppen/Schneider*, ebd., 67. Diese Technik ist aber noch nicht ausgereift genug für einen Masseneinsatz und basiert überdies im Unterschied zur elektronischen Signatur auf der Geheimhaltung des verwendeten Verfahren, die jedoch beim weltweiten Einsatz kaum zu gewährleisten ist.

Kontrollinstanzen ausreicht. Auch ein regelmäßiger Austausch des Schlüssels – der im Fall der Kompromittierung die Zahl der auszutauschenden Ausweise entscheidend reduzieren würde – würde nicht zu einer zu hohen Zahl von Zertifikaten führen.[2052]

Im Prinzip ist diese Vorgehensweise auch dann durchführbar, wenn der Personalausweis als Reisedokument eingesetzt wird. Erforderlich ist allerdings eine Verpflichtung aller teilnehmenden Staaten, im Fall der Ungültigkeit eines verwendeten Zertifikats unverzüglich alle anderen Länder zu informieren. In Staatenverbünden, die – wie die Europäische Union – politisch eng kooperieren, erscheint dies praktikabel. Für einen weltweiten Einsatz dürfte es jedoch sinnvoll sein, eine internationale Organisation mit der Informationsübermittlung zu Zertifikaten und Sperrungen zu betrauen. Das gilt insbesondere für den Reisepass, hat jedoch mittelbar auch Auswirkungen auf den Personalausweis, da aus Effizienzgründen eine einheitliche Prüfumgebung für beide Dokumente anzustreben ist.

Die ICAO New Technology Working Group hat ein Modell für ein solches System erarbeitet.[2053] Sie schlägt vor, dass jeder Staat autonom geheime Schlüssel zum Signieren der Ausweisdaten herstellt. Die ICAO soll nicht etwa die Rolle einer Wurzel-Zertifizierungsinstanz übernehmen, sondern lediglich eine Liste mit allen Zertifikaten der Staaten (und ihrer Ausgabestellen) verwalten.[2054] Gleichzeitig wird empfohlen, die Zertifikate durch die ICAO signieren zu lassen. Hierdurch würde die Organisation als eine „de facto"-Zertifizierungsinstanz[2055] für das Gesamtsystem agieren. Sperrt ein Staat ein Zertifikat oder verwendet er ab einem bestimmten Zeitpunkt ein neues, so informiert er innerhalb von 48 Stunden die ICAO, die die Information an alle anderen Staaten weitergibt.[2056]

Eine Zentralstelle in jedem Staat erzeugt Schlüsselpaare und Zertifikate für jede Ausgabestelle innerhalb des staatlichen Territoriums.[2057] Die geheimen Schlüssel werden jedoch nicht an die Ausgabestellen weitergegeben. Der Signiervorgang erfolgt vielmehr, indem diese Zweigstellen – in Deutschland also die Personalausweisbehörden – die Ausweisdaten an die Zentralstelle senden. Dort werden sie mit dem geheimen Schlüssel signiert, der der Ausgabestelle zugeordnet ist. Ist die Zentralstelle gleichzeitig der Hersteller des Reisedokuments, so kann sie den signierten Datensatz im Chip speichern und das Dokument zur Ausgabestelle zurücksenden.

Im Ergebnis würde jeder Ausgabestelle für maschinenlesbare Reisedokumente weltweit ein Signaturschlüsselpaar mit Zertifikat zugeordnet. Alle öffentlichen Schlüssel sollen von der ICAO in einem zentralen Verzeichnis verwaltet werden. Der hierzu erforderliche Aufwand ist allerdings beträchtlich. Allein in Deutschland müssten etwa 6.500 Schlüsselpaare und Zertifikate erstellt werden, die jedoch nicht dezentral, sondern zentral beim Hersteller der Reisedokumente verwahrt und eingesetzt würden. Dies erleichtert die Geheimhaltung der einzelnen Schlüssel, da ansonsten in jeder Ausgabestelle eine Hochsicherheitsumgebung aufgebaut werden müsste. Indes sind überzeugende Gründe dafür, jeder Ausgabestelle überhaupt einen eigenen geheimen Schlüssel zuzuordnen, nicht ersichtlich (und werden von der ICAO auch nicht angeführt). Zwar würde so die Zuordnung eines signierten Ausweisdatensatzes zu einer bestimmten Ausgabestelle erreicht. Diese Information ist jedoch

2052 Die ICAO schlägt den Austausch der Schlüssel alle drei bis fünf Jahre vor, s. *ICAO* 2004d, 26.
2053 *ICAO* 2003b; *dies*. 2004d.
2054 *ICAO* 2003b, 9; s.a. *dies*. 2004d, 8, 12 ff., 28 f.
2055 *ICAO* 2003b, 13.
2056 ICAO 2004d, 13, 27 f.; s.a. *dies*. 2004d, 14.
2057 Das wird von der *ICAO* (2003b, 11) vorgeschlagen. Diese betont allerdings auch, dass das genaue Verfahren Sache der einzelnen Staaten sei. Für die künftige Reisepässe mit biometrischen Daten soll offenbar das BSI die Rolle der Zentralstelle übernehmen, s. http://www.heise.de/newsticker/meldung/59512.

für den Prüfvorgang von untergeordneter Relevanz; hier kommt es vielmehr auf die Integrität und Authentizität der Daten an. Soll dennoch die Ausgabe durch eine bestimmte Stelle für den Prüfenden erkennbar sein, könnte auch die Zentralstelle diese Information bestätigen und in ihre eigene Signatur einschließen. Ein dezentrales PKI-System für die Ausgabestellen ist damit zur Absicherung der biometrischen Daten überflüssig. Hingegen müssen die Personalausweisbehörden über qualifizierte Signaturkarten verfügen, wenn sie elektronische Ausweise ausstellen sollen.[2058] Dies kann jedoch unabhängig von der Signatur der biometrischen Daten und damit von einer Zertifikatsliste der ICAO erfolgen.

Der Technical Report schlägt des Weiteren vor, die elektronische Signatur über den gesamten Inhalt der maschinenlesbaren Zone gemäß ICAO DOC 9303 zu erstrecken.[2059] Die Zone enthält persönliche Daten des Ausweisinhabers und die Seriennummer des Personalausweises. Werden diese Angaben zusammen mit den biometrischen Daten in einer einheitlichen Signatur bestätigt, so wird nicht nur die Integrität des biometrischen Datensatzes, sondern auch seine Zugehörigkeit zu einem bestimmten Ausweis nachgewiesen (logische Integration). Die bisherige maschinelle Prüfung des Reisedokuments in optoelektronischer Form kann so mit der Prüfung der im Chip gespeicherten Daten kombiniert werden. Damit wird ausgeschlossen, dass ein biometrischer Datensatz auf dem Chip ausgetauscht wird. Gleichzeitig ist es bei kontaktlosen Schnittstellen nicht möglich, den Chip des zu prüfenden Ausweises – äußerlich unbemerkt – zu zerstören, einen anderen Chip in die Reichweite des Lesegeräts zu bringen und dieses so zu täuschen.[2060] Da in diesem Fall die signierten Daten nicht mit denen der maschinenlesbaren Zone der Kartenoberfläche übereinstimmen, ist dieser Angriff ausgeschlossen, der ansonsten leicht durchführbar wäre.

6.2.1.2 Authentisierung zwischen Ausweis und Lesegerät

Die elektronische Signatur der im Chip gespeicherten Ausweisdaten sichert die Integrität und Authentizität, nicht jedoch die Vertraulichkeit der Daten. Hierzu könnte ein Verfahren der gegenseitigen Authentisierung zwischen digitalem Personalausweis und Lesegerät eingesetzt werden. Dabei überprüft das Lesegerät die Echtheit des Chips und der Chip, ob das Lesegerät zur Anforderung der Daten berechtigt ist.[2061] Nur wenn beide Prüfungen erfolgreich sind, gibt der Chip die Daten frei. Diese Form der Authentisierung kann gleichzeitig mit dem Aushandeln von Secure Messaging-Schlüsseln verbunden werden, sodass im Anschluss eine verschlüsselte Übertragung der biometrischen Daten ermöglicht wird.[2062]

Auch die gegenseitige Authentisierung setzt allerdings ein welt- oder (für den Personalausweis) zumindest europaweites Vertrauenssystem voraus. Jedes berechtigte Lesegerät muss zertifiziert und mit einer Kennung versehen werden, die von der Chipkarte überprüft werden kann. Dies erfordert eine interoperable Prüfstruktur, die bislang nicht existiert, und deren Realisierbarkeit unklar ist. Möglich wäre, die Authentisierungsschlüsseln zwischen den Staaten in einem ähnlichen Verfahren auszutauschen, wie die ICAO für die Signaturprüfschlüssel vorgeschlagen hat.

2058 S.o. 5.2.1.2.

2059 *ICAO* 2003b, 6; *dies*. 2004d, 15; vgl. für Deutschland die Regelung in § 1 Abs. 3 PersAuswG.

2060 Vgl. zu diesem und anderen Angriffen auf biometrische Systeme oben 4.3.8.1.

2061 S. *Rankl/Effing* 2002, 571; *Struif/Scheuermann/Ullrich/Kraas*, in: Reichl/Roßnagel/Müller 2005, 191; s.a. *Scheuermann*, DuD 2005, 66, 68; eine solche Authentisierung wird etwa beim Ausweis in Hongkong eingesetzt, s.o. 3.2.2.3; entsprechende Überlegungen gibt es beim EU-Reisepass, allerdings nur für die Fingerabdrucks- und nicht für die Gesichtsdaten; vgl. *Kügler*, c't 5/2005, 84, 89.

2062 S. *Struif/Scheuermann*, in: Reichl/Roßnagel/Müller 2005, 170.

Problematisch ist, dass in einem globalen System von zertifizierten Kontrollstellen kaum dauerhaft verhindert werden kann, dass Prüfgeräte gestohlen werden oder sonst abhanden kommen. Zur Lösung dieses Problems werden in Zertifikatssystemen die Zertifikate oder Kennungen derjenigen Geräte gesperrt, die nicht mehr zu Handlungen im System autorisiert sind. Die Wirksamkeit dieses Mechanismus' setzt jedoch voraus, dass vor einem Datenaustausch beide Partner Zugriff auf eine Gesamtliste der Zertifikate haben, ihre Informationen abrufen und diese verarbeiten können. Das ist derzeit für Kartenterminals, nicht jedoch für Chipkarten technisch machbar. Sie verfügen einerseits nicht über genügend Verarbeitungskapazität, andererseits könnten sie eine Online-Verbindung zur Gesamtliste nur vermittelt durch das Lesegerät aufbauen, dessen Echtheit und Berechtigung gerade geprüft werden soll.

Im Ergebnis ist es für die Chipkarte damit nur möglich, die ursprüngliche Berechtigung des Lesegeräts zu überprüfen. Auch diese Form der gegenseitigen Authentisierung stellt allerdings eine deutliche Sicherheitsverbesserung dar. Der Diebstahl eines staatlichen Ausweislesegeräts erfordert eine erhebliche kriminelle Energie, sodass nicht damit zu rechnen ist, dass diese Geräte in großem Stil in Umlauf gelangen. Eine Authentisierungslösung kann zwar nicht gegen den Zugriff eines hoch motivierten Angreifers schützen, wohl aber das für den Ausweisinhaber unmerkliche Auslesen der biometrischen Daten an kontaktlosen Schnittstellen durch beliebige staatliche und private Stellen verhindern. Im Interesse der informationellen Selbstbestimmung ist deshalb ein interoperables Authentisierungssystem zum Schutz der Daten anzustreben.

Als schwächere Methode der gegenseitigen Authentisierung kommt ein alternatives Verfahren in Betracht.[2063] Dabei muss das Lesegerät vor dem Auslesevorgang einen ausweisspezifischen Datensatz an den Chip senden, der aus dem Hashwert über Personalausweisnummer, Vor- und Nachname erzeugt wird. Hierzu muss das Lesegerät diese Daten gespeichert haben. Der Idee nach soll dazu erforderlich sein, diese zuerst optisch aus der maschinenlesbaren Zone des Ausweises auszulesen. Dadurch würde der Auslesevorgang für den Inhaber transparent, weil der Vorgang einen direkten optischen Kontakt zwischen Lesegerät und Personalausweis erfordert. Es wäre beispielsweise nicht mehr möglich, die Daten unmerklich im Vorbeigehen auszulesen.

Das Verfahren bietet jedoch gegenüber einer kryptographischen Authentisierung nur einen erheblich verminderten Schutz. Ein unberechtigter Datenabruf bei Verlust, Erpressung oder Diebstahl wird nicht verhindert. Außerdem sind die Ausweisdaten bei einer Reihe von – gerade staatlichen – Stellen verfügbar. [2064] Wenn etwa ein ausländischer Staat die Daten bei der Einreise speichert, ist es danach möglich, diese auch ohne Kenntnis des Ausweisinhabers kontaktlos abzurufen. Dies setzt zwar voraus, die Datensätze aller Inhaber (oder zumindest derjenigen, die kontrolliert werden sollen) in allen kontaktlosen Lesegeräten zu speichern. Das dürfte derzeit unrealistisch sein. Andererseits muss bei der Einführung einer Basistechnologie wie der Ausgestaltung von Pässen und Personalausweisen die künftige Technikentwicklung mitbedacht werden.

2063 S. z.B. *ICAO* 2004d, 15 f., 21; *Kügler* 2004, 7; *ders.*, c't 5/2005, 84, 88 f. Das im Folgenden beschriebene Verfahren wurde im Auftrag des BSI auch praktisch umgesetzt und getestet, s. näher http://www.bsi.bund.de/literat/faltbl/F25GRT.htm; s.a. http://www.heise.de/newsticker/meldung/59512; vgl. auch die positive Stellungnahme des Chaos Computer Club, http://www.ccc.de/updates/2005/bsipaesse?language=de.

2064 In diesem Sinne etwa die Kritik von *Pfitzmann*, vgl. *Schulzki-Haddouti*, c't 10/2005, 94 f.

6.2.1.3 Verschlüsselung der biometrischen Daten

Die Vertraulichkeit der biometrischer Daten kann auch dadurch hergestellt werden, dass diese auf dem Chip des digitalen Personalausweises verschlüsselt gespeichert werden. Selbst im Fall des Auslesens durch Unberechtigte würde dann ein Missbrauch der Daten verhindert. Die ICAO hat ausdrücklich keine Entscheidungen über eine Verschlüsselung getroffen.[2065] Diese könnte in asymmetrischer und symmetrischer Form geschehen.

Eine asymmetrische Verschlüsselung mit einem individuellen Schlüssel pro Ausweis stößt jedoch auf unüberwindliche Schwierigkeiten in der Praxis. Der geheime Schlüssel zum Entschlüsseln muss entweder im Lesegerät oder im Ausweis verfügbar sein. Eine Speicherung im Lesegerät ist unmöglich, weil dieses die geheimen Schlüssel aller Personalausweise (beziehungsweise aller Reisedokumente weltweit) vorhalten müsste. Wird der Schlüssel im Ausweischip gespeichert, so muss ihn der Inhaber persönlich freischalten. Dies könnte mit Hilfe einer PIN geschehen. Dadurch würde aber der Zugriff auf die elektronisch gespeicherten Daten ohne die Mitwirkung des Karteninhabers unmöglich gemacht. Das ist aus mehreren Gründen für die hoheitliche Identifizierungsfunktion nicht akzeptabel.[2066] In einer Kontrollsituation haben die staatlichen Instanzen ein hohes und legitimes Interesse daran, die Daten auch gegen den Willen des Ausweisinhabers auszulesen. Auch im Fall der Bewusstlosigkeit oder Bewegungsunfähigkeit wäre ein Zugriff nicht möglich. Schließlich besteht die Gefahr des Vergessens der PIN, zumal diese nur sehr selten eingesetzt würde.

Die symmetrische Verschlüsselung weist demgegenüber – ähnlich wie die gegenseitige Authentisierung zwischen Karte und Lesegerät – Sicherheitsprobleme auf. Jede zur Entschlüsselung berechtigte Stelle müsste über den symmetrischen Schlüssel zum Zugriff verfügen. Dies wären in Deutschland nicht nur stationäre Entschlüsselungsgeräte an den Grenzen und in jeder Polizeidienststelle, sondern perspektivisch vermutlich auch eine Vielzahl von mobilen Kontrollgeräten. Die Zahl der europa- und weltweiten Kontrollstellen ist kaum abzuschätzen. Eine derartige Menge von Lesegeräten schließt die dauerhafte Geheimhaltung eines symmetrischen Schlüssels aus.

Aus staatlicher Sicht bedeutet die symmetrische Verschlüsselung damit keine wirkliche Sicherung, da mit entsprechender krimineller Energie (Diebstahl eines Entschlüsselungsgeräts, Erpressung oder Bestechung von Beamten) eine Entschlüsselung möglich ist. Ist diese Energie vorhanden, so dürften auch Straftatbestände in diesem hoheitlichen Bereich kaum einen wirksamen Schutz bedeuten.

Dennoch stellt eine symmetrische Verschlüsselung eine Sicherung für das Grundrecht auf informationelle Selbstbestimmung dar.[2067] Ähnlich wie beim Problem des Abhandenkommens von zertifizierten Lesegeräten[2068] ist nämlich nicht davon auszugehen, dass der Entschlüsselungsschlüssel in der Öffentlichkeit allgemein bekannt wird.[2069] Damit besteht zumindest eine Sicherung gegen ein weit verbreitetes missbräuchliches Auslesen und Verwenden der biometrischen Daten, insbesondere im privaten Umfeld. Selbst wenn das

2065 Vgl. *ICAO* 2004d, 17, 22.

2066 Mit anderem Akzent *Roßnagel/Hornung*, in: Reichl/Roßnagel/Müller 2005, 232 f.

2067 *Roßnagel/Hornung*, in: Reichl/Roßnagel/Müller 2005, 233; *dies*., DuD 2005, 69, 71 f.; *Hornung*, KJ 2004, 344, 358.

2068 Allerdings wären die Probleme einer allgemeinen Verbreitung des Entschlüsselungsschlüssels gravierender als das Abhandenkommen eines einzelnen Lesegeräts, da dann im Grundsatz jedermann Zugriff auf die Daten hätte.

2069 Die Erfahrungen mit dem System der EC-Karte, in dem jeder Geldautomat über den Hauptschlüssel zum Zugriff verfügt, zeigen, dass eine Geheimhaltung jedenfalls nicht völlig unrealistisch ist.

Entschlüsselungsgeheimnis allgemein bekannt werden sollte, wäre seine missbräuchliche Verwendung eine Straftat nach § 202a StGB.[2070] Hierdurch wird ein Abschreckungseffekt erzielt, der eine zusätzliche Sicherung darstellt: Im Unterschied zu einem Angreifer, der sich von der Überwindung einer staatlichen Kontrollstelle erhebliche Vorteile verspricht, ist im nicht-hoheitlichen Bereich kaum damit zu rechnen, dass eine größere Zahl von Tätern das Risiko der Bestrafung eingehen. Aufgrund dessen ist eine Verschlüsselung trotz der genannten Kompromittierungsgefahren zum Schutz der Daten geboten.

6.2.1.4 Verfahren bei Zerstörung des Chips und eintretender Unsicherheit der kryptographischen Sicherungen

Die Sicherheit der Verfahren der elektronischen Signatur, Authentisierung und Verschlüsselung basiert auf der Sicherheit der eingesetzten Algorithmen. Unabhängig davon, welche dieser Methoden (oder welche Kombination von ihnen) zur Sicherung der biometrischen Daten eingesetzt wird, kann deshalb die Vertraulichkeit, Integrität und Authentizität dadurch in Frage gestellt werden, dass die verwendeten Algorithmen nicht mehr unüberwindlich sind. Die Verfügbarkeit kann auch bei Beschädigungen des Chips gefährdet sein. In beiden Fällen fragt sich, ob der Ausweis seine Gültigkeit verliert.[2071] Bestimmungen zur Ungültigkeit von Personalausweisen finden sich in den Ausführungsgesetzen der Länder zum Personalausweisgesetz. Der Ausweis wird danach etwa dann ungültig, wenn die einwandfreie Identitätsfeststellung nicht mehr gegeben ist, der Ausweis unbefugt verändert wurde und zwingend vorgeschriebene Eintragungen fehlen oder nicht zutreffen.[2072]

Ein Gesetz zur Einführung des digitalen Personalausweises würde die Speicherung biometrischer Daten verbindlich vorschreiben. Für den Fall der Zerstörung des Chips oder der Unbrauchbarkeit der auf ihm gespeicherten Daten würde deshalb eine zwingend vorgeschriebene Eintragung fehlen. Dieses Fehlen führt zur Ungültigkeit des Ausweises, ohne dass es auf ein Verschulden des Ausweisinhabers ankommt.[2073] Problematisch ist allerdings, dass dieser im Regelfall nicht erkennen können wird, ob der Chip noch funktionsfähig ist. Die in den Bundesländern normierte Pflicht des Inhabers, den Personalausweis im Fall der Ungültigkeit abzugeben,[2074] muss deshalb restriktiv ausgelegt werden. Sie greift nur dann ein, wenn die Ungültigkeit für den Inhaber erkennbar ist. Dies wird sich regelmäßig erst bei einem erfolglosen Kontrollversuch ergeben. Damit es nicht zu unverhältnismäßigen Beeinträchtigungen kommt, muss der Ausweis in diesem Fall als Sichtausweis akzeptiert werden, das heißt ohne Verwendung der Biometrie. Es sind also nicht nur aus datenschutzrechtlicher Sicht,[2075] sondern auch aufgrund der Eignung zur hoheitlichen Identifikation effektive Rückfallsysteme erforderlich. Denkbar wäre allerdings eine Anordnung, den Ausweis auszutauschen. Diese könnte anlässlich des Kontrollversuchs erfolgen, bei dem die Unbenutzbarkeit der elektronisch gespeicherten Daten festgestellt wird.

Die Unsicherheit darüber, ob die biometrischen Daten aufgrund der nicht mehr gegebenen Eignung der verwendeten Algorithmen noch integer sind,[2076] lässt sich zunächst mit

2070 Bei Handeln gegen Entgelt oder in Schädigungs- oder Bereicherungsabsicht kommt auch § 44 Abs. 1 BDSG in Betracht.
2071 Vgl. hierzu schon *Roßnagel/Gitter/Hornung*, in: Reichl/Roßnagel/Müller 2005, 147.
2072 S. etwa § 5 Abs. 2 LPAuswG Bbg., § 6 LPAuswG Hess., § 5 LPAuswG Rh.-Pf.; vgl. auch *Medert/Süßmuth* 1998, Teil C Rn. 56 ff.
2073 S. für die bisherigen Daten *Medert/Süßmuth* 1998, Teil C Rn. 60.
2074 S.o. 5.2.5 (Fn. 1959).
2075 S.o. 4.2.2.4.7.
2076 Vgl. hierzu bereits oben 5.2.5.

der Unsicherheit der allgemeinen Sicherheitsmerkmale des Ausweises vergleichen. Reichen diese zur Gewährleistung seiner Fälschungssicherheit nicht aus, so werden ab einem bestimmten Zeitpunkt neue Sicherheitsmerkmale eingeführt. Da der Prozess ihrer Kompromittierung graduell abläuft, erfolgt überdies eine kontinuierliche Weiterentwicklung der Merkmale, ohne dass jedoch die schon ausgegebenen Personalausweise von der Einführung neuer Sicherheitsmechanismen an ungültig werden. Das spräche dafür, ein Weiterbestehen der Gültigkeit trotz der Unsicherheit der Algorithmen anzunehmen.

Es fragt sich jedoch, ob dieser Vergleich mit den allgemeinen Sicherheitsmerkmalen zutrifft.[2077] Bei diesen kann die Weiterverwendung der alten Ausweise toleriert werden, weil eine Vielzahl von redundanten Schutzmechanismen gleichzeitig vorhanden ist. Die biometrischen Daten hingegen können zwar durch unterschiedliche Signatur-, Verschlüsselungs- und Authentisierungsverfahren gesichert werden. Diese basieren jedoch durchweg auf kryptographischen Verfahren. Sind diese nicht mehr hinreichend sicher, so besteht auch kein anderweitiger Schutz. Darin liegt ein entscheidender Unterschied zu den allgemeinen Sicherheitsmerkmalen. Überdies kann die Unsicherheit über die Integrität und Authentizität der biometrischen Daten umso weniger toleriert werden, je mehr Gewicht diese Daten in Zukunft bei der Identitätsprüfung erhalten werden. Die Unsicherheit der verwendeten kryptographischen Verschlüsselungs- und Signaturverfahren zum Schutz der biometrischen Daten stellt damit einen Fall der Nichteignung zur einwandfreien Identitätsfeststellung dar. Sie ist der irreparablen Verschmutzung des Papiers vergleichbar und führt im Grundsatz zur Ungültigkeit des Dokuments.[2078] Das schließt nicht aus, dass die Vorlage bei Sichtkontrollen ohne elektronischen Datenabgleich toleriert wird, vergleichbar mit der heutigen Situation, dass ein Ausweis nicht maschinenlesbar ist, der kontrollierende Beamte dies aber nicht feststellen kann, weil er nicht über ein Gerät zum automatisierten Lesen verfügt.

6.2.2 Biometrische Lebenderkennung

Überwindungsversuche mit Fake-Angriffen sind ein Grundproblem jedes biometrischen Systems und können dessen Eignung für die hoheitliche Identifizierung und den Einsatz zum rechtsverbindlichen Handeln mit der elektronischen Signatur in Frage stellen. Bei Fake-Angriffen wird versucht, eine möglichst naturgetreue Abbildung des biometrischen Merkmals herzustellen und so das System zu täuschen. Insbesondere Gesichts-, aber auch Iris- und Fingerabdruckserkennungssysteme sind für diese Form des Angriffs anfällig.[2079] Bei der Gesichtserkennung kann ein Überwindungsversuch mittels Photos, Videos oder Kunstköpfen erfolgen. Eine Irisnachbildung gelingt bisweilen mit Glasaugen, Irisattrappen, Photos oder bedruckten Kontaktlinsen. Mit Hilfe von Gummi- oder Gelatinefingern lassen sich Fingerabdrucksverfahren täuschen; bei einfachen Sensoren genügt hierzu bisweilen sogar ein Fingerabdruck auf Tesafilmstreifen. Wenn die Systeme nicht über Sicherungen gegen derartige Angriffe verfügen, haben diese eine sehr hohe Erfolgswahrscheinlichkeit.[2080]

2077 S. zum Folgenden *Roßnagel/Gitter/Hornung*, in: Reichl/Roßnagel/Müller 2005, 147.

2078 Davon losgelöst ist die Frage, ob bei der Überwindbarkeit der Mechanismen die Kosten der Neuausstellung dem Bürger aufgebürdet werden können; s. dazu unten 6.2.5.

2079 S. zu den folgenden Bsp. *Woodward/Orlans/Higgins* 2003, 140 ff. m.w.N.; *Breitenstein* 2002, 39, 45, 50; *Albrecht* 2003a, 55 m.w.N.; vgl. für die Gesichtserkennung auch *BSI/BKA/Secunet* 2004, 72 f.

2080 In einem Test der Zeitschrift c't wurden im Jahre 2002 sämtliche Systeme mit Fake-Angriffen überwunden, s. *Thalheim/Krissler/Ziegler*, c't 11/2002, 114 ff.

Als Schutzmechanismus werden in der Praxis Verfahren zur Lebenderkennung eingesetzt. Diese sollen prüfen, ob tatsächlich ein biometrisches Merkmal einer lebenden Person präsentiert wird. Beim Finger kann das durch eine Kontrolle von Hautfarbe, Fingerpuls, elektrischer Leitfähigkeit und Reflexen geschehen.[2081] Gesichtserkennungsverfahren können dreidimensionale Gesichtsstrukturen, Augenbewegungen und Blinzeln kontrollieren,[2082] bei der Iris werden kontinuierliche Pupillenbewegungen und Reflexionseigenschaften der feuchten Augenhornhaut (Kornea) gemessen.[2083] Allerdings sind die Verfahren kein Allheilmittel. Die Erfahrung zeigt vielmehr, dass immer neue Angriffe entwickelt werden, die bisher die bestehenden Systeme stets überlistet haben.[2084]

Neben diesen technischen Möglichkeiten der biometrischen Systeme ist die manuelle Kontrolle eine der effektivsten Methoden der Lebenderkennung. Sie kann in jedem Einzelfall durchgeführt werden; möglich ist aber auch die Schaffung einer Kontrollumgebung, in der der Angreifer gegenwärtigen muss, beobachtet zu werden. Letzteres lässt sich beispielsweise durch eine sichtbare Überwachungskamera realisieren. Allerdings wirkt diese Maßnahme nur gegen Angriffe, die mittels Kamera erkennbar sind, also nicht gegen Gummiüberzüge für Finger, bedruckte Kontaktlinsen und gleichartige Vorgehensweisen.

Für den Sonderfall des digitalen Personalausweises ist das Problem der Lebenderkennung danach deutlich entschärft. Sofern eine individuelle Kontrolle durch Sicherheitsbehörden stattfindet, können sich die kontrollierenden Beamten vergewissern, dass keine Attrappe eingesetzt wird. An Massenkontrollstellen an Grenzen und Flughäfen wird allerdings auch erwogen, die Kontrolle auf Verdachtsfälle zu konzentrieren und im normalen Betrieb keine manuelle Überprüfung mehr vorzunehmen, um Kontrollkapazitäten effektiver zu nutzen. Bei einigen der bereits im Einsatz befindlichen Systeme wurde für Personen, die zuvor eine Sicherheitsüberprüfung durchlaufen hatten,[2085] die Möglichkeit geschaffen, die Grenze in vollautomatischen Kontrollschleusen zu passieren. Derzeit gibt es im Rahmen der Beratungen der ICAO Pläne, für Reisende mit unterschiedlichem „risk level" verschiedene Kontrollprozeduren einzuführen.[2086] Sollte ein solches Verfahren ohne manuelle Überprüfung auch beim digitalen Personalausweis für einen Teil der Bevölkerung eingesetzt werden (was neben den hier beschriebenen technischen Schwierigkeiten zu massiven Akzeptanzproblemen führen dürfte),[2087] müssten die biometrischen Systeme eine Lebenderkennung garantieren.

Insgesamt lässt sich festhalten, dass das Problem im Bereich staatlicher Identifikationsdokumente deutlich abgemildert ist. Das stellt sich für eine denkbare Signaturfunktion anders dar.[2088] Hier ist die Lebenderkennung eines der hauptsächlichen Sicherheitsprobleme. Eine Freischaltung der Signaturkarte mittels biometrischen Systemen führt bei qualifizierten Signaturverfahren zu weitreichenden Haftungsrisiken für den Signaturschlüssel-Inhaber. Deshalb können derartige Verfahren nur dann zugelassen werden, wenn sie eine überwindungssichere Lebenderkennung garantieren. Folglich muss jeder Ort, an dem signiert wird, also insbesondere der heimische PC des Nutzers, mit entsprechenden Senso-

2081 *TAB* 2002, 14.
2082 *Breitenstein* 2002, 45; *Albrecht* 2003a, 55.
2083 *Breitenstein* 2002, 50; s.a. *Woodward/Orlans/Higgins* 2003, 142 ff.
2084 *Bromba* 2004, unter 6; s.a. *Konferenz der Datenschutzbeauftragten* 2002, unter 4. Ein Problem bei der technischen Umsetzung ist der relativ hohe Zeitbedarf der Lebenderkennung, s. *Woodward/Orlans/Higgins* 2003, 147.
2085 So konzentrierte sich das – mittlerweile tlw. eingestellte – US-amerikanische INSPASS auf Vielflieger (in der Regel Geschäftsreisende). Personen mit Vorstrafen waren ausgeschlossen.
2086 Vgl. http://www.icao.int/icao/en/atb/fal/fal12/documentation/fal12ip007_en.pdf.
2087 S.u. 7.3.3.1.
2088 Zum Einsatz von Biometrie zur Freischaltung des Signaturschlüssels vgl. oben 5.2.6.

ren ausgerüstet werden. Außerdem besteht die große Herausforderung darin, auf der Signaturkarte einen Prüfmechanismus zu installieren, der sichergestellt, dass die Karte ausschließlich Daten akzeptiert, die von derartigen Sensoren erfasst und zwischen Sensor und Kartenchip nicht manipuliert wurden. Dies kann bislang noch nicht garantiert werden. Hierin liegt einer der Hauptgründe dafür, dass noch keinem biometrischen Verfahren eine der PIN gleichwertige Sicherheit attestiert wurde.

6.2.3 Kontaktlose oder kontaktorientierte Schnittstelle

Wenn der digitale Personalausweis zu Kontrollzwecken mit Peripheriesystemen interagiert, kommen grundsätzlich kontaktorientierte, kontaktlose und kombinierte (Dual Interface-) Schnittstellen in Betracht, wobei aufgrund der langen Lebensdauer des Personalausweises von vornherein nur passive kontaktlose Chips (die nicht über eine eigene Stromversorgung verfügen) einsetzbar sind.[2089] Ein Chip mit kontaktloser Schnittstelle ließe sich in das bisherige laminierte Format integrieren.[2090] Er ist allerdings wegen der Transparenzprobleme grundsätzlich datenschutzrechtlich schlechter zu bewerten als kontaktorientierte Chips.[2091]

Aus technischer Sicht wird die Wahl der Schnittstelle von mehreren Anforderungen beeinflusst. Kontaktorientierte Systeme haben eine kürzere Lebensdauer als RF-Chips, weil die Kontakte offen liegen und deshalb durch Verschmutzung oder Verschleiß in ihrer Funktionsfähigkeit beeinträchtigt werden können.[2092] Kontaktlose Chips lassen außerdem deutlich höhere Übertragungsraten zu. Dies verkürzt die Dauer des Kontrollvorgangs. Je nach Größe des biometrischen Datensatzes wirkt sich das signifikant auf den Investitionsbedarf an Kontrollstellen aus. Der Vorteil kontaktorientierter Schnittstellen liegt in der höheren Sicherheit: Ein einfaches Mitschneiden der übertragenen Daten und deren Manipulation ist deutlich erschwert. In Hochsicherheitsanwendungen sollten deshalb immer Kontaktschnittstellen verwendet werden.

Aus diesem Grund gibt es bislang keinen kontaktlosen Chip, der zur Verwendung in einer sicheren Signaturerstellungseinheit zertifiziert ist. Nur solche zertifizierten Komponenten dürfen jedoch zur Erstellung qualifizierter elektronischer Signaturen eingesetzt werden. Die Entscheidung für eine Signaturfunktion des digitalen Personalausweises impliziert deshalb zugleich eine Entscheidung für eine kontaktorientierte Schnittstelle und – da diese nur bei einer genormten Lage der Kontakte einsetzbar ist – den Wechsel des Formats auf die Chipkarte. Denkbar ist es, für die biometrischen Daten einen separaten Chip mit kontaktloser Schnittstelle einzubringen oder einen Dual Interface-Chip zu verwenden, auf dem sowohl die Signaturschlüssel als auch die biometrischen Daten gespeichert sind.[2093] Auch in diesem Fall ist jedoch wegen der Signaturfunktion die Verwendung einer Chipkarte erforderlich.

Das Chipkartenformat kann für den digitalen Personalausweis bei einem Wohnortswechsel zu Schwierigkeiten führen. Bislang wird in diesem Fall ein Adressaufkleber auf dem Ausweiskörper angebracht; von diesen Aufklebern gibt die Bundesdruckerei jährlich ca. 6 Millionen Stück ab. Das bisherige Verfahren ist problematisch, wenn die Karte häufig

2089 *ICAO* 2004b, 10; vgl. zum Folgenden auch *Struif/Scheuermann*, in: Reichl/Roßnagel/Müller 2005, 167 ff.

2090 Daneben würde auch eine weitgehende technische Übereinstimmung mit den Visa-Aufklebern erzielt, die in Zukunft ebenfalls mit biometrischen Daten ausgestattet werden sollen.

2091 S.o. 4.2.2.4.5.

2092 S. *ICAO* 2004b, 9.

2093 So die Empfehlung von *Struif/Scheuermann*, in: Reichl/Roßnagel/Müller 2005, 167 f., 294.

in Chipkartenleser eingeführt wird, weil der Aufkleber dabei abblättern kann. Als Lösung bieten sich unterschiedliche Varianten an.[2094] Ein Adressaufkleber kann zunächst auf einem Bereich der Karte aufgebracht werden, der – soweit das Kartenlesegerät das zulässt – nicht in das Gerät eingeführt wird. Das ist auch beim Chipkartenformat unter Einhaltung der Standards der ICAO möglich, wenn auf vorgesehene Zusatz-Optionen wie Magnetstreifen, Barcodes oder optische Speicher verzichtet wird.[2095] Alternativ könnte auf dem Ausweis ein Bereich unterhalb der Adresse frei bleiben. Bei einem Umzug würde die alte Adresse per Lasergravur ausgestrichen und die neue in den freien Bereich eingetragen. Da dieser begrenzt ist, kann dieses Verfahren zwar nicht beliebig wiederholt werden. Es dürfte aber praktikabel sein, an die Bürger einen neuen Personalausweis abzugeben, die während des Gültigkeitszeitraums des Ausweises häufiger umziehen. Schließlich ist auch ein Verzicht auf die optische Speicherung und die lediglich elektronische Ablage denkbar.[2096] Dies würde es auch erleichtern, die Adressdaten zu verändern.

Aus Herstellersicht ist eine Umstellung auf eine Chipkarte relativ leicht zu bewerkstelligen: Die Bundesdruckerei GmbH produziert bereits Personalausweise in diesem Format für andere Staaten. Es ist jedoch möglich, dass der Wechsel zu einer Kostenerhöhung des Gesamtsystems „Personalausweis“ führt. Sollte diese erheblich sein, wäre sie gegen die Vorteile abzuwägen, die ein signaturfähiger Personalausweis bietet.[2097] Im Ergebnis dürften diese Gesichtspunkte gegenüber den Argumenten der Kostenerhöhung überwiegen, sofern diese nicht zu groß ist. Die Entscheidung hängt letztlich maßgeblich von den Rahmenbedingungen ab, insbesondere der Verfügbarkeit anderer Signaturkarten und Anwendungen zum tatsächlichen Zeitpunkt der Einführung.

6.2.4 Organisationsfragen

Die Einführung eines allgemeinen digitalen Personalausweises bringt eine Reihe von organisatorischen Fragen mit sich, bei deren Umsetzung die Anforderungen an eine sichere und datenschutzgerechte Ausgestaltung zu beachten sind. Hierbei ist zwischen den biometrischen Merkmalen und der Signaturfunktion zu unterscheiden.[2098]

6.2.4.1 Biometrische Daten

Um die personalausweisrechtlich erforderliche Zuordnung des Ausweises zum richtigen Individuum zu garantieren, ist eine Hochsicherheitsumgebung beim biometrischen Enrolment erforderlich.[2099] Eine solche Umgebung zu installieren, ist insbesondere für große Benutzergruppen schwierig.[2100] Die Einrichtung einer einzigen, zentralen Stelle für die Digitalisierung der biometrischen Daten würde eine Erleichterung bedeuten, verlangt jedoch die Übermittlung einer hochwertigen Abbildung des Merkmals an die zentrale Stelle. Bei der Gesichtserkennung ist dies denkbar. Hier wird zurzeit ein Bild an die Bundesdruckerei GmbH versandt, das mit Blick auf die biometrische Weiterverarbeitung opti-

2094 S. *Roßnagel/Gitter/Hornung*, in: Reichl/Roßnagel/Müller 2005, 239.
2095 Vgl. *Struif/Scheuermann*, in: Reichl/Roßnagel/Müller 2005, 181.
2096 Diese Lösung wird es beim belgischen Personalausweis geben, s.o. 3.2.1.3.
2097 S. *Roßnagel/Gitter/Hornung/Strasser*, in: Reichl/Roßnagel/Müller 2005, 319 ff.; oben 2.1.1.
2098 Vgl. zum Folgenden ausführlich *Strasser/Müller/Roßnagel/Gitter*, in: Reichl/Roßnagel/Müller 2005, 243 ff.; s.a. *Gitter/Strasser*, DuD 2005, 74, 76 f.
2099 S.a. *Strasser/Müller/Roßnagel/Gitter*, in: Reichl/Roßnagel/Müller 2005, 244 ff.
2100 *TAB* 2002, 10.

miert werden könnte.[2101] Auch beim Fingerabdruck könnte ein Papierbild an den Hersteller übermittelt werden.[2102] Für die Iris ist dagegen eine dezentrale Digitalisierung unumgänglich.

Auch bei Gesicht und Fingerabdruck kann aus einem anderen Grund nicht auf eine Ausstattung der Personalausweisbehörden mit biometrischen Erkennungssystemen verzichtet werden.[2103] Um sicherzugehen, dass der Personalausweis an den richtigen Inhaber ausgegeben wird, ist ein Vergleich der im Chip gespeicherten Daten mit der Person erforderlich, die den Ausweis abholt. Im Rahmen der Ausweisherstellung gibt es nämlich keine Möglichkeit, die Zugehörigkeit biometrischer Daten zum Antragsteller zu kontrollieren. Es besteht deshalb die Gefahr, dass über eine Einspeisung falscher Daten – absichtlich oder irrtümlich – falsche Identitäten hergestellt werden. Der Test ist auch im Interesse des Inhabers, weil nur so eventuelle Fertigungsfehler erkannt werden, die sonst bei einer späteren Kontrolle zu Problemen führen können.

Infolgedessen führt kein Weg am Aufbau einer entsprechenden dezentralen Infrastruktur in den Personalausweisbehörden vorbei. Deren Zahl beträgt derzeit über 6.500 und liegt damit erheblich unter der der Städte und Gemeinden, von denen es in Deutschland 16.121 gibt.[2104] Andererseits verfügen die Personalausweisbehörden – auch dort, wo sie in der Gemeinde angesiedelt sind – in aller Regel über eine Zahl von Zweigstellen, Bürgerbüros oder ähnliche Einrichtungen, in denen bislang ein Personalausweis beantragt werden kann. Über die Gesamtzahl dieser Stellen gibt es, soweit ersichtlich, keine Statistik. Die Zahl der Standorte, die zum Enrolment ausgerüstet werden muss, ist aber in jedem Fall deutlich höher als die Zahl der Personalausweisbehörden.[2105] Sie könnte nur durch eine Zentralisierung der Erfassung reduziert werden. Beispiele hierfür gibt es aus dem Ausland: Oman bewerkstelligt die Ausgabe seiner Ausweise an ca. 2,7 Millionen Bürger mit nur zwölf Registrierungs- und Ausgabestellen. Gegen eine derartige Organisation – die in Deutschland lediglich etwa 360 Stellen für das gesamte Bundesgebiet erfordern würde – sprechen Argumente der Bürgernähe und -freundlichkeit. Schon die Reduzierung auf eine einzige Antragsstelle pro Personalausweisbehörde wäre mit erheblichen Belastungen für die Bürger verbunden. Insbesondere in den Landkreisen und Verwaltungsgemeinschaften der Flächenländer wären weite Strecken für die Antragstellung und die Ausgabe zurückzulegen.

Eine Alternative hierzu könnte die Einrichtung mobiler Einheiten zum Enrolment sein. Es ist zwar fraglich, ob bei diesen die erforderlichen Sicherheitsstandards garantiert werden können. Auf der anderen Seite muss in jedem Fall eine Lösung für Bürger gefunden werden, die wegen körperlicher Behinderungen oder aus anderen Gründen nicht persönlich in der Personalausweisbehörde erscheinen können.[2106] Bisher ist es nach Landesrecht beispielsweise möglich, dass der Antragsteller bei schweren körperlichen Gebrechen durch einen Behördenmitarbeiter in seiner Wohnung oder in einem Krankenhaus aufgesucht

2101 Das würde insbesondere eine Frontalaufnahme anstelle des bisherigen Halbprofilbildes erfordern, s. *BSI/BKA/Secunet* 2004, 9 f.

2102 *TAB* 2004, 7.

2103 Vgl. *Roßnagel/Gitter/Hornung*, in: Reichl/Roßnagel/Müller 2005, 149.

2104 Vgl. *Wohlfarth*, RDV 2002, 231. Die kleinere Zahl ergibt sich aus den Zuständigkeitsregelungen der Länder, die die Behörden tlw. in Verwaltungsgemeinschaften ansiedeln, s.o. 2.2.1.3 (Fn. 158).

2105 Das bleibt unerwähnt in den Kostenberechnungen von *Booz Allen Hamilton/Bundesdruckerei/ZN Vision* 2003 (zitiert nach *TAB* 2004, 62 ff.).

2106 S.a. *Struif/Scheuermann/Küblbeck/Heusinger/Ronge/Schneider/Kitamura*, in: Reichl/Roßnagel/Müller 2005, 77 f.

wird.[2107] Deshalb muss zumindest eine geringe Anzahl mobiler Erfassungsgeräte zur Verfügung gestellt werden.

Bei einer dezentralen Merkmalserhebung müssen die Personalausweisbehörden die materiellen und personellen Ressourcen für das Enrolment bereitstellen. Außerdem sind eine vollständige Digitalisierung des Verfahrens und die Bereitstellung eines sicheren Datenübertragungsweges zwischen Behörde und Hersteller erforderlich. Hier gibt es mit dem DIGANT-Verfahren bereits ein von der Bundesdruckerei GmbH entwickeltes System, das auch in der Praxis eingesetzt wird. Im März des Jahres 2005 übermittelten jedoch erst 3.000 der ca. 6.500 Personalausweisbehörden die Daten in elektronischer Form,[2108] während in einer Vielzahl von Behörden noch keine Schnittstelle zu dem System bestand.

Die Daten des bisherigen Ausweises werden nach § 2a Abs. 1 PersAuswG bei den Personalausweisbehörden in Personalausweisregistern gespeichert. Eine – technisch machbare – Speicherung auch der weiteren biometrischen Merkmale ist datenschutzrechtlich unzulässig.[2109] Insofern muss keine Änderung des Registers und seiner Abläufe erfolgen.[2110]

Im Betriebsstadium benötigt jede Stelle, die die biometrischen Daten kontrollieren soll, eine Matching-Einheit. Dies ist für die stationären Grenz- oder Flughafenstellen relativ leicht umsetzbar. Je nach Zahl der zu kontrollierenden Personen und Dauer des Kontrollvorgangs müssen dabei allerdings eine größere Zahl von Geräten vorgehalten werden. Ein für die US-Regierung erstelltes Gutachten empfiehlt beispielsweise, auch für Grenzübergänge mobile biometrische Geräte an Warteschlangen einzusetzen, um die Wartezeiten zu minimieren.[2111] Hierdurch würde die Zahl der Geräte deutlich erhöht.

Erst recht würde die Ausstattung einer Vielzahl von Polizeistreifen schnell zu enormen Kosten führen. Ob diese Investitionen sinnvoll sind, muss auf der Basis einer Kosten-Nutzen-Analyse bewertet werden, die Sicherheitsgewinne und finanziellen Aufwand gegeneinander abwägt. Dabei ist zu berücksichtigen, dass Polizeistreifen zurzeit nicht über ein Lesegerät für die maschinell lesbaren Zonen des Personalausweises verfügen, sondern diesen lediglich im Rahmen von Sichtkontrollen nutzen. Sogar stationäre Kontrollstellen wie Polizeibehörden untersuchen Ausweisdokumente häufig nur mit Hilfe von Lupen und UV-Lampen, ohne eine Überprüfung mittels eines automatischen Lesers durchzuführen. Werden diese Verfahren beibehalten, reduzieren sich auch die Kosten.[2112] Bestehen im Rahmen einer Sichtkontrolle Zweifel über die Identität, können zentrale Kontrollgeräte in Polizeidienststellen genutzt werden. Falls die Zahl der Zweifelsfälle gering ist, kann sogar auf die Geräte der Personalausweisbehörden zurückgegriffen werden.

Eine letzte Organisationsfrage stellt sich schließlich hinsichtlich der Beteiligung der Bundesdruckerei GmbH am Verfahren. Vorstellbar wäre, die Herstellung des digitalen Personalausweises in einem Vergabeverfahren auszuschreiben, an dessen Ende auch die Beauftragung eines anderen Bewerbers stehen könnte.[2113] Dieser müsste allerdings eine gleichwertige Sicherheit des Herstellungsprozesses und des Endproduktes garantieren. Neben diesen faktischen Aspekten würde eine Beauftragung einer anderen Stelle die Ände-

2107 S. z.B. Nr. 3.1.2 der hessischen Durchführungsverordnung, StAnz Hess. 2002, 3171.

2108 Zum jeweils aktuellen Stand s. http://www.bundesdruckerei.de/de/behoerde/3_1/index.html.

2109 Vgl. oben 4.2.2.4.3; s.a. *Roßnagel/Hornung*, in: Reichl/Roßnagel/Müller 2005, 135 ff.

2110 Die technisch-organisatorische Gestaltung des Personalausweisregisters bleibt damit weiterhin Sache der jeweiligen Personalausweisbehörde (s. bisher *Medert/Süßmuth* 1998, § 2a Rn. 4).

2111 *International Biometric Group* 2003, 11.

2112 Im Gegensatz zur Auffassung von *Koch* (2002, 22) muss deshalb auch künftig nicht jeder Polizeibeamte über ein Gerät zur Prüfung der biometrischen Merkmale verfügen.

2113 Für den Personalausweis wäre auch eine Beauftragung mehrerer Bewerber zulässig. Gemäß Art. 3 Abs. 2 der Verordnung (EG) Nr. 2252/2004 (s.o. 3.1.2) dürfen die Mitgliedstaaten der EU jedoch für den Reisepass nur eine einzige Stelle mit der Herstellung betrauen.

rung von Normen erfordern. Zwar findet sich im Personalausweisrecht keine ausdrückliche Bestimmung, die die Herstellung des Ausweises der Bundesdruckerei GmbH zuweist. Diese wird jedoch in einer Vielzahl von Verfahrensvorschriften erwähnt. So darf nach § 3 Abs. 3 Satz 1 PersAuswG eine zentrale, alle Seriennummern umfassende Speicherung nur bei der Bundesdruckerei GmbH und ausschließlich zum Nachweis des Verbleibs der Ausweise erfolgen. Der Aufdruck „Bundesdruckerei" auf dem gegenwärtigen Personalausweises steht nicht im Ermessen des Herstellers, sondern wird durch die Anlage 1 zur Personalausweismusterverordnung[2114] verbindlich vorgeschrieben. Auch einige Landespersonalausweisgesetze[2115] und Durchführungsverordnungen[2116] nehmen auf die Bundesdruckerei GmbH Bezug. Aufgrund dieser Regelungen hat die Bundesdruckerei GmbH nach geltendem Recht das Herstellungsmonopol für den Personalausweis inne.[2117] Soll dies in Zukunft geändert werden, müsste eine neutrale Formulierung dieser Vorschriften erfolgen.

6.2.4.2 Signaturfunktion

Falls der digitale Personalausweis mit einer Signaturfunktion ausgerüstet werden sollte, muss ein Organisationsmodell für die Zusammenarbeit zwischen Personalausweisbehörden und Zertifizierungsdiensteanbietern entwickelt werden. Da aus signatur- und datenschutzrechtlicher Sicht eine Vielzahl von Modellen zulässig ist,[2118] handelt es sich nicht nur um ein rechtliches, sondern auch um ein verwaltungs- und betriebswirtschaftliches Problem.[2119]

Sinnvoll ist, bei den Tätigkeiten des Zertifizierungsdiensteanbieters zwischen technologieabhängigen und technologieunabhängigen Aufgaben zu unterscheiden. Technologieabhängige Aufgaben sind solche, die auf der Basis unterschiedlicher technischer Methoden erbracht werden können; technologieunabhängige Aufgaben werden dagegen von unterschiedlichen Anbietern im Wesentlichen einheitlich erledigt. Konkurrieren mehrere Methoden für die Erbringung einer technologieabhängigen Aufgabe miteinander, so steht zu erwarten, dass sich einerseits die beste Lösung am Markt durchsetzt, andererseits jeder Anbieter bestrebt ist, seine eigene Lösung kontinuierlich weiterzuentwickeln. Deshalb sollten technologieabhängige Aufgaben nach Möglichkeit nicht in einem standardisierten staatlichen Verfahren, sondern durch konkurrierende private Anbieter erfüllt werden. Bei technologieunabhängigen Aufgaben sind diese negativen Effekte dagegen nicht zu erwarten, da sie auch bei einem funktionierenden Wettbewerb von allen Anbietern mehr oder weniger identisch erbracht werden.

Im Rahmen der Tätigkeit eines Zertifizierungsdiensteanbieters sind die Registrierung des Antragstellers, die Aushändigung der sicheren Signaturerstellungseinheit und die Unterrichtung über Sicherheitsmaßnahmen bei der Signaturerstellung und -prüfung technologieunabhängige Aufgaben.[2120] Diese erfordern zwar nach neuer Rechtslage nicht mehr einen direkten Kontakt zum Signaturschlüssel-Inhaber, ein solcher Kontakt ist im Interesse

2114 Verordnung zur Bestimmung der Muster der Personalausweise der Bundesrepublik Deutschland v. 2. 7.1986, BGBl. I 1986, 1009, zuletzt durch Art. 4 V des Gesetzes v. 3.12.2001, BGBl. I, 3274.

2115 Vgl. z.B. § 11 LPersAuswG Rh.-Pf.

2116 S. etwa Nr. 3.1.1, 4.1, 4.2, 6, 7.3, 9.2, 11.5, 13.2 der hessischen Bestimmungen, StAnz Hess. 2002, 3171.

2117 S.a. BVerwG, Urt. v. 21.2.1995 – Buchholz 402.02 PersAuswG Nr. 8.

2118 S.o. 5.2.2 und 4.3.6.2.2.2.

2119 S. zum Folgenden *Strasser/Müller/Roßnagel/Gitter*, in: Reichl/Roßnagel/Müller 2005, 260 ff., 268 ff.; *Gitter/Strasser*, DuD 2005, 74 ff.

2120 Vgl. *Strasser/Müller/Roßnagel/Gitter*, in: Reichl/Roßnagel/Müller 2005, 370 f.; s.a. *Gitter/Strasser*, DuD 2005, 74, 76 f.

der Rechtssicherheit jedoch wünschenswert.[2121] Deshalb bietet sich eine Übernahme durch die Personalausweisbehörden an. Schlüsselerzeugung, Personalisierung, Zertifizierung, Verzeichnis- und Sperrdienst sind dagegen technologieabhängig. Sie sollten den Zertifizierungsdiensteanbietern überlassen werden, um einen technischen Innovationswettbewerb zu ermöglichen.

Falls die Personalausweisbehörden auf diese oder eine ähnliche Art nur mit einzelnen Zertifizierungsdiensteanbietern kooperieren, hat dies Auswirkungen auf den Wettbewerb zwischen den Anbietern.[2122] Um wettbewerbsrechtliche Probleme zu vermeiden, sind die technologieunabhängigen Aufgaben deshalb allen Zertifizierungsdiensteanbietern gleichermaßen anzubieten. Durch die Berechnung eines angemessenen Entgelts für dieses Angebot werden auch beihilferechtliche Vorgaben erfüllt.

6.2.5 Kosten

Die Kosten des digitalen Personalausweises sind einerseits für die politische Entscheidung über die Einführung wichtig; andererseits handelt es sich um eine Frage der Verhältnismäßigkeit, weil die Bundesregierung beispielsweise für den Reisepass bereits angekündigt hat, die Kosten – deren Höhe sie im Januar des Jahres 2005, also neun Monate vor dem zu diesem Zeitpunkt genannten Einführungstermin, nicht angeben konnte – in vollem Umfang den Antragstellern aufzuerlegen.[2123] Wo die Grenze der Unverhältnismäßigkeit liegt, wird im Einzelfall schwer zu beurteilen sein. Sie würde aber auf jeden Fall deutlich überschritten, falls für den Einzelnen (so Mutmaßungen für den Pass im Januar 2005)[2124] Kosten bis zu 300 Euro entstehen sollten.

Es ist derzeit schwer möglich, die Kosten der Einführung eines digitalen Personalausweises abzuschätzen. Die hauptsächlichen Kostenfaktoren sind dagegen erkennbar:[2125]

- Mitentscheidend ist zunächst die Wahl des biometrischen Merkmals, weil die Preise für die Geräte zum Enrolment und zur Kontrolle erheblich variieren. Unter den drei Merkmalen, die zurzeit hauptsächlich in Erwägung gezogen werden (Gesicht, Iris und Fingerabdruck) ist die Iris das mit Abstand teuerste Merkmal. Einerseits sind die Kosten der Kontrollgeräte höher, andererseits gibt es bislang nur einen einzigen Patentinhaber weltweit (*John Daugman*), sodass die Gefahr einer technologischen Abhängigkeit bestünde.[2126] Sollte sich erweisen, dass biometrische Daten des Gesichts sich schneller verändern als die anderer Merkmale, könnte das zu einer Laufzeitverkürzung und damit zu höheren Ausgaben führen. Auch eine Kombination von zwei oder gar drei Merkmalen würde die Kosten in die Höhe treiben.
- Ein weiterer Faktor ist die Zahl der Stellen, in denen ein Enrolment erfolgt (Ausstellungsebene). Diese Stellen müssen mit den entsprechenden Geräten ausgerüstet werden, für die Anschaffungskosten und Platzbedarf in den Behörden anfallen. Au-

2121 S.o. 5.2.2.

2122 S. dazu *Roßnagel/Gitter*, in: Reichl/Roßnagel/Müller 2005, 160 ff.; *Gitter/Strasser*, DuD 2005, 74, 76.

2123 Vgl. die Antwort auf die Kleinen Anfrage der FDP-Fraktion im Januar 2005, BT-Drs. 15/4616, 5 f.

2124 S. http://www.heise.de/newsticker/meldung/55233. Die Bundesregierung dementiert das als „völlig aus der Luft gegriffen", s. http://www.heise.de/newsticker/meldung/ 55110. Ende Mai 2005 wurde ein Preis von 59 Euro bekannt gegeben, s. http://www.heise.de/newsticker/meldung/60149.

2125 Vgl. zum Folgenden auch *Strasser/Müller/Roßnagel/Gitter*, in: Reichl/Roßnagel/Müller 2005, 243 ff.; *ICAO* 2004a, 29; *LSE* 2005, 6 f.

2126 Das wird außer Acht gelassen von *Booz Allen Hamilton/Bundesdruckerei/ZN Vision* 2003 (zitiert nach *TAB* 2004, 65), wo lediglich darauf abgestellt wird, dass die zu erwarteten Hardwarekosten für Fingerabdrucks-, Iris- und Gesichtserkennungssysteme nur um ca. 12 % voneinander abweichen.

ßerdem sind die Bediensteten – offenbar ca. 35.000 Personen[2127] – zu schulen. Zwar ist die zentrale Erfassung der biometrischen Merkmale die deutlich günstigere Variante. Aufgrund der Notwendigkeit, die Funktionsweise der fertigen Ausweise zu testen, müssen die Personalausweisbehörden jedoch in jedem Fall über biometrische Geräte verfügen. Es ist damit zu rechnen, dass die Antragstellung aufgrund des Enrolments mehr Zeit als bislang in Anspruch nehmen wird. Selbst wenn dieses – was sehr optimistisch erscheint – nur zehn Sekunden dauern sollte,[2128] kommt noch die verlängerte Dauer bei der Ausgabe hinzu. Beides erhöht den Personalbedarf.

- Auch die Stellen, an denen Kontrollen durchgeführt werden, müssen mit Prüfgeräten ausgestattet werden. Inwieweit sich darüber hinaus ein zusätzlicher Personalbedarf ergibt, hängt von den Möglichkeiten einer automatisierten Kontrolle ab. In jedem Fall müssen für die Mitarbeiter, die mit der Kontrolle befasst sind, entsprechende Schulungen durchgeführt werden. Die Kostenabschätzung von *Booz Allen Hamilton/Bundesdruckerei/ZN Vision*[2129] geht von insgesamt lediglich 400 Kontrollstationen an Flughäfen, Landgrenzen und Seehäfen aus. Eine Ausrüstung aller 2.800 INPOL-berechtigten Datenstationen des BGS[2130] würde zu einer deutlichen Erhöhung der dort geschätzten Kosten führen. Das gilt in noch stärkerem Maße, falls auch Polizeistationen einbezogen und mobile Kontrollen ermöglicht würden.
- Zu den Anschaffungskosten kommen laufende Ausgaben für die Wartung der biometrischen Geräte und technische Verbesserungen.
- Die Form der Speicherung bestimmt die Kosten des einzelnen Ausweises. Am kostengünstigsten wäre die Verwendung optisch aufgedruckter Daten, die im Rahmen dieser Arbeit jedoch nicht erörtert wird, da sie aufgrund zu hoher Fehlerraten zur biometrischen Verifikation nicht geeignet ist.[2131] Nach Schätzungen würden für sie nur einmalig 21,2 Millionen Euro und laufende Kosten von 4,5 Millionen Euro anfallen.[2132] Der Unterschied zwischen kontaktlosen und kontaktbehafteten Systemen spielt demgegenüber – die erforderliche dezentrale Ausrüstung der Personalausweisbehörden vorausgesetzt – für die einmaligen Kosten im Rahmen des Herstellungsprozesses nur eine untergeordnete Rolle (geschätzt werden 613,7 gegenüber 668,7 Millionen Euro).[2133] Allerdings ist die kontaktbehaftete Variante bei den geschätzten laufenden Kosten mit 610,2 Millionen Euro pro Jahr fast doppelt so teuer wie die kontaktlose Speicherung (331,5 Millionen Euro).[2134] Problematisch ist insbesondere, dass die Umstellung auf das Chipkartenformat eine Abkoppelung des Herstellungsprozesses von dem der Plastikkarte bedeuten würde, die bislang in den Reisepass eingenäht wird und in Bezug auf den Herstellungsprozess und die Sicherheitsmerkmale (wenn auch nicht in Bezug auf die enthaltenen Daten) mit dem

2127 S. http://www.heise.de/newsticker/meldung/59512.
2128 *Booz Allen Hamilton/Bundesdruckerei/ZN Vision* 2003, 80 (zitiert nach *TAB* 2004, 38). Für die Gesichtserkennung sind nach anderen Angaben (*OECD* 2004, 25) allein 30 Sekunden für die Aufnahme der Bilder erforderlich.
2129 2003, 126 ff. (abgedruckt bei *TAB* 2004, 62 ff.).
2130 *Strasser/Müller/Roßnagel/Gitter*, in: Reichl/Roßnagel/Müller 2005, 247.
2131 *BSI/BKA/Secunet* 2004, 9 f., 53.
2132 *Booz Allen Hamilton/Bundesdruckerei/ZN Vision* 2003 (zitiert nach *TAB* 2004, 71 f.).
2133 *Booz Allen Hamilton/Bundesdruckerei/ZN Vision* 2003 (zitiert nach *TAB* 2004, 70, 75).
2134 *Booz Allen Hamilton/Bundesdruckerei/ZN Vision* 2003 (zitiert nach *TAB* 2004, 72, 76).

Personalausweis identisch ist.[2135] Eine Trennung könnte die Produktionskosten erhöhen. Falls die Chipkarte über andere Sicherheitsmerkmale als der Reisepass verfügen sollte, müssten an Kontrollstellen überdies unterschiedliche Prüfgeräte für beide Dokumente verfügbar sein.

- In den Berechnungen von *Booz Allen Hamilton/Bundesdruckerei/ZN Vision* wurden mögliche Kosten für eine Absicherung der biometrischen Daten durch elektronische Signatur und Verschlüsselung explizit nicht berücksichtigt.[2136] Die Begründung, dieser Aufwand könne „nicht direkt dem biometrischen System zugeordnet werden", ist indes nicht zutreffend. Wenn eine Absicherung der Daten sowohl im staatlichen Interesse ist (Sicherung der Integrität und Authentizität der Daten) als auch dem datenschutzrechtlich notwendigen Schutz der Vertraulichkeit der Daten des Ausweisinhabers dient, so stehen die Kosten für derartige Maßnahmen selbstverständlich im direkten Zusammenhang mit der Einführung biometrischer Daten im Ausweis. Dies führt zu einer Erhöhung der Kosten, die in der Studie genannt werden.
- Wenn der digitale Personalausweis eine Signaturfunktion beinhaltet, müssen die Personalausweisbehörden personelle Ressourcen bereitstellen, falls sie Aufgaben im Rahmen des Antrags- und Ausgabeprozesses übernehmen. Hierfür ist allerdings eine Vergütung durch die Zertifizierungsdiensteanbieter denkbar, da diese die Kosten für die Erbringung der Aufgaben in einem eigenen Prozess oder durch einen anderen Dienstleister (bislang regelmäßig die Deutsche Post AG im Postident-Verfahren) ersparen.
- Die Kosten für die Zertifikatsvergabe und -verlängerung sowie für sonstige Zertifizierungsdienstleistungen verursachen für den Staat keine Kosten, weil die Signaturfunktion freiwillig sein und (wie bei bisherigen Signaturkarten) von den Karteninhabern bezahlt werden wird. Eine qualifizierte Signaturfunktion erfordert jedoch einen leistungsfähigeren Chip, der aus Sicherheitsgründen über eine kontaktorientierte Schnittstelle verfügen muss. Beides verteuert die Herstellung gegenüber einer Lösung, bei der nur biometrische Daten gespeichert werden. Andererseits dürfte diese Variante insgesamt billiger sein als die Verbreitung separater Signaturkarten. Nach Angaben des Branchenverbandes BITKOM aus dem Jahre 2002 würde eine Signaturfunktion die Herstellung des Ausweises lediglich um 5 Euro verteuern.[2137]
- Eine eventuelle Veränderung der Laufzeit des Ausweises würde sich signifikant auf die Kosten auswirken. Kontaktschnittstellen haben eine eher geringere Lebensdauer, da sie durch den direkten physischen Kontakt mehr beansprucht werden. Die Verwendung von Biometrie kann wegen der fehlenden Erkenntnisse über die Langzeitstabilität der Merkmale für eine Verkürzung der Laufzeit sprechen. Gleiches gilt beim Einsatz von PKI, weil die Sicherheit der Algorithmen kaum über einen Zeitraum von zehn Jahren gesichert werden kann. Die ICAO bemüht sich darum, diese Laufzeit – die international üblich ist – beizubehalten,[2138] hat aber gleichzeitig den Staaten empfohlen, bei der Verwendung von Chips eine fünfjährige Gültigkeit zu erwägen.[2139] Für Deutschland würde dies – was etwa in der Studie des Büros für

2135 Eine kontaktlose Variante könnte demgegenüber nicht nur mit dem Reisepass, sondern auch mit den zukünftigen Visa-Aufklebern, die ebenfalls biometrische Daten enthalten sollen, einheitlich ausgestaltet werden.

2136 *Booz Allen Hamilton/Bundesdruckerei/ZN Vision* 2003 (zitiert nach *TAB* 2004, 64).

2137 S. Presseerklärung des BITKOM, Frankfurter Rundschau v. 15.10.2002.

2138 *ICAO* 2004b, 5.

2139 *ICAO* 2004a, 40, 47.

Technikfolgenabschätzung aus dem Jahre 2004 unerwähnt bleibt – eine Verdoppelung der Kosten bei Beantragung, Produktion und Ausgabe des Gesamtausweissystems bedeuten. Dieser Faktor wirkt unabhängig von der Ausgestaltung des Ausweises und der entsprechenden Prozesse und könnte deren Einfluss auf die Gesamtkosten entscheidend überlagern.

Insgesamt dürften die Kosten eines digitalen Personalausweises erheblich sein. So wird beispielsweise die Umsetzung des neuen biometrischen US-amerikanischen Visa-Programms nach Schätzungen des dortigen Rechnungshofs 15 Milliarden USD kosten.[2140] Die britische Regierung plant, zur Kostendeckung für die kombinierte Ausgabe des neuen Reisepasses und des geplanten Personalausweises eine Gebühr von insgesamt 122 Euro zu erheben.[2141]

In Deutschland würden sich die Kosten des Personalausweises auf mehrere Körperschaften verteilen. Die Träger der Personalausweisbehörden (also im Regelfall die Gemeinden) hätten den überwiegenden Teil der Kosten des Antrags- und Ausgabeverfahrens zu übernehmen. Bereits heute ist die Gebühr von acht Euro (§ 1 Abs. 6 Satz 1 PersAuswG) – die überdies bei Bedürftigkeit und bei der erstmaligen Ausstellung an unter 21jährige nicht erhoben wird – nicht kostendeckend. Durch die Bereitstellung von Geräten, Personal und Räumlichkeiten würden weitere Belastungen entstehen. Auch eine Verteuerung des Herstellungsprozesses würde – vorbehaltlich einer Erhöhung der Gebühr – zu Lasten der Gemeinden gehen, da diese den Ausweis bei der Bundesdruckerei GmbH bezahlen müssen. Für andere Körperschaften fallen vor allem Kosten für Prüfgeräte an: Der Bund hätte die Grenzkontrollstellen auszurüsten, während die Ausstattung der Polizeistationen Sache der Länder wäre.

Auch im privaten Bereich könnten Investitionskosten anfallen. Bislang verbietet § 4 Abs. 3 PersAuswG hier zwar die Verwendung von elektronisch im Ausweis gespeicherten Daten, eine Änderung der Norm ist jedoch denkbar und bei Einrichtung technischer Schutzvorkehrungen zulässig.[2142] In diesem Fall würde sich das Infrastrukturproblem auch bei privaten Einrichtungen stellen. Für Institutionen, die – wie Kreditinstitute – auf eine sichere Identifizierung ihrer Geschäftspartner angewiesen sind, dürften sich die entsprechenden Investitionen lohnen.

Ein nicht zu unterschätzendes „worst case"-Szenario ergibt sich schlussendlich aus der Gefahr einer schlagartigen Unsicherheit der verwendeten kryptographischen Algorithmen. In diesem Fall müssen die Ausweise ausgetauscht werden, da die kontrollierenden Stellen sich nicht mehr auf die Integrität der Daten verlassen können und diese nicht mehr gegen missbräuchlichen Zugriff geschützt sind. Da der Bürger keinen Einfluss auf die technische Sicherheit hat, wäre es auch unzulässig, ihn mit den Kosten der Neuausstellung zu belasten. Daraus resultiert ein erhebliches finanzielles Risiko des Staates.

6.3 Besonderheiten der elektronischen Gesundheitskarte

Die rechtlichen Anforderungen zur Gewährleistung der Vertraulichkeit der auf und mittels der elektronischen Gesundheitskarte gespeicherten Daten zum Schutz ihrer Zweckbindung und zur Ermöglichung eines abgestuften Zugriffs im Einzelfall stellen eine große Herausforderung für die Einrichtung der Telematik-Infrastruktur im Gesundheitswesen dar. In einigen Bereichen ergeben sich verschiedene Umsetzungsmöglichkeiten, die im

2140 S. http://futurezone.orf.at/futurezone.orf?read=detail&id=223693&tmp=78277.
2141 Vgl. http://www.heise.de/newsticker/meldung/52899.
2142 S.o. 4.2.2.5.

Folgenden erörtert werden. Überdies stellt sich wie beim Personalausweis die Frage der Verhältnismäßigkeit der Kosten.

6.3.1 Datensicherheit

Da die elektronische Gesundheitskarte viel stärker als der digitale Personalausweis mit Peripheriesystemen interagiert, stellen sich die Datensicherheitsprobleme in Teilbereichen anders dar. Das Zusammenwirken beschränkt sich nicht auf das Auslesen von Daten durch Lesegeräte, sondern betrifft auch die Zugangsfunktion zu Daten, die in Serversystemen gespeichert werden. Infolgedessen sind zur Umsetzung der datenschutzrechtlichen Anforderungen Maßnahmen zur Sicherung der Daten nicht nur im Chip der Karte, sondern auch in externen Datenbanken und auf den Übermittlungswegen zu implementieren. Wegen der hohen Sensibilität der Daten ist im Gesundheitswesen auf eine Datenübertragung über das Internet zu verzichten und stattdessen ein gesichertes Intranet aufzubauen.[2143] Dazu sind keine separaten Leitungen erforderlich; stattdessen kann ein Virtuelles Privates Netz (VPN)[2144] verwendet werden.

Die Daten auf Servern sind sicher zu verschlüsseln. Der Zugang zu Datenverarbeitungsanlagen ist mit Passwörtern oder biometrischen Systemen zu sichern und der physische Zutritt zu den Verarbeitungsbereichen durch bauliche Maßnahmen zu erschweren. Durch Verschlüsselungsverfahren kann eine Kenntnisnahme durch die speichernden und übermittelnden Stellen (inklusive deren Administratoren) ausgeschlossen oder zumindest erschwert werden. Bei einer externen Datenhaltung oder -übertragung im Gesundheitswesen sind deshalb immer derartige Verfahren erforderlich.[2145]

Die gespeicherten Daten müssen überdies gegen Angriffe gesichert sein, die über Netzwerkanbindungen geführt werden. Hierzu sind in der speichernden Stelle bei den Rechnern, die nicht physisch von Datenleitungen nach außen getrennt sind, geeignete Firewalls einzusetzen.[2146] Das ist insbesondere wichtig, wenn Daten in Pull-Verfahren Dritten zur Verfügung gestellt werden, die Benutzer sie also (nach erfolgter Autorisierung) selbständig abrufen.[2147]

Aufgrund der Gefahren für das Recht auf informationelle Selbstbestimmung ist auf den Aufbau zentraler Speicherstellen für die Gesundheitsdaten grundsätzlich zu verzichten. Zwar hätte diese Form der Speicherung Vorteile gegenüber einer verteilten Datenhaltung, bei der die Verfügbarkeit des Gesamtsystems von der der Subsysteme abhängt.[2148] Denkbar wäre deshalb eine zentrale Speicherstruktur für solche Daten, die unter großem Zeit-

---

2143 *BITKOM/VDAP/VHitG/ZVEI* 2003, 67; *Jürgens* 2003, unter 4.4.1.4; Roßnagel-*Schirmer*, Kap. 7.12, Rn. 101.

2144 S. näher *Martius* 2000, 9 ff. m.w.N.; *Tanenbaum* 2003, 840 ff.; vgl. für das Gesundheitswesen auch *Schwetlick* 2004, 30 ff.; *Goldschmidt/Goetz/Hornung*, mdi 2/2004, 61, 66.

2145 *Konferenz der Datenschutzbeauftragten* 1995a; Richtlinien der *BÄK*, DÄ 1996, A-2809, 2812; *Wehrmann/Wellbrock*, CR 1997, 754, 748; *Der Hamburgische Datenschutzbeauftragte* 1998, 78; *Hermeler* 2000, 105; *Bultmann/Wellbrock/Biermann/Engels/Ernestus/Höhn/Wehrmann/Schurig* 2002, 19; *Schaar*, RDV 2003, 59, 66; *Jürgens* 2003, unter 2.3; *BITKOM/VDAP/VHitG/ZVEI* 2003, 7, 55 f.

2146 *Hermeler* 2000, 105 f.; *Jürgens* 2003, unter 2.3; *GDD* 2002, 120 ff. Mit Firewalls lassen sich auch abgestufte logische Zugriffskontrollen implementieren, s. *BITKOM/VDAP/VHitG/ZVEI* 2003, 58 f.; zur technischen Funktionsweise vgl. *Tanenbaum* 2003, 837 ff.

2147 *Goetz* 2001, 125 f. Bei Push-Verfahren, die einen selbständigen aktiven Versand einer verantwortlichen Stelle beinhalten, ist es leichter möglich, Anlagen vom Netz abzuschotten, die Daten speichern.

2148 *Bultmann/Wellbrock/Biermann/Engels/Ernestus/Höhn/Wehrmann/Schurig* 2002, 22. Besondere Probleme ergeben sich, sofern eine Übermittlung zwischen Leistungserbringern im Einzelfall erfolgen muss, da dann eine Abhängigkeit von Praxisöffnungszeiten besteht. Eine derartige Struktur liegt jedoch außerhalb des Systems der Gesundheitskarte.

druck ständig verfügbar sein müssen. Auf der anderen Seite haben diese Daten, bei denen es sich regelmäßig um Notfallinformationen handeln wird, ohnehin keinen so großen Speicherbedarf, dass sie nicht auch auf der elektronischen Gesundheitskarte selbst abgelegt werden könnten. Für Anwendungen ohne Zeitdruck ist es akzeptabel, mögliche Verzögerungen durch einen (seltenen) Ausfall von Subsystemen hinzunehmen, weil ein erheblicher datenschutzrechtlicher Gewinn erzielt werden kann.

Häufiger als der Ausfall von Servern dürfte das Problem auftreten, dass einer der Beteiligten seine Chipkarte nicht verfügbar hat oder diese nicht funktionstüchtig ist. Auch die lokale Infrastruktur, insbesondere die Kartenlesegeräte, können defekt sein. Am „einfachen" Beispiel des Verfahrensablaufs beim elektronischen Rezept lassen sich die Anforderungen an die Verfügbarkeit demonstrieren. Dieser Ablauf setzt voraus, dass drei Beteiligte (der Versicherte, der behandelnde Arzt und der Apotheker) ihre Chipkarte zur Hand haben, Arzt und Apotheker die PIN erinnern und alle Karten funktionsfähig ist. Darüber hinaus müssen der Praxiscomputer des Arztes und der des Apothekers, bei der Serverlösung darüber hinaus auch die Netzwerkverbindungen und Server einsatzbereit sein. Ist dies nicht vollständig zu gewährleisten, müssen alternative Verfahren bereitgestellt werden. Beim Rezept kann folglich auf das papierbasierte Verfahren kaum völlig verzichtet werden.[2149] Überdies ist eine Lösung für die Rezeptausstellung bei Hausbesuchen erforderlich.[2150] Soll auch diese mittels der elektronischen Gesundheitskarte erfolgen, müssen Ärzte, die Hausbesuche vornehmen, neben den stationären Lesegeräten in den Praxen auch über mobile Dual-Slot Lesegeräte verfügen, die eine gegenseitige Authentisierung von Gesundheitskarte und elektronischem Heilberufsausweis ermöglichen.

Bei der Verschlüsselung der Gesundheitsdaten ist zu differenzieren. Solange nur eine Stelle Daten (auf eigenen Datenträgern oder bei externen Dienstleistern) speichert und wieder abruft, kann mit symmetrischer Verschlüsselung gearbeitet werden. Werden jedoch Daten mit Hilfe der elektronische Gesundheitskarte zwischen mehreren Leistungserbringern übermittelt, so muss zwischen gerichteter und ungerichteter Kommunikation unterschieden werden.

Im Fall der gerichteten Kommunikation steht der Empfänger der Daten bereits fest, wenn der Absender diese erstellt. Beispiele aus dem Gesundheitswesen sind der elektronische Arztbrief an einen bereits feststehenden Empfänger und die Übermittlung eines Untersuchungsergebnisses an einen Leistungserbringer, der die Untersuchung in Auftrag gegeben hat.[2151] Auch der Versand an eine Institution oder Abteilung ist eine gerichtete Kommunikation. Um diese Form der Übermittlung zu ermöglichen, kann eine Hybridverschlüsselung verwendet werden, bei der die Daten symmetrisch verschlüsselt und danach der dabei verwendete Verschlüsselungsschlüssel (Session-Key) mit dem öffentlichen Schlüssel des Empfängers (oder der empfangenden Institution) asymmetrisch verschlüsselt werden.[2152] Das verschlüsselte Dokument und der Session-Key werden dann an den Empfänger versandt. Dabei ist auch eine Übermittlung an mehrere Empfänger problemlos zu bewerkstelligen: Hierzu muss nicht das gesamte Dokument, sondern lediglich der Session-Key mit dem öffentlichen Schlüssel des weiteren Empfängers neu verschlüsselt werden. Für die gerichtete Kommunikation im Gesundheitswesen in verschlüsselter Form existiert das so genannte HCP (Health Care Professionals')-Protokoll, das Lösungen für die Au-

2149 *BITKOM/VDAP/VHitG/ZVEI* 2003, 61; *ATG/GVG* 2001a, 24.
2150 *Warda/Noelle* 2002, 121.
2151 *BITKOM/VDAP/VHitG/ZVEI* 2003, 49 f.
2152 S. im Einzelnen oben 2.3.2.

thentisierung, Transportverschlüsselung und Nicht-Abstreitbarkeit im Rahmen der Datenübermittlung bietet.[2153]

Bei der ungerichteten Kommunikation entscheidet nicht der Absender, sondern ein Dritter (später) darüber, wer Zugriff auf die Daten haben soll. Ein Anwendungsfall ist die Überweisung an einen Spezialisten, bei der der Versicherte aufgrund der freien Arztwahl einen beliebigen Leistungserbringer wählen kann. Gleiches gilt für das elektronische Rezept (das in einer beliebigen Apotheke einzulösen ist), den elektronischen Arztbrief an einen noch nicht feststehenden Empfänger und die Krankenhauseinweisung.[2154] In diesen und ähnlichen Situationen, die im Gesundheitswesen überwiegen,[2155] ist das beschriebene asymmetrische Verfahren nicht anwendbar. Hier muss die Gesundheitskarte als Sicherungsmittel eingesetzt werden, sodass ein Zugriff zwar mit einem beliebigen elektronischen Heilberufsausweis, aber nur mit der einmaligen Gesundheitskarte des Versicherten möglich ist.

Praktisch kann eine solche ungerichtete Kommunikation folgendermaßen abgewickelt werden:[2156] Der zu übermittelnde Datensatz erhält eine einmalige Vorgangskennung und wird mit einem ebenfalls einmaligen symmetrischen Schlüssel verschlüsselt. Kennung und Schlüssel werden in einem geschützten Speicherbereich der elektronischen Gesundheitskarte abgelegt. Danach wird das symmetrisch verschlüsselte Dokument mit dem asymmetrischen Schlüssel eines Servers verschlüsselt, an diesen übermittelt und dort (in der ursprünglichen, das heißt symmetrisch verschlüsselten Form) gespeichert. Der Versicherte begibt sich im Anschluss zu dem Leistungserbringer seiner Wahl. Dieser authentifiziert sich mit Hilfe seines elektronischen Heilberufsausweises. Sodann gibt der Versicherte mit seiner PIN die Vorgangskennung und den symmetrischer Schlüssel aus der Gesundheitskarte zum Auslesen frei. Anschließend wird eine elektronische Anfrage an den Server erstellt, die die Vorgangskennung enthält. Mit ihrer Hilfe wird das entsprechende Dokument auf dem Server ermittelt, mit dem öffentlichen Schlüssel des anfragenden Leistungserbringers verschlüsselt und an diesen übermittelt. Der Leistungserbringer formt die Daten unter Verwendung des symmetrischen Schlüssels in den ursprünglichen Klartext um. Eine solche Art der Übermittlung ermöglicht es dem Versicherten, frei über den Empfänger der Daten zu entscheiden; gleichzeitig ist es an keiner Stelle des Übertragungsweges (insbesondere nicht auf dem Server) möglich, die Daten einzusehen, weil nur der Karteninhaber über den symmetrischen Schlüssel verfügt.

Eine Alternative zu diesem Ablauf besteht dann, wenn die elektronische Gesundheitskarte über einen sicheren asymmetrischen Verschlüsselungsmechanismus verfügt. In diesem Fall kann der symmetrische Schlüssel mit dem öffentlichen Schlüssel des Versicherten verschlüsselt und den Daten beigefügt anstatt auf der Gesundheitskarte selbst gespeichert zu werden. Der Versicherte kann dann beim jeweiligen Leistungserbringer den symmetrischen Schlüssel entschlüsseln und zur Verfügung stellen. Mit dieser Ende-zu-Ende-Verschlüsselung wird jeder Zugriff durch Serverbetreiber und andere Dritte zuverlässig ausgeschlossen.

Neben diesen Techniken zur Garantie der Vertraulichkeit der Kommunikation sind Maßnahmen erforderlich, die Datenverarbeitungsvorgänge nachweisbar festhalten, um eine datenschutzrechtliche Kontrolle dieser Vorgänge zu ermöglichen und die Nichtabstreitbar-

2153 Mit der Entwicklung wurde 1998 begonnen; s. *Goetz* 2001, 114 ff.; *Warda/Noelle* 2002, 139 ff.

2154 *BITKOM/VDAP/VHitG/ZVEI* 2003, 50; *Warda/Noelle* 2002, 16.

2155 *Warda/Noelle* 2002, 59; *Grätzel v. Grätz* 2004c, 132.

2156 Vgl. zum Folgenden *Bultmann/Wellbrock/Biermann/Engels/Ernestus/Höhn/Wehrmann/Schurig* 2002, 28 f.; *Warda/Noelle* 2002, 143 ff.; *Grätzel v. Grätz* 2004c, 133; *Goldschmidt/Goetz/Hornung*, mdi 2/2004, 61, 66 f.

keit von Datenübermittlungen, insbesondere in Haftungsfällen, zu bewirken.[2157] Bei verteilten Systemen im Gesundheitswesen ist zur Protokollierung eine Kombination verschiedener Verfahren nötig. Systemweite Aktionen wie Übermittlungen zwischen verschiedenen Beteiligten können im System festgehalten werden.[2158] Das ist bei lokalen Aktionen wie Zugriffen vor Ort (beispielsweise auf Server, die nicht über Netzverbindungen erfolgen, und auf die elektronische Gesundheitskarte) nicht möglich, sodass es einer lokalen Protokollierung bedarf.[2159]

Eine der größten Herausforderungen für den Einsatz von Telematik im Gesundheitswesen wird die Langzeitaufbewahrung elektronischer Dokumente unter Verwendung qualifizierter elektronischer Signaturen sein.[2160] Die Telematik-Expertise der Wirtschaft beschränkt sich hierzu für das Gesundheitswesen auf den allgemeinen Verweis, es seien bereits Archivierungsverfahren verfügbar.[2161] Demgegenüber muss aber betont werden, dass bislang keine Erfahrungen mit der Aufbewahrung über die Zeiträume bestehen, die im Gesundheitswesen vorgeschrieben sind. Die Mindestaufbewahrungsfrist für die ärztliche Dokumentation beträgt nach § 10 Abs. 3 MBO-Ä 2004 zehn Jahre. Daneben bestehen gesetzliche Vorschriften.[2162] So schreibt § 15 Abs. 1 TPG eine Aufbewahrung von mindestens zehn, § 14 Abs. 3 Satz 1 Transfusionsgesetz von mindestens fünfzehn Jahren vor. Gemäß § 28 Abs. 3 Satz 1 RöV sind Aufzeichnungen über Röntgenbehandlungen nach der letzten Behandlung 30 Jahre lang aufzuheben. Nach § 42 Abs. 1 Satz 2 StrlSchV müssen Aufzeichnungen über die Strahlenbelastung nach den §§ 40, 41 StrlSchV sogar so lange aufbewahrt werden, bis die überwachte Person das 75. Lebensjahr vollendet hat oder vollendet hätte, mindestens jedoch 30 Jahre nach Beendigung der jeweiligen Beschäftigung. Schließlich archivieren viele Leistungserbringer bereits heute aus beweistechnischen Gründen die Dokumente für 30 Jahre.[2163]

Wenn die Dokumentation mit Hilfe qualifizierter elektronischer Signaturen erfolgen soll, so müssen die archivierten Daten und die verwendeten Signaturen nach § 17 SigV immer wieder neu signiert werden.[2164] Für ein Verfahren, das dies datenschutz- und signaturgesetzkonform und für große Archive effektiv ermöglicht, wurde bisher erst ein Prototyp in dem Forschungsprojekt ArchiSig entwickelt.[2165] Um diesen Ansatz zu einem verlässlichen Archivierungssystem fortzuführen, sind noch große Anstrengungen erforderlich.

Schließlich dürfen die allgemeinen Sicherheitsanforderungen an die elektronische Gesundheitskarte nicht zu gering sein. Da auf die Daten ohnehin nur unter Verwendung eines (hochsicheren und mit qualifizierten Signaturverfahren ausgerüsteten) elektronischen Heilberufsausweises zugegriffen werden kann, könnte man zwar erwägen, geringere Stan-

---

2157 Die Kontrollierbarkeit der Datenverarbeitung ist (neben der Durchsetzung von Betroffenenrechten) ein Grundproblem dezentraler und verteilter Datenspeicherung, s. *Bizer* 2002, 22.

2158 Bei Übermittlungen zwischen Leistungserbringern ohne jede zentrale Struktur wäre dagegen ein Quittungsverfahren unter Verwendung elektronischer Signaturen erforderlich, s. *Bultmann/Wellbrock/Biermann*/*Engels/Ernestus/Höhn/Wehrmann/Schurig* 2002, 25 f.

2159 Der Zugriff auf die Karte ist gemäß § 291a Abs. 6 Satz 2 SGB V zu protokollieren, s.o. 4.2.3.4.2.3.

2160 *Goetz* 2001, 55; *Jürgens* 2003, unter 2.4; zu den rechtlichen Problemen bereits *Kilian*, NJW 1987, 697 ff.

2161 *BITKOM/VDAP/VHitG/ZVEI* 2003, 55, 59 f.

2162 S.a. die Bsp. bei *Laskaridis* 2003, 228 ff.

2163 S. *Inhester*, NJW 1995, 685, 688; *Bäumler*, MedR 1998, 400, 4001; *Hermeler* 2000, 28; *GDD* 2002, 38.

2164 S. zu dieser Norm RMD-*Roßnagel/Pordesch*, § 17 SigV, Rn. 1 ff.

2165 Vgl. *Roßnagel/Fischer-Dieskau/Pordesch/Brandner*, CR 2003, 301 ff.; *Brandner/Pordesch*, DuD 2003, 354 ff.; *Fischer-Dieskau/Roßnagel/Steidle*, MMR 2004, 451 ff.; s.a. http://www.archisig.de → Ergebnisse.

dards genügen zu lassen. Es wäre dann jedoch möglich, diese nicht sichere Gesundheitskarte bei jedem Arztbesuch, aber auch bei Verlust durch einen beliebigen Heilberufsausweis auszuspähen. Das ist angesichts der hohen Sensibilität der Daten nicht akzeptabel. Entsprechend geht auch die Gesetzesbegründung zum GKV-Modernisierungsgesetz davon aus, dass die elektronische Gesundheitskarte ein als sicher zertifiziertes Betriebssystem erhalten wird.[2166]

6.3.2 Anonymisierung und Pseudonymisierung

Im Unterschied zum digitalen Personalausweis sind im System der elektronischen Gesundheitskarte Verfahren der Anonymisierung und Pseudonymisierung denkbar.[2167] Anonyme Daten können zur medizinischen Forschung und zur Gewinnung von Strukturdaten eingesetzt werden. Das stößt dann an Grenzen, wenn über einen längeren Zeitraum hinweg bestimmte Individuen beobachtet werden sollen. Kommt es bei dieser Beobachtung nicht auf den einzelnen Versicherten, sondern nur auf die Zusammenführung der zu ihm gehörenden Daten unter einer exakten Kennung an, so sind Pseudonyme zu verwenden. Bei diesen Anforderungen handelt es sich um ein allgemeines Problem der Datenverarbeitung im Rahmen der medizinischen Forschung und der Kontrolle des Gesundheitswesens. Das gilt auch für die Anordnung einer Pseudonymisierung von Leistungs- und Abrechnungsdaten durch die Arbeitsgemeinschaft für Aufgaben der Datentransparenz in § 303c Abs. 1 und 2 SGB V.[2168]

Pseudonymisierungsverfahren können auch beim Aufbau einer elektronischen Patientenakte verwendet werden. In der Telematik-Expertise wird dazu folgendes System vorgeschlagen (so genanntes „dreistufiges Sicherheitskonzept für Directory"):[2169] Im Rahmen eines Behandlungsfalls werden zunächst die Identität des Versicherten und die des Leistungserbringers miteinander verknüpft. Beide identifizieren sich mit ihrer jeweiligen Chipkarte. Diese erste Verknüpfung wird als Eintrag separat gespeichert. Im zweiten Schritt erfolgt eine Verknüpfung des Leistungserbringers mit dem konkreten „Geschäftsvorfall". Auch dieser Eintrag wird separat gespeichert. Der erste Eintrag verweist mit einem Pointer auf den zweiten, aber nicht umgekehrt. Das dritte Datenobjekt sind die eigentlichen Daten des Geschäftsvorfalls, also die Behandlungsinformationen. Auf diese wird mit Hilfe eines Pointers des zweiten Eintrags verwiesen, auch hier findet jedoch keine umgekehrte Verknüpfung statt. Im Ergebnis ist nur der erste Eintrag mit der Identität des Versicherten verknüpft, während es mit großer Sicherheit unmöglich ist, aus den Daten eines konkreten Geschäftsvorfalls auf einen Patienten zurückzuschließen.

6.3.3 Umsetzbarkeit der Zugriffsrechte

Die geltenden Zugriffsregelungen in § 291a Abs. 4 bis 6 SGB V sehen ein ausdifferenziertes Zugriffssystem für die auf oder mittels der elektronischen Gesundheitskarte gespeicherten Daten vor, das technisch umzusetzen ist. Überdies bestehen weitere – verfassungsrechtliche – Anforderungen, die eine Möglichkeit der selektiven Freischaltung von Infor-

2166 S. BT-Drs. 15/1525, 144.
2167 S.o. 4.3.2.3.
2168 S. zum Verfahren der §§ 303a bis 303f SGB V *Goldschmidt/Goetz/Hornung*, Management-Handbuch Krankenhaus 2004, Rn. 22 ff. und oben 4.3.2.3.
2169 *BITKOM/VDAP/VHitG/ZVEI* 2003, 30 ff.

mationen durch den Versicherten und den technischen Schutz auch der Versicherungsstammdaten erzwingen.[2170]

6.3.3.1 Absicherung eines abgestuften Zugriffsschutzes

Erste Voraussetzung für einen abgestuften Zugriffsschutz ist die Prüfung der Rolleneigenschaft des zugreifenden Leistungserbringers. Dies kann durch elektronische Heilberufsausweise und andere Berufsausweise umgesetzt werden.[2171] Wenn es sich bei diesen – wie in § 291a Abs. 5 Satz 3, 1. Halbsatz SGB V gefordert – um Signaturkarten handelt, die zur Erstellung qualifizierter Signaturen in der Lage sind, so ist es möglich, für die verschiedenen Gruppen von Leistungserbringern (beispielsweise Ärzte, Zahnärzte, Apotheker) unterschiedliche Attribut-Zertifikate zu vergeben, in denen die Zugehörigkeit zu der jeweiligen Kategorie von Berechtigten bestätigt wird.

Diese Attribut-Zertifikate müssen vor dem Zugriff überprüft werden. Die sicherste Möglichkeit hierzu ist die Überprüfung durch die elektronische Gesundheitskarte. Dabei stellt sich allerdings – vergleichbar der Authentisierung zwischen digitalem Personalausweis und Lesegerät[2172] – das Problem gesperrter Attribut-Zertifikate, beispielsweise in den Fällen des Verlusts des Heilberufsausweises oder des Entzugs der Approbation.[2173] Um sicherzustellen, dass der elektronische Heilberufsausweis des Leistungserbringers zum Zeitpunkt des Zugriffs noch gültig ist, müsste die Gesundheitskarte an sich selbständig eine OCSP-Abfrage durchführen. Das scheitert jedoch an der Kapazität des Chips; überdies würde die Abfrage durch den Computer desjenigen Leistungserbringers vermittelt, dessen Berechtigung gerade geprüft werden soll.

Möglich ist der Gesundheitskarte selbst dagegen die Prüfung, ob der elektronische Heilberufsausweis ursprünglich berechtigt war, das heißt im System der Gesundheitskarte angemeldet wurde. Hierzu könnte für eine Zentralstelle, beispielsweise die Bundesärztekammer, ein qualifiziertes Basiszertifikat ausgestellt werden, mit dem alle Attribut-Zertifikate einer bestimmten Berufsgruppe signiert werden. Das Basiszertifikat wird danach in allen Gesundheitskarten gespeichert und zur Signaturprüfung des anfragenden Leistungserbringers verwendet. Für den Fall des Ablaufs und der Sperrung des Basiszertifikats müsste eine Möglichkeit des Online-Updates eingerichtet werden, um nicht alle im Umlauf befindlichen Gesundheitskarten einziehen zu müssen. Durch ein solches Verfahren wird zwar nicht die aktuelle, wohl aber die ursprüngliche Berechtigung des anfragenden Leistungserbringers durch die Gesundheitskarte selbst kontrolliert und dadurch der Zugriff durch beliebige Dritte verhindert.

Die Überprüfung der aktuellen Gültigkeit der Zertifikate des Heilberufsausweises (und der Gesundheitskarte) muss demgegenüber auf der Applikations-Ebene, also durch den Praxis- oder anderen Computer, erfolgen. Das bietet zwar keinen Schutz gegen einen Missbrauch unter Verwendung anderer Computer und Software, verhindert aber zumindest im Regelbetrieb das Auslesen von Daten mittels eines gesperrten Heilberufsausweises. Der Praxiscomputer hat zur Überprüfung eine OCSP-Abfrage durchzuführen. Wenn der Heilberufsausweis über Schlüssel und Zertifikate eines qualifizierten Zertifizierungsdiensteanbieters verfügt, so kann auf dessen Verzeichnis- und Sperrdienst zurückgegriffen werden.

2170 S.o. 4.2.3.4.2.

2171 S. etwa *Warda/Noelle* 2002, 91 ff.; *Goetz* 2001, 106 ff.; *Reichow/Hartlep/Schmidt*, MedR 1998, 162, 163 ff.; zur Standardisierung bereits oben 6.1.2.

2172 S.o. 6.2.1.2.

2173 Der neue § 291a Abs. 5a Satz 3 SGB V verlangt in diesem Fall die unverzügliche Sperrung des Heilberufsausweises.

Hierdurch wird der Aufbau eines separaten Dienstes für das Gesundheitswesen entbehrlich.

Aufgrund der Befugnis des Versicherten, einzelne Gesundheitsinformationen auch gegenüber Leistungserbringern zurückzuhalten, ist über diese grundsätzliche Kontrolle der Berechtigung hinaus ein abgestuftes Zugriffssystem zu implementieren.[2174] Es gibt mehrere Möglichkeiten, dies technisch umzusetzen. Denkbar ist, für jede Information, die der Leistungserbringer abruft, die gesonderte Eingabe einer PIN zu verlangen. Das dürfte jedoch in der Praxis zu Belastungen und Zeitverzögerungen führen, insbesondere bei größeren Datenmengen, die sich aus einer Vielzahl von Einzelinformationen zusammensetzen. Als Alternative wird deshalb ein zweistufiges Verfahren diskutiert.[2175] Zunächst soll, wie oben beschrieben, sichergestellt werden, dass der Zugriff durch einen berechtigten Leistungserbringer erfolgt. Nunmehr werden auf dessen Bildschirm unterschiedliche Datenfelder dargestellt und der Versicherte nennt dem Leistungserbringer die Speicherbereiche, auf die dieser zugreifen soll. Die Bereiche können inhaltlich oder nach Anlässen geordnet werden, also entweder nach zusammengehörenden Informationskomplexen (zum Beispiel alle Daten einer fortgesetzten Behandlung) oder nach Untersuchungs- und Behandlungsfällen. Außerdem kann der Versicherte die Namen der Fächer frei wählen.

Im Ergebnis realisiert dieses Verfahren einen gestuften Zugriff, bietet aber keine Sicherung gegen einen missbrauchenden Leistungserbringer. Ein gewisser Schutz besteht allerdings darin, dass der Zugriff auf die auf oder mittels der Gesundheitskarte gespeicherten Daten auf der Karte protokolliert wird. Dadurch wird der Missbrauch zwar nicht unmittelbar verhindert. Da der Leistungserbringer jedoch damit rechnen muss, dass sein Verhalten offenbar wird und straf- oder standesrechtliche Folgen nach sich zieht, dürfte ein erheblicher Abschreckungseffekt eintreten.

Als technische Ergänzung könnte es dem Karteninhaber ermöglicht werden, bestimmte Informationen generell freizugeben oder generell von der allgemeinen Freigabe auf der ersten Stufe auszunehmen. Derartige generelle Einstellungen sind beispielsweise für Datenordner bei der Zusammenarbeit in Netzwerken üblich. Der Patient könnte so einzelne Angaben (beispielsweise besonders sensible, selten gebrauchte Informationen) durch das Erfordernis einer zusätzlichen Eingabe einer PIN sichern. Hierbei würde die Datenstruktur und -ordnung nicht verändert. Diese könnte sich nach wie vor an den einzelnen Krankheiten oder Behandlungen ausrichten; lediglich einzelne Datensätze würden für den Leistungserbringer gesperrt.

Dieses Verfahren ist allerdings keine Alternative, sondern nur eine Ergänzung zu dem beschriebenen zweistufigen Vorgehen, weil es gerade keine Freigabe des Zugriffs im Einzelfall ermöglicht, sondern generell ausgerichtet ist.[2176] Überdies ist das derzeit diskutierte Zweistufenverfahren auch ohne ergänzende Sicherung für den Versicherten schon relativ kompliziert. Daran werden die Grenzen eines abgestuften Zugriffsmanagements deutlich. Zur Eingabe der PIN auf der ersten Stufe ist erforderlich, dass der Karteninhaber mental zum Erinnern der PIN und physisch zur Eingabe mittels Nummerntasten fähig ist. Wenn auf der zweiten Stufe mit einer Visualisierung der Datenfelder gearbeitet wird, müssen Äquivalente für sehbehinderte Patienten eingerichtet werden. Das größte Problem

2174 Vgl. oben 4.2.3.4.2.

2175 S.a. *ATG/GVG* 2005, 33 ff.; Herr Dr. *Goetz* (KV Bayerns) war so freundlich, einige Fragen zu diesem Themenkreis zu beantworten.

2176 Selbst eine Beschränkung auf bestimmte Gruppen von Leistungserbringern wäre keine Lösung, weil ein Patient zwischen Angehörigen derselben Gruppe (z.B. zwei Augenärzten) bestimmte Daten selektiv freigeben können muss. Eine Beschränkung des Zugriffs auf einzelne Leistungserbringer wäre technisch machbar, dürfte aber so unpraktisch sein, dass davon kein Gebrauch gemacht werden würde.

dürfte die Komplexität des Speicher- und Zugriffssystems sein. Je mehr Daten oder Verweise auf der Gesundheitskarte gespeichert werden, desto weniger kann der Inhaber den Inhalt der Datenfelder und die Relevanz für eine konkrete Behandlungssituation überblicken. Selbstgewählte Namen können zu einer einfacheren, aber auch zu einer komplizierteren Organisation der Informationen führen. Außerdem ist der Patient zumindest beim Arzt in einer Situation, in der sein Interesse weniger auf die Sicherung seiner Privatsphäre, als vielmehr auf eine schnelle und optimale Gesundheitsversorgung gerichtet ist. Er wird deshalb leichter bereit oder zu überzeugen sein, den gesamten Datenbestand freizugeben. Insgesamt wird die Verwaltung der Daten schon für jüngere, technisch interessierte Versicherte eine große Herausforderung werden. Für ältere, behinderte und chronisch kranke Patienten dürfte es schwierig, wenn nicht gar unmöglich sein, eine selbstbestimmte Entscheidung über den Zugriff im Einzelfall zu treffen.

Aus grundrechtlicher Sicht ist diese Situation problematisch, weil eine Überforderung großer Bevölkerungsteile durch eine zu hohe Komplexität des Zugriffssteuerungssystems zwar formal die Entscheidungsbefugnis und informationelle Selbstbestimmung der Betroffenen wahrt, materiell jedoch mit beiden in Konflikt gerät.[2177] Durchschaut der Patient das Zugriffssystem nicht, bleibt ihm letztlich nur die Wahl, durch die vollständige Freischaltung der Gesundheitskarte auf sein informationelles Selbstbestimmungsrecht zu verzichten oder durch die Verweigerung des Zugriffs seine Gesundheit zu gefährden.

In dieser Situation kann der Ausweg nur in einer Stärkung des Arzt-Patient-Verhältnisses liegen. Dieses wird von gegenseitigem Vertrauen geprägt, weil der Patient selbstbestimmt entscheidet, mit welchen Leistungserbringern er kommuniziert, und der Leistungserbringer nach außen schweigepflichtig und -berechtigt ist. Vertrauen ist unabdingbar, weil die ärztliche Tätigkeit notwendigerweise die Kenntnis sensibler Informationen voraussetzt. Für die Gruppe derjenigen, die bereit und in der Lage sind, ihre Daten im Einzelnen zu verwalten, bleibt ein System des abgestuften technischen Zugriffsschutzes sinnvoll und erforderlich. Für die übrigen Versicherten muss der Arzt Fürsorgefunktionen übernehmen. Unter den Bedingungen einer weitreichenden automatisierten Datenverarbeitung im Gesundheitswesen erweitert sich die Fürsorgepflicht des Arztes also auf den Schutz der informationellen Selbstbestimmung seiner Patienten. Er muss dafür sorgen, dass die elektronische Datenverarbeitung nur zu deren Wohle eingesetzt wird und sie sie – soweit möglich – nachvollziehen können. Diese erweiterte Fürsorgepflicht setzt rechtlich eine Stärkung des Schweigegebots und -rechts nach außen voraus. Gleichzeitig müssen die beteiligten Leistungserbringer darin geschult werden, die sich aus den neuartigen Abläufen gegenüber dem Patienten ergebende höhere Verantwortung wahrzunehmen.

6.3.3.2 Verwendung von Biometrie

Die Verwendung biometrischer Verfahren kommt – wie bei anderen Chipkarten – bei der elektronischen Gesundheitskarte als Alternative zur PIN in Betracht, wenn auch angesichts des engen Zeitrahmens nicht für die erste Kartengeneration. Ein wesentlicher Vorteil könnte die Unabhängigkeit von der PIN und den mit ihr verbundenen Problemen sein.

Ähnlich wie bei der Verwendung im Rahmen der elektronischen Signatur wäre bei der Gesundheitskarte ein Matching-On-Card erforderlich, weil die Sicherheit des Matching-Ergebnisses durch die Karte selbst überprüfbar sein muss. Das Problem der Lebenderkennung, die eine der größten Schwierigkeiten bei der Verwendung zur Freischaltung des

2177 S. bereits *BSI* 1995, 62.

Signaturschlüssels darstellt,[2178] ist für die Gesundheitskarte entschärft, weil bei dieser der Zugriff in einer beobachteten Umgebung stattfindet. Aufgrund der Bindung an den Einsatz eines elektronischen Heilberufsausweises würde ein erfolgreicher Replay-Angriff zumindest die Mitwirkung eines Leistungserbringers voraussetzen.

Sicherheitstechnisch problematisch wäre demgegenüber die Einrichtung eines Verfahrens, das keine Mitwirkung des Versicherten voraussetzt, weil dann bei Patienten, die dauerhaft oder temporär zu gewillkürten Bewegungen außerstande sind, ein Matching (mit nachfolgendem Datenzugriff) auch gegen ihren Willen erfolgen könnte. Außerdem ist zu beachten, dass die Krankheit, deretwegen sich der Patient in Behandlung begibt, gerade dasjenige Merkmal betreffen kann, mit dem er sich authentifizieren will.[2179] Ein vollständiger Verzicht auf die PIN dürfte deshalb nicht möglich sein.

6.3.3.3 Zugriff mittels einer eigenen Signaturkarte des Versicherten

§ 291a Abs. 5 Satz 3, 2. Halbsatz SGB V bestimmt, dass der Karteninhaber auf die selbst zur Verfügung gestellten Daten (§ 291a Abs. 3 Satz 1 Nr. 5) auch mittels einer eigenen Signaturkarte zugreifen kann, die „über eine qualifizierte elektronische Signatur verfügt".[2180] Denkbar wäre zwar auch, auf der Gesundheitskarte ein qualifiziertes Signaturverfahren einzurichten und so ein Zugriffsmanagement zu ermöglichen. Der Gesetzeswortlaut spricht jedoch von einer „eigenen" Signaturkarte des Versicherten, die Gesetzesbegründung von Versicherten, die „selbst" über eine solche verfügen.[2181] Damit ist eine separate Signaturkarte des Versicherten gemeint.

Zu klären ist, wie die elektronische Gesundheitskarte überprüfen kann, ob es sich um eine Signaturkarte des Versicherten handelt. Wenn dieser bei der Ausstellung und Personalisierung der Gesundheitskarte bereits über eine Signaturkarte verfüg, kann die Zertifikatsnummer des qualifizierten Zertifikats zur Sicherung des Zugriffs auf die selbst zur Verfügung gestellten Daten auf der Gesundheitskarte gespeichert werden. Beim Zugriff überprüft der Chip der Gesundheitskarte die von der anfragenden Signaturkarte erstellte qualifizierte Signatur und das zugehörige Zertifikat. Verfügt der Karteninhaber zum Zeitpunkt der Personalisierung jedoch noch nicht über eine Signaturkarte, so muss in diesem System nachträglich die Verknüpfung auf der Karte eingerichtet werden. Außerdem ist bei jedem Wechsel des qualifizierten Zertifikats eine Veränderung des Kontrollmechanismus erforderlich, die umständlich und organisatorisch aufwendig ist.

Als Alternative kommt folgender Ablauf in Betracht: Der Zugriff auf das Datenfeld wird bereits bei der Ausstellung der elektronischen Gesundheitskarte mit einer eindeutigen Kennung verknüpft. Hierzu könnte beispielsweise die Krankenversichertennummer verwendet werden, die in Zukunft gemäß § 290 SGB V krankenkassenübergreifend eindeutig vergeben wird. Bei der Beantragung der eigenen qualifizierten Signaturkarte des Versicherten wird für diesen ein Attribut-Zertifikat ausgestellt, das die Zugehörigkeit der Versichertennummer bestätigt. Die Gesundheitskarte kann nunmehr anhand des Attribut-Zertifikats überprüften, ob der berechtigte Versicherte auf das Datenfeld zugreift.

Allerdings müsste innerhalb der Gesundheitskarte eine vollständige Signaturprüfung ablaufen. Hierzu könnte das Zertifikat der Regulierungsbehörde auf der Karte gespeichert werden. Mit dem darin enthaltenen öffentlichen Schlüssel ließe sich das Zertifikat eines

---

2178 S.o. 6.2.2.

2179 *BSI* 1995, 78.

2180 Die Formulierung ist, ebenso wie die für den elektronischen Heilberufsausweis (s.o. 2.2.2.2, Fn. 256), ungenau. Die Signaturkarte „verfügt" nicht über eine qualifizierte Signatur, sondern stellt sie her.

2181 BT-Drs. 15/1525, 145.

beliebigen akkreditierten Zertifizierungsdiensteanbieters auch dann überprüfen, wenn dieser seinen Betrieb erst nach Ausstellung der Gesundheitskarte aufgenommen hätte. Anhand dieses Zertifikats würde das Attribut-Zertifikat des Versicherten geprüft. Voraussetzung wäre, dass – vergleichbar der Prüfung der Berechtigung des Leistungserbringers – die Möglichkeit bestünde, das Zertifikat der Regulierungsbehörde auf der Karte auszutauschen, sollte dies wegen einer Sperrung erforderlich sein.

Aus Sicht des Versicherten ist bedenklich, dass ein Zugriff auch mit einem gesperrten Attribut-Zertifikat möglich wäre, weil die Karte keine Möglichkeit hat, eine OCSP-Abfrage durchzuführen. Überdies verursacht die beschriebene Lösung zusätzliche Kosten für das Attribut-Zertifikat, das nur zum Zweck des Zugriffs auf die Gesundheitskarte eingesetzt wird.

Angesichts dieses aufwendigen Verfahrens dürfte es de lege ferenda vorzugswürdig sein, auf den Einsatz einer separaten Signaturkarte des Versicherten zu verzichten und stattdessen einen sicheren Zugriffsschutz auf der elektronische Gesundheitskarte selbst einzurichten. Die aktuelle Gesetzesfassung ist der Regelung des Zugriffs durch einen Leistungserbringer nachgebildet: Anstelle des elektronischen Heilberufsausweises ist eine Signaturkarte des Versicherten erforderlich. Da dieser sich aber ohnehin gegenüber seiner Gesundheitskarte mittels PIN authentifizieren kann, erscheint der Einsatz einer zusätzlichen Karte (der mit der Eingabe einer weiteren PIN verbunden wäre) wenig sinnvoll.

6.3.4 Organisationsfragen

Für die Funktionsfähigkeit des Gesamtsystems „elektronische Gesundheitskarte“ sind, ähnlich dem System des digitalen Personalausweises, die dezentrale Ausstattung einer Vielzahl von Beteiligten mit technischen Einrichtungen und der Aufbau einer Gesamtinfrastruktur erforderlich. Hierfür ist an sich gemäß § 291a Abs. 7 in Verbindung mit § 291b SGB V die Gesellschaft für Telematik zuständig. Dem Bundesministerium für Gesundheit und Soziale Sicherung wurde jedoch in § 291b Abs. 4 Satz 4 SGB V die rechtliche Befugnis zu einer Ersatzvornahme eingeräumt.

Das Antrags- und Ausgabeverfahren für die Gesundheitskarte bedarf einer Modifizierung gegenüber dem bisherigen Ablauf. Da die Karte (außer bei Versicherten bis zum 16. Lebensjahr und Personen, deren Mitwirkung bei der Erstellung des Lichtbildes nicht möglich ist) ein Photo des Inhabers enthalten wird, muss dieser – vergleichbar dem bisherigen Personalausweisverfahren – einen Antrag stellen, dem das Bild beigefügt wird. Wird der technische Zugriffsschutz mittels einer PIN bewerkstelligt, muss ein PIN-Brief übergeben oder mit der Briefpost übermittelt werden. Die persönliche Übergabe ist die sicherere Variante und hat auch den Vorteil einer eindeutigen Vergleichsmöglichkeit des Bildes mit dem Versicherten, erfordert jedoch die Bereitstellung entsprechender Ressourcen durch die Krankenkassen, die Nutzung des Postident-Verfahrens oder die Einrichtung regionaler krankenkassenübergreifender Registrierungsstellen.[2182]

Zur Produktion und Personalisierung der Gesundheitskarten ist eine sichere Umgebung bei den Herstellern zu gewährleisten. Dies ist umsetzbar. Deutlich aufwendiger wird demgegenüber die Ausrüstung aller Beteiligten mit Kartenlesegeräten und anderem technischem Zubehör werden, welches für die Funktionsweise der elektronischen Gesundheitskarte benötigt wird. Sämtliche 130.000 Arztpraxen, 2.200 Krankenhäuser, 20.000 Apothe-

2182 Für letzteres gibt es Angebote externer Dienstleister, s. http://www.aerztezeitung.de/docs/2005/02/18/030a1402.asp?cat=/computer/telemedizin.

ken und 54.000 Praxen von Zahnärzten und andere Heilberufen in Deutschland[2183] müssen entsprechend ausgestattet werden. Hieraus ergibt sich ein erheblicher Investitionsbedarf bei den Beteiligten, weil die bisherigen Systeme nicht für hochentwickelte Gesundheitskarten und Heilberufsausweise ausgelegt sind. An alle Leistungserbringer (270.000 Ärzte, 77.000 Zahnärzte, 22.000 Apotheker),[2184] in Teilbereichen auch an die Angehörigen ihres Hilfspersonals, müssen im Übrigen Heil- und anderen Berufsausweise ausgegeben werden. Dazu kommen Security Module Cards für die beteiligten Institutionen. Die Gesamtzahl der Karten wird nach Schätzungen 1,8 Millionen betragen.[2185] Die Ausgabe und Verwaltung der Attributszertifikate bedarf eines effektiven Zertifikatsmanagements. Die Krankenkassen sind schließlich nach § 291a Abs. 2 Satz 2 und Abs. 3 Satz 5 SGB V in Verbindung mit § 6c Abs. 2 BDSG zur unentgeltlichen Bereitstellung von Geräten und Anlagen zur Wahrnehmung des Auskunftsrechts verpflichtet.[2186]

Neben diesen dezentralen Einrichtungen erfordern alle Anwendungen der Gesundheitskarte, deren Datenmengen über ihre Speicherkapazität hinausgehen, die Einrichtung eines hochverfügbaren verteilten Serversystems. Hierzu müssen entsprechende Anlagen eingerichtet und vernetzt werden. Der Datentransfer muss standardisiert und verschlüsselt ablaufen. Einige Anwendungen erfordern die Zusammenarbeit sämtlicher Beteiligter im Gesundheitswesen. Das elektronische Rezept wird beispielsweise vom Arzt ausgestellt, vom Versicherten in die Apotheke übermittelt, dort weiterbearbeitet und schließlich von der Krankenkasse abgerechnet. Derartige Abläufe haben einen hohen Abstimmungs- und Koordinierungsbedarf.[2187] Wie groß dieser ist, wird deutlich, wenn man sich vergegenwärtigt, dass es derzeit noch mehr als 180 unterschiedliche Praxiscomputersysteme der ambulanten und mehr als 60 Klinik-Informationssysteme der stationären Versorgung gibt.[2188]

Um die Herausforderungen einer effektiven Zusammenarbeit der Beteiligten zu bewältigen, werden die Spitzenorganisationen der Beteiligten an der Selbstverwaltung im Gesundheitswesen in §§ 291a Abs. 7 Satz 1, 291b Abs. 1 SGB V verpflichtet, mittels einer Gesellschaft für Telematik innerhalb einer vom Bundesministerium für Gesundheit und Soziale Sicherung gesetzten Frist (§ 291b Abs. 4 Satz 4 SGB V) technische Vorgaben sowie Inhalt und Struktur der Datensätze für deren Bereitstellung und Nutzung festzulegen. Zu diesem Zweck wurde am 11. Januar 2005 von den Verbänden der Krankenkassen und der Leistungserbringer die „gematik Gesellschaft für Telematikanwendungen der Gesundheitskarte GmbH“ gegründet.[2189] Sie kann gemäß § 291b Abs. 2 Nr. 2 SGB V mit der Mehrheit von 67 Prozent der sich aus den Geschäftsanteilen ergebenden Stimmen entscheiden.

Sollte keine Vereinbarung erfolgen, so ist das Ministerium nach § 291b Abs. 4 Satz 4 SGB V befugt, im Benehmen mit den zuständigen obersten Landesbehörden ohne Zustimmung des Bundesrates die Einzelheiten durch eine Rechtsverordnung zu bestimmen. In dieser Möglichkeit liegt eine – für Deutschland – bemerkenswerte Eingriffsmöglichkeit in die Selbstverwaltungsstrukturen des Gesundheitswesens. Bis zum GKV-Modernisierungsgesetz existierte keine Instanz, die verbindliche Vorgaben für Standards und Ausges-

2183 Vgl. *Merten*, DÄ 2004, C 17.
2184 Die exakten Zahlen sind umstritten, s.o. Fn. 88 (S. 43).
2185 Vgl. http://www.heise.de/newsticker/meldung/59473.
2186 S.o. 4.3.3.4.
2187 *Dierks/Nitz/Grau* 2003, 181.
2188 Vgl. *Goldschmidt/Goetz/Hornung*, mdi 2/2004, 61, 65; s.a. *Berger & Partner* 1997, 31.
2189 S. *Rabbata*, DÄ 2005, A 96; s.a. *Hornung/Goetz/Goldschmidt*, WI 2005, 171, 175, 178.

taltung einer Telematik-Plattform hätte vorgeben können. Es bleibt abzuwarten, ob das Ministerium von dieser Befugnis Gebrauch machen muss und wird.[2190]

6.3.5 Kosten

Auch bei der elektronischen Gesundheitskarte stellt sich die Frage der Verhältnismäßigkeit der Kosten. Für die Karte selbst werden zwar keine Gebühren erhoben, die Kosten werden jedoch im Rahmen der paritätischen Finanzierung zum Teil von den Versicherten, zum Teil von den Arbeitgebern aufgebracht. Anders als beim Personalausweis[2191] wird die Einführung der Gesundheitskarte auch zu unmittelbaren Einspareffekten führen.

Die Höhe der Kosten wird durch die erforderlichen Komponenten der Telematik-Infrastruktur bestimmt. Für jeden Versicherten sowie für nicht versicherte Empfänger von laufenden Leistungen zum Lebensunterhalt und von Hilfe in besonderen Lebenslagen ist eine Karte erforderlich, ebenso für die Leistungserbringer im System. Die Lesegeräte in Praxen, Apotheken und Krankenkassen dürften teurer als üblich sein, weil zur gegenseitigen Authentisierung von Gesundheitskarte und Heilberufsausweis ein Kartenlesegerät mit zwei Kartenschlitzen erforderlich ist.[2192] Schließlich sind die Einrichtung einer hochverfügbaren Serverarchitektur und die Schulung und Fortbildung der Mitarbeiter der Leistungserbringer und Krankenkassen zu berücksichtigen.

Im Unterschied zum digitalen Personalausweis sind die Kostenberechnungen bei der elektronischen Gesundheitskarte schon weiter fortgeschritten. Es wird mit Anlaufinvestitionen von 1,2 bis 1,5 Milliarden Euro gerechnet.[2193] Befürchtungen, diese Summe könnte sich auf bis zu 3,4 Milliarden Euro mehr als verdoppeln, werden von der Bundesregierung und vom Branchenverband BITKOM zurückgewiesen.[2194] Zu den Kosten kommen etwa 290 Millionen Euro für die Einführung des elektronischen Heilberufsausweises hinzu.[2195] Diese werden voraussichtlich von den Ärzten getragen; im Gespräch sind Anschaffungskosten von 30 bis 40 Euro und eine jährliche Gebühr von 50 bis 60 Euro,[2196] hinzu kommen je nach technischer Ausstattung der jeweiligen Praxis 2.000 bis 10.000 Euro für Hard- und Software.[2197]

Diesen Kosten sind die Einsparungen durch die Einführung der Gesundheitskarte gegenüberzustellen. Mittelfristig erhoffen sich die Beteiligten Einspareffekte von bis zu 1 Milliarde Euro pro Jahr.[2198] Ein nicht unerheblicher Teil davon soll durch die Bekämpfung

---

2190 Die Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten *Sehling*, *Storm*, *Widmann-Mauz*, weiterer Abgeordneter und der Fraktion der CDU/CSU v. 30.3.2004 (BT-Drs 15/2810) lässt eine deutliche Zurückhaltung gegenüber staatlichen Vorgaben erkennen. Sie betont vielmehr an mehreren Stellen, es handele sich um Aufgaben der Selbstverwaltung.

2191 Dieser bewirkt zwar durch die Erhöhung der Identifizierungssicherheit auch materielle Vorteile (Schadensvermeidung), diese sind jedoch kaum zu beziffern.

2192 *TeleTrusT* 2004, 20.

2193 Vgl. *Goldschmidt/Goetz/Hornung*, mdi 2/2004, 61, 68 m.w.N.; die Bundesregierung nennt 0,7 bis 1,4 Mrd. Euro, s. die Antwort auf die Kleine Anfrage (Fn. 2190), 12; allgemein zu den Kosten der Telematik im Gesundheitswesen *Warda/Noelle* 2002, 198 ff.; *Debold & Lux* 2001; s.a. *Grätzel v. Grätz* 2004c, 122 ff.; 180 ff. (dort auch zu den Kosten einzelner Anwendungen); Studien zum Einfluss des Technikeinsatzes auf die Gesamtbehandlungskosten sind rar, s. ebd., 189.

2194 S. http://www.heise.de/newsticker/meldung/52840.

2195 *Warda/Noelle* 2002, 200.

2196 S. http://www.aerztezeitung.de/docs/2004/12/20/232a0103.asp.

2197 Vgl. *Rabbata*, DÄ 2005, A 96; http://www.heise.de/newsticker/meldung/58391.

2198 So die Begründung des Gesetzesentwurfs (BT-Drs. 15/1525, 173) und die Antwort auf die Kleine Anfrage (s.o. Fn. 2190), 13. Die Betriebskosten werden zwischen 75 und 147 Mio. Euro betragen, s. ebd.; skeptisch gegenüber den Einsparmöglichkeiten *Grätzel v. Grätz* 2004c, 123.

des Chipkartenmissbrauchs erreicht werden. Schätzungen – die allerdings erheblich divergieren – gehen von einem jährlichen Volumen von bis zu 1 Milliarde Euro aus.[2199] Da die bisherige Krankenversichertenkarte kein Photo enthält und eine Vorlage des Personalausweises beim Leistungserbringer nicht üblich ist, ist die Verwendung durch Nichtberechtigte relativ einfach. Überdies besteht das Problem ungerechtfertigter Zuzahlungsbefreiungen, deren Volumen angeblich 250 Millionen Euro jährlich beträgt.[2200] Beides könnte durch die Einführung der elektronischen Gesundheitskarte vermindert werden, weil diese bei den allermeisten Versicherten[2201] ein Bild des Inhabers und Informationen zum Zuzahlungsstatus enthalten wird. Dessen elektronische Speicherung wird außerdem die Weiterverwendung der Karte bei einer Änderung des Status ermöglichen. Gegenwärtig werden 14 Millionen der jährlich 18,7 Millionen neuen Krankenversichertenkarten nur deshalb ausgegeben, weil sich der Zuzahlungsstatus ändert.[2202]

Die tatsächliche Höhe der Einspareffekte ist stark umstritten. Während die Bundesregierung davon ausgeht, dass sich die Investitionskosten innerhalb von zwei Jahren amortisieren, wird dies nach Berechnungen des Wirtschaftsforschungsunternehmens *Soreon* erst nach sechs Jahren der Fall sein.[2203] Problematisch ist auch die ungleiche Verteilung von Kosten und Nutzen: Während die Einspareffekte vor allem auf Seiten der gesetzlichen Krankenkassen eintreten, führt das System der Gesundheitskarte zu erheblichen Investitionskosten bei Ärzten und Apothekern.[2204] Schließlich können bestimmte Einspareffekte der Einführung der Gesundheitskarte oder aber der Einführung einer bestimmten Anwendung (wie dem elektronischen Rezept)[2205] zugerechnet werden, sodass die Kosten-Nutzen-Relation bis zu einem gewissen Grad unbestimmt bleiben wird.

Der neue § 291a Abs. 7 Satz 4 SGB V bestimmt, dass die Spitzenorganisationen der Beteiligten im Gesundheitswesen eine Vereinbarung zur Finanzierung der Gesellschaft für Telematik, der Anlaufinvestitionen und der laufenden Kosten der Telematikinfrastruktur vereinbaren. § 291a Abs. 7a bis Abs. 7e SGB V sieht hierfür ein sehr detailliertes Refinanzierungssystem vor.

2199 S. *Sosna*, Nordlicht aktuell 3/2003, 10 ff. Die große Unsicherheit über den tatsächlichen Umfang des Missbrauchs wird daran deutlich, dass anderen Angaben zufolge lediglich ein Schaden von 630.000 Euro pro Jahr anzunehmen ist, s. *Warda/Noelle* 2002, 98 m.w.N. Die Gültigkeit auch der bisherigen Versichertenkarte wird in absehbarer Zeit mit der sog. Verax-Liste online prüfbar sein, s. http://www.aerztezeitung.de/docs/2005/03/22/052a1402.asp?cat=/computer/telemedizin.

2200 S. *Dierks/Nitz/Grau* 2003, 185; *Warda/Noelle* 2002, 99.

2201 Ausnahmen gelten für Versicherte bis zum 16. Lebensjahr sowie Versicherte, deren Mitwirkung bei der Erstellung des Lichtbildes nicht möglich ist, s. § 291 Abs. 2 Satz 1, letzter Halbsatz SGB V.

2202 *Grätzel v. Grätz* 2004c, 123.

2203 S. *v. Grätzel v. Grätz* 2004a; *ders*. 2004c, 124.

2204 *Dierks/Nitz/Grau* 2003, 186. Entsprechend umstritten ist die Verteilung der Kosten, s. http://www.heise.de/newsticker/meldung/49601. Eine grundsätzliche Einigung wurde im August 2004 herbeigeführt: die Krankenkassen tragen ca. 1 Mrd. Euro, Ärzte, Zahnärzte und Apotheker ca. 600 Mio. Euro. Die Investitionskosten der Leistungserbringer könnten durch Transaktionsgebühren, bspw. für die elektronischen Rezepte, refinanziert werden, s. http://www.aerztezeitung.de/docs/2004/08/23/148a0104.asp?cat=/politik/gesundheitssystem_uns; http://www.aerztezeitung.de/docs/2004/08/23/148a0403.asp?cat=/computer/telemedizin. Ein Gutachten soll klären, wie die Nutzenverteilung des Systems zu bestimmen ist, s. http://www.aerztezeitung.de/docs/2005/01/21/010a0603.asp?cat=/politik/gesundheitssystem_uns; s.a. *Grätzel v. Grätz* 2004c, 118 f.

2205 Zu den hierbei möglichen Einsparungen vgl. etwa *ATG/GVG* 2001a, 16 f.

6.4 Die Umsetzung des JobCard-Verfahrens

Im Rahmen der Umsetzung des JobCard-Verfahrens ergeben sich einige Einzelfragen, nämlich der Verfügbarkeit einer datenschutzgerechten Alternative zur Verwendung der Sozialversicherungs- und Zertifikatsnummern, der Notwendigkeit eines papierbasierten Rückfallsystems, der Möglichkeit einer Ende-zu-Ende-Verschlüsselung und der Verwendung qualifizierter Signaturen durch die Arbeitgeber.

Nach dem bisherigen Konzept soll in der Registratur Fachverfahren die Zertifikatsnummer des Arbeitnehmers mit seiner Sozialversicherungsnummer verknüpft werden. Nach einer weitgehenden Verbreitung von Signaturkarten wird in der Zentralen Speicherstelle mit der Zertifikatsnummer als Ordnungskriterium gearbeitet werden. Als datensparsame Alternative kommt in Betracht, aus der Zertifikatsnummer zunächst mittels eines Hash-Algorithmus' ein Einwegpseudonym zu berechnen und dieses Pseudonym der Sozialversicherungsnummer zuzuordnen oder es – im späteren Echtbetrieb – als Ordnungskriterium zu verwenden.[2206] Beim Abruf der Daten wird der Vorgang wiederholt und so der einschlägige Datensatz bestimmt. Das hat den Vorteil, dass in der Registratur Fachverfahren keine Speicherung der Zertifikatsnummern erforderlich ist. Mit der zunehmenden Verbreitung von Signaturverfahren könnte es sonst dazu kommen, dass diese Nummern in einer Vielzahl von Lebensbereichen als Ordnungskriterium fungieren würden. Das könnte zu bedenklichen Datenzusammenführungen führen, die bei der Verwendung von Einwegpseudonymen verhindert werden können.

Dieses Verfahren kann seine volle Wirkung allerdings aufgrund einer Besonderheit nur bei Geheimhaltung des Hash-Algorithmus' entfalten. Im Normalfall nützt dessen Kenntnis einem Angreifer nichts, weil der Algorithmus nicht zur Rückwärtskonstruktion einsetzbar ist und der Hash-Wert unabhängig von der Größe des Ausgangswerts eine fest definierte Länge hat. Die Zertifikatsnummer hat jedoch ebenfalls eine definierte Länge und einen definierten Aufbau. Deshalb ist es bei Kenntnis des Hash-Algorithmus' möglich, alle denkbaren Zertifikatsnummern in Einwegpseudonyme umrechnen, so eine Komplettliste mit allen denkbaren Pseudonymen zu erstellen und damit Zertifikatsnummern und Pseudonyme auch ohne Umkehrung des Algorithmus' eindeutig zuzuordnen.

Da die vom Beschäftigten angemeldete Signaturkarte im JobCard-Verfahren erst dann eingesetzt werden wird, wenn der Leistungsfall eintritt, können Schwierigkeiten auftreten. Liegt zwischen der Anmeldung und dem Leistungsfall ein größerer Zeitraum, wird es voraussichtlich in erheblichem Umfang zu einem Vergessen der PIN kommen, weil – jedenfalls solange andere Anwendungen für die elektronische Signatur noch nicht sehr verbreitet sind – die Beantragung von Leistungen der Arbeitslosenversicherung für eine Vielzahl von Karteninhabern der erste Einsatz dieser Nummer sein dürfte. Ein Vergessen der PIN verursacht Probleme im Abrufsystem des JobCard-Verfahrens: Nur anhand einer Zertifikatsnummer, die bereits mit der Sozialversicherungsnummer verknüpft wurde, ist nämlich die Bestimmung der benötigten Daten in der Zentralen Speicherstelle möglich. Eine Lösung könnte die Verwendung eines Personal Unblocking Keys (PUK) sein, sofern sichergestellt ist, dass nur der Berechtigte über die PUK verfügen kann.[2207]

2206 *Hornung/Roßnagel*, K&R 2004, 263, 268.

2207 Sowohl nach dem alten Maßnahmenkatalog des BSI als auch nach jüngsten Feststellungen der RegTP ist die PUK grundsätzlich wie eine PIN zu behandeln. Sie muss mindestens acht Stellen lang sein und darf nur für die Rückstellung des PIN-Zählers und für das Auswechseln der PIN eingesetzt werden. Für diese Zwecke darf sie maximal zehnmal verwendet werden und muss nach dem dritten Fehlversuch gesperrt werden; s. hierzu bereits RMD-*Roßnagel/Hammer*, § 5 SigV 1997 Rn. 84.

Abrufprobleme treten auch bei einem Verlust der Karte auf. Um einen Zugriff auf die Daten zu gewährleisten, gibt es zwei Möglichkeiten. Denkbar ist zunächst ein papierbasiertes Verfahren. Der Arbeitslose könnte bei seinem Zertifizierungsdiensteanbieter seine Zertifikatsnummer erfragen und diese der Arbeitsagentur mitteilen. Deren Mitarbeiter müsste wie bisher eine Identifizierung vornehmen und würde danach eine Anfrage an die Zentrale Speicherstelle senden, die – jetzt manuell – anhand der Zertifikatsnummer die Daten bestimmen würde.

Ein derartiges Verfahren führt jedoch zu erheblichen Effizienzeinbußen des Gesamtsystems. Überdies könnte es einzelne Betroffene dazu verleiten, diesen Weg anstelle des vorgesehenen Abrufs mittels der Signaturkarte zu nutzen. Vorzugswürdig erscheint es deshalb, bei Verlust der Karte oder Vergessen der PIN eine Pflicht zur Neuanmeldung mit einer neuen Karte einzuführen und die Sozialversicherungsnummer mit der neuen Zertifikatsnummer zu verknüpfen.[2208] Dies ist ohnehin dann erforderlich, wenn ein Zertifikat spätestens nach fünf Jahren seine Gültigkeit verliert (§ 14 Abs. 3 Satz 1 SigV) und ein neues ausgestellt werden muss. Für die Zentrale Speicherstelle ändert sich hierdurch zunächst nichts, da sie intern ohnehin mit der Sozialversicherungsnummer arbeitet. Wird in Zukunft die Zertifikatsnummer als Ordnungskriterium verwendet, kann die Registratur Fachverfahren eine Historie über die verschiedenen Nummern eines Antragstellers verwalten, mit deren Hilfe der Abruf bewerkstelligt werden kann. In einem solchen System kann ein Bürger auch verschiedene Schlüssel und Zertifikate verwenden, ohne dass dies für den Datenabruf Probleme verursacht.[2209]

Die Datenschutzbeauftragten des Bundes und der Länder forderten Ende des Jahres 2004, die Möglichkeit einer Ende-zu-Ende-Verschlüsselung unter Verwendung des geheimen Verschlüsselungsschlüssels der Signaturkarte des Arbeitnehmers zu prüfen und hierzu ein Gutachten in Auftrag zu geben.[2210] Die Umsetzbarkeit eines solchen Verfahrens ist unklar. Zunächst müssten bereits bei Projektstart alle versicherten Arbeitnehmer über eine Signaturkarte verfügen. Das wäre selbst bei einer gesetzlichen Verpflichtung nur schwer umzusetzen. Schon vereinzelte Weigerungen würden aber zu erheblichen Effizienzeinbußen führen, weil der Arbeitgeber gewährleisten müsste, die Daten dieser Arbeitnehmer auf anderem Wege zu übermitteln oder selbst zu speichern.

Außerdem führt die Ende-zu-Ende-Verschlüsselung beim normalen Austausch und Verlust der Signaturkarte zu großen Schwierigkeiten. Da die Daten mit dem geheimen Schlüssel der Karte verschlüsselt werden, sind sie dann nicht mehr verwertbar. Im Fall des normalen Kartenwechsels könnten die Daten umgeschlüsselt, also mit dem geheimen Schlüssel der alten Karte ent- und mit dem öffentlichen Schlüssel der neuen Karte wieder verschlüsselt werden.[2211] Dazu müsste sich der Arbeitnehmer allerdings in eine Arbeitsagentur begeben, die Daten dort von der Zentralen Speicherstelle abrufen, umschlüsseln und zurücksenden. Dieses Verfahren wäre umständlich und vermutlich auch teuer. Um das Problem des Verlusts der Karte zu lösen, wird vorgeschlagen, die Daten bei den Arbeitgebern so lange elektronisch zu archivieren, wie es die jeweiligen gesetzlichen Speicherfristen erfordern.[2212] Damit wird freilich ein hauptsächliches Ziel des gesamten Projekts, die

2208 *Hornung/Roßnagel*, K&R 2004, 263, 266.

2209 Das wird übersehen von *Ernestus*, DuD 2004, 404, 407, wonach die Zertifikatsnummer aufgrund der kürzeren Gültigkeit des Zertifikats per se nicht als Ordnungskriterium geeignet sein soll.

2210 S. *AKT*, DuD 2005, 29 ff.; *ULD* 2005, 16; skeptisch gegenüber der Umsetzbarkeit allerdings *Der Bundesbeauftragte für den Datenschutz* 2005, 44 f.

2211 *AKT*, DuD 2005, 29, 32.

2212 Vgl. *AKT*, DuD 2005, 29, 31.

Entlastung der Arbeitgeber von der Aufbewahrungspflicht,[2213] konterkariert. Eine Lösung dieses Problems könnte ein Key Recovery Verfahren sein, bei dem die Session-Keys des jeweiligen Datensatzes bei einem oder mehreren vertrauenswürdigen Dritten gespeichert würden. Auch dann müssten aber vor der ersten Speicherung Signaturkarten an alle Betroffenen ausgegeben werden. Im Ergebnis erscheint das Modell der Ende-zu-Ende-Verschlüsselung aus mehreren Gründen nur schwer realisierbar.

Fraglich ist schließlich, ob auch die Arbeitgeber qualifizierte Signaturverfahren verwenden sollten. Ein Schriftformerfordernis – das diese Signaturstufe erfordern würde – besteht für die Bescheinigungen nicht,[2214] sodass de lege lata keine qualifizierten Verfahren erforderlich sind. Nur diese garantieren jedoch rechtlich, dass eine hoch funktionsfähige Zertifizierungsinfrastruktur besteht. Im Interesse der Integrität und Authentizität der Daten gerade bei der Online-Übertragung sollten deshalb qualifizierte Signaturen eingesetzt werden. Abgesehen davon, dass diese auch für Arbeitnehmer verbindlich vorgeschrieben werden, ergibt sich für die Arbeitgeber keine unzumutbare Belastung, da die Signaturen im Batch-Betrieb erzeugt werden können.[2215]

Eine entsprechende Signatur der Daten erleichtert auch deren Prüfbarkeit nach einem längeren Zeitraum in der Zentralen Speicherstelle. Das Problem der Langzeitarchivierung[2216] der Bescheinigungsdaten ist allerdings dann entschärft, wenn diese ausschließlich für die Berechnung der Ansprüche aus der Arbeitslosenversicherung verwendet werden, da in diesem Fall nur ein relativ kurzer Aufbewahrungszeitraum erforderlich ist. Dies kann sich allerdings dann anders darstellen, wenn das Archiv in Zukunft auch für andere Zwecke eingesetzt werden sollte.[2217]

2213 S.o. 2.1.3.

2214 Nach § 16 DEÜV sollen diese vielmehr durch Datenübertragung oder auf maschinell verwertbaren Datenträgern (in Zukunft nur noch durch Datenübertragung) erfolgen, wobei geeignete Maßnahmen zur Sicherstellung von Datenschutz und Datensicherheit vorzusehen sind. Bei der Nutzung allgemein zugänglicher Netze sind Verschlüsselungsverfahren anzuwenden.

2215 Zu dieser „Massensignatur“ vgl. *Roßnagel/Fischer-Dieskau*, MMR 2004, 133 ff.

2216 S. bereits oben 6.3.1 a.E.

2217 Denkbar wäre u.a. der Einsatz zur Berechnung von Wohngeld, BAföG und Kindergeld, s. *ITSG* 2003.

7 Akzeptanzfragen

Eine umfassende Betrachtung groß angelegter Technologieprojekte erfordert neben der Analyse von Rechtsproblemen und technischer Machbarkeit auch die Untersuchung ihrer Sozialverträglichkeit. Nur so lässt sich die gesamte gesellschaftliche Dimension von Projekten wie dem digitalen Personalausweis, der elektronischen Gesundheitskarte oder des JobCard-Verfahrens erfassen.[2218]

Auf verfassungsrechtlicher Ebene stehen den Vorhaben nach den gefundenen Ergebnissen – jedenfalls in bestimmten Ausgestaltungsformen – keine unüberwindlichen Hindernisse entgegen. Für praktische Schwierigkeiten ist eine Lösung durch wissenschaftlich-technischen Fortschritt zu erwarten. Daraus folgt, dass weder die rechtliche noch die technische, sondern die politische Umsetzbarkeit maßgeblich über die Einführung entscheidend wird.

Einer der wesentlichen Faktoren dafür ist die Akzeptanz in der Bevölkerung. Dabei ist zu unterscheiden: Akzeptanz betrifft zunächst den Bereich von Recht, Rechtsstaat und Rechtsakten, wobei hier wiederum unterschieden werden kann zwischen der Akzeptanz von Gesetzen,[2219] Urteilen[2220] und Verwaltungsentscheidungen.[2221] Von diesem hoheitlichen Bereich ist die Akzeptanz der Anwendung einer neuen Technik im privaten Umfeld abzugrenzen,[2222] in dem die Einführung grundsätzlich auf freiwilliger Basis erfolgt und dementsprechend durch andere Umstände bestimmt wird. Selbst wenn die Implementation neuer Technologien, wie etwa am Arbeitsplatz, mehr oder weniger gezwungenermaßen geschieht, bleiben doch auf der Durchsetzungsebene fundamentale Unterschiede, etwa die Möglichkeit von Ausweichmaßnahmen wie Betriebswechsel,[2223] Partizipationsrechte wie die betriebliche Mitbestimmung sowie ganz generell die Tatsache, dass dem Betroffenen nicht der Staat, sondern eine Privatperson gegenüber steht.

Schließlich kann es aber auch eine Kombination aus den Bereichen der Rechts- und Technikakzeptanz geben, nämlich dann, wenn es um die Akzeptanz eines Gesetzes geht, das die Einführung einer neuen Technologie vorschreibt. Genau dies ist bei Chipkartenausweisen der Fall. Neben dem neuartigen Medium selbst werden regelmäßig auch einige Daten oder neuartige Anwendungen (biometrische Identifikationsdaten, elektronisches Rezept) verbindlich vorgeschrieben. Damit überschneiden sich die rechtlichen und technischen Akzeptanzfaktoren. Konkret bedeutet das, dass auf Seiten der Skeptiker sowohl Argumentationslinien aus dem hoheitlich-rechtlichen (etwa die Überwachungsproblematik) wie aus dem technischen Bereich (zum Beispiel die Folgen des Einsatzes von Chipkarten für mit derartigen Techniken nicht vertraute Bevölkerungsteile) zu erwarten sind.

2218 S. zur Akzeptanz des digitalen Personalausweises bereits *Roßnagel/Hornung*, in: Reichl/Roßnagel/Müller 2005, 301 ff.

2219 Vgl. z.B. *Hill*, JZ 1988, 377 ff.; *ders*., DÖV 1988, 666 ff.; *Röken*, DÖV 1989, 54 ff.; *Würtenberger*, Sonderheft 39/1999 der KZfSS, 380 ff.

2220 S. etwa *Benda*, DÖV 1983, 305 ff.; zur Akzeptanz von Verfassungsgerichtsurteilen *Limbach* 1998, 258 ff.; *Adamovich* 1998, 247 ff.

2221 Insbesondere *Würtenberger* 1996; *ders*., NJW 1991, 257 ff.

2222 Hierzu etwa *Müller* 1994; *Reichwald* 1978; *Simon* 2001, 85 ff. und die Beiträge in *Kistler/Jaufmann* (Hrsg.) 1990.

2223 Auch wenn dies in manchen Bereichen eine bloß theoretische Möglichkeit sein mag (es ist unrealistisch, den Betrieb zu wechseln, weil dieser einen neuen Betriebsausweis einführt, der biometrische Daten beinhaltet), bleibt der Unterschied bestehen.

7.1 Der Begriff der Akzeptanz

Im allgemeinen deutschen Sprachgebrauch ist der Begriff „Akzeptanz“ eine relativ neue Erscheinung.[2224] Noch im Jahre 1982 ergab eine systematische Analyse von mehr als fünfzig deutschen Nachschlagewerken und Wörterbüchern, dass er nicht als Stichwort geführt wurde.[2225] Erst ein Jahr später erschien der Begriff im Duden, während das zugrundeliegende Phänomen zuvor eher mit „Annahme“ beschrieben wurde.[2226] In den folgenden zehn Jahren hielt der Akzeptanzbegriff Einzug in alle Bereiche von Politik-, Wissenschafts- und Alltagssprache. Seit dieser Zeit gibt es nämlich eine zunehmende Zahl gesellschaftlicher Probleme, die – wie Euro-Einführung, Transrapid, gentechnisch veränderte Lebensmittel, Asyl- und Einwanderungsrecht, Ladenschluss, Rechtschreibreform, gleichgeschlechtliche Lebenspartnerschaft und Veränderungen im Sozialversicherungs- und Rentensystem – nicht mehr nur währungs- und verkehrstechnische, ökonomische, biologische, religiöse und juristische Probleme sind, sondern auch und vermehrt Akzeptanzfragen aufwerfen.[2227]

Alltagssprachlich kann Akzeptanz als die Bereitschaft definiert werden, eine Entscheidung anzuerkennen, anzunehmen oder zu dulden.[2228] Im Übrigen ist die Begriffsbildung insgesamt eher inhomogen. Der Akzeptanzbegriff lässt sich als solches nicht ausschließlich einer Wissenschaftsdisziplin zuordnen, sondern weist Bezüge zur Soziologie, Politikwissenschaft, Psychologie und Rechtswissenschaft auf.

Aus rechtswissenschaftlicher Perspektive ist zwischen rechtlicher Akzeptabilität einerseits und der Akzeptanz von Recht andererseits zu unterscheiden. Akzeptabilität ist die Frage der Übereinstimmung einer Maßnahme oder Handlung mit dem Recht und damit ein normatives Problem. Die Übereinstimmung kann sich auf unterschiedliche rechtliche Ebenen beziehen, etwa auf die Frage des Einklangs mit der Rechtsordnung insgesamt (Rechtmäßigkeit) oder mit übergeordneten Normen (Verfassungsmäßigkeit). Was demgegenüber die Begriffsbildung in der rechtswissenschaftlichen Literatur zur Akzeptanz angeht, so wird diese verstanden als die Frage nach der Beachtung und Einhaltung des Rechts.[2229]

Inhaltlich schließt Akzeptanz nach dem meist weiten Verständnis dieser Literatur Einstellungen des Konsenses, des Einverständnisses und der Identifikation mit Normen, aber auch des Dissenses ein.[2230] Die zunächst überraschende Einbeziehung auch des Dissenses über eine Sachfrage wird damit erklärt, dass Akzeptanz auch dann vorliegen könne, wenn eine Norm zwar nicht für „richtig“, aber doch für (noch) anerkennungswürdig und (noch) vertretbar angesehen werde.[2231] Derartiges könne etwa darauf basieren, dass eine Entscheidung demokratisch legitim zustande gekommen sei. Fasst man Akzeptanz derart weit, so kann man sie begrifflich gegen das Rechtsbewusstsein abgrenzen: Normakzeptanz meint

---

2224 Zu „Verbreitung, Stellenwert und Karriere“ des Akzeptanzbegriffs vgl. *Lucke* 1995, 33 ff.

2225 S. *Pressmar* 1982, 324 f.

2226 *Czybulka*, Die Verwaltung 1993, 27, 32; *Eppler* 1992, 169. Die zeitliche Parallele des Auftauchens im Duden zum gescheiterten ersten Versuch der Volkszählung ist sicher zufällig, nichtsdestotrotz bezeichnend.

2227 *Lucke* 1998, 17.

2228 S. z.B. *Strauß* 1995, 335.

2229 *Herzog* 1984, 127.

2230 *Würtenberger* 1987, 81; *ders*. 1996, 61 f.; *ders*, NJW 1991, 257, 258 f.; *ders*., Sonderheft 39/1999 der KZfSS, 380, 381; ähnlich *Kindermann* 1986, 66; *Rehbinder* 2003, 155, der die Vertretbarkeit des Regelungsgehalts einer Norm ausreichen lässt (allerdings soll insoweit auch ein „inneres Bejahen“ erforderlich sein, s. ebd., 158, 169).

2231 *Würtenberger*, Sonderheft 39/1999 der KZfSS, 380, 381.

danach, dass die Rechtsunterworfenen Rechtsnormen als Regeln annehmen, die zu befolgen sind, Rechtsbewusstsein hingegen, dass sie diese Regeln für richtig halten.[2232]

Auch andere Typologisierungen weisen in dieselbe Richtung. Unterschieden werden etwa drei Formen der Akzeptanz.[2233] Die erste ist die der Überzeugung sachlicher Richtigkeit auf Seiten des Betroffenen. Die zweite Form bildet das Abfinden mit der Entscheidung bei fortbestehender gegenteiliger Meinung. Ein typisches Beispiel ist die unterlegene Partei in einem rechtskräftig abgeschlossenen Prozess. Schließlich soll auch das Weiterwirken gegen die Entscheidung mittels legaler Handlungsoptionen, etwa auf parlamentarisch-politischem Wege, als noch von der Akzeptanz erfasst werden. Die zweite und dritte Variante bilden Gruppen so genannten „formalen Gehorsams".

Nach anderer Ansicht genügt es dagegen nicht, nur auf irgendeinem Wege sicherzustellen, dass die Betroffenen sich letztlich nicht gegen eine Maßnahme wehren.[2234] Entscheidend sei vorrangig die Akzeptanz der Entscheidungsinhalte selbst. Danach wäre die Einbeziehung der Kategorie des „formalen Gehorsams" fragwürdig, weil es dort gerade nicht um eine innere Übereinstimmung mit dem Inhalt der jeweiligen Norm oder Einzelfallentscheidung, sondern um deren äußere Befolgung geht. Betrachtet man den Sprachgebrauch, so liegt hier eine Unterscheidung nach den Kategorien „Akzeptieren" und „Respektieren" nahe. Akzeptieren ließe sich dann fassen als innere Überein- und Zustimmung zum Inhalt einer Entscheidung, Respektieren als Einsicht in deren Verbindlichkeit, die trotz fortbestehenden inneren Dissenses einhergeht mit ihrer inhaltlichen Befolgung. Da auch dieses Respektieren letztlich auf einer freiwilligen Befolgung des Rechts basiert, ist mit dieser Unterscheidung jedoch nichts gewonnen. Das Kriterium der Freiwilligkeit, und nicht deren innerer Grund, ist für die Abgrenzung zur zwangsweisen Durchsetzung des Rechts entscheidend.

Schließlich wendet sich die Auffassung, die die Akzeptanz des Entscheidungsinhalts fordert, im Wesentlichen dagegen, dass der Staat das Rechtssystem so organisiert, „dass über komplizierte Prozesse der Verstrickung und hohe Hürden für die Wahrnehmung der eigenen Beschwerdemacht u.ä. gesichert wird, dass die Betroffenen sich letztlich nicht wehren".[2235] Es geht es also mehr um die Abschreckung von der Geltendmachung an sich vorhandener eigener Rechte. Ein aus einem solchen Abschreckungsprozess resultierendes Stillhalten dürfte aber auch nach den oben beschriebenen Auffassungen nicht mehr als Akzeptanz gelten, denn der Einzelne trifft keine aktive, selbstbestimmte Entscheidung, eine bestimmte Norm oder Maßnahme, die seiner Überzeugung widerspricht, für noch vertretbar zu halten.

Der Akzeptanzbegriff muss diese Form der Konformität einschließen, weil ein totaler Konsens in der Sache in jeder pluralistischen Gesellschaft utopisch ist und zur Vermeidung einer „Gewissenskontrolle" staatlicherseits nicht angestrebt werden darf. Auch wenn die Unterlegenen eines demokratischen Entscheidungsprozesses das Ergebnis inhaltlich ablehnen, so fällt ihre Entscheidung, dieses Ergebnis fortan als gültig anzusehen, in den Bereich der Akzeptanz. Im Ergebnis ist damit den eingangs erläuterten Auffassungen darin zuzustimmen, dass auch der „formale Gehorsam" von der Akzeptanz umfasst wird.[2236]

2232 *Roellecke*, JZ 1997, 577.

2233 *Benda*, DÖV 1983, 305, 306.

2234 *Hoffmann-Riem*, AöR 1990, 400, 415. Auch nach *Raiser* (1998, 120) stellt die Befolgung einer Norm aufgrund der Befürchtung hoheitlichen Zwangs keine Akzeptanz dar.

2235 *Hoffmann-Riem*, AöR 1990, 400, 415.

2236 Dabei sollte nicht übersehen werden, dass es jenseits dieser definitorischen Frage sinnvoll sein kann, auf der Einstellungsebene weiter zu differenzieren. Die Effektivität einer Maßnahme wird etwa durchaus davon abhängen, aus welchem inneren Grund das Recht befolgt wird.

Neben dieser rechtswissenschaftlichen Perspektive ist für die weitere Betrachtung vor allem die Begriffsbildung in der Soziologie relevant.[2237] Hier finden sich eine eher technik- und anwendungsbezogene und eine eher sozial- oder gesellschaftsorientierte Ausrichtung.

Erstere definiert Akzeptanz beispielsweise als „die Bereitschaft des Anwenders, in einer konkreten Anwendungssituation das vom Techniksystem angebotene Nutzungspotential aufgabenbezogen abzurufen".[2238] Überwiegend wird Akzeptanz als zweidimensionales Phänomen begriffen: Sie ist zum einen Einstellungsakzeptanz im Sinne einer relativ dauerhaften kognitiven und affektiven Wahrnehmungsorientierung, zum anderen Verhaltensakzeptanz hinsichtlich der Nutzung einer Anwendung in beobachtbarem Verhalten.[2239] Akzeptabilität wird dagegen als die „Annehmbarkeit oder Hinnehmbarkeit [einer Technik] relativ zu einem kulturellen Rahmen" beschrieben.[2240]

Die zweite, eher gesellschaftsorientierte Richtung definiert Akzeptanz, in enger Anlehnung an die Macht- und Herrschaftsdefinitionen *Webers*,[2241] als „die Chance, für bestimmte Meinungen, Maßnahmen, Vorschläge und Entscheidungen bei einer identifizierbaren Personengruppe ausdrückliche oder stillschweigende Zustimmung zu finden und unter angebbaren Bedingungen aussichtsreich auf deren Einverständnis rechnen zu können".[2242] Danach lassen sich zwölf verschiedene Ausdrucksformen der Akzeptanz von der „auf Informationen basierenden Einwilligung im Bewusstsein vorhandener Alternativen (informed consent)" bis zum „wider Willen und gegen besseres Wissen abgerungenem Einverständnis (forced compliance)" unterscheiden.[2243] Akzeptabilität wird definiert als „die prinzipielle Erwartbarkeit mehrheitlichen Einverständnisses auf der objektivierbaren Grundlage allgemein anerkannter und rational begründeter gesellschaftlicher, politischer, wirtschaftlicher etc. Oberziele".[2244] Damit ergibt sich ein enger Bezug zu soziologischen Legitimationstheorien: Akzeptanz ist danach die subjektiv-soziale Kehrseite der Legitima-

---

2237 Die Frage, unter welchen Voraussetzungen Gesetzesgehorsam auf Grund besserer Einsicht freiwillig geleistet wird, ist außerdem ein Feld der politischen Psychologie, vgl. *Würtenberger* 1987, 82 m.w.N.; s. aus politikwissenschaftlicher Sicht *Weinberger* 1998, 73 ff. Unter psychologischen Gesichtspunkten wird der enge Zusammenhang von Akzeptanzentscheidungen mit individuellen Zielvorstellungen, der Bereitschaft zur Kommunikation und der Fähigkeit zu Einsicht und Toleranz betont, s. *Lucke* 1995, 50 ff. m.w.N.; *Pichler*/*Giese* 1993, 46.

2238 *Reichwald* 1978, 31; ähnlich *Müller* 1994, 55 (Akzeptanz als „die positive Wertschätzung einer Innovation (Idee, Sachverhalt, Person) bei gleichzeitiger Handlungsbereitschaft") und *Simon* 2001, 87 („‚Akzeptanz'...steht im Widerspruch zum Begriff Ablehnung und bezeichnet die positive Annahmeentscheidung einer Innovation durch die Anwender"); s.a. *Kubicek* 2003, 97 ff. m.w.N.; *Jaufmann*/*Kistler* 1991; vgl. daneben aus wirtschaftswissenschaftlicher Perspektive *Hecker* 1997 (insbes. 123 ff.); *Kollmann* 1998, 44 ff.

2239 *Müller-Böling/Müller* 1986, 25 ff.; *Simon* 2001, 87; *Steiger* 1995, 6; *Harnischfeger/Kolo/Zoche* 1997, 3 ff. m.w.N. Man kann auf der Ebene der Einstellungen weiter zwischen generellen Einstellungen und der (auf eine Anwendung bezogenen) Nutzungsbereitschaft differenzieren. Diese beiden unterscheiden sich von der tatsächlichen Nutzung dadurch, dass es sich um mentale Vorgänge handelt, die ein anderes soziologisches Forschungsinstrumentarium erfordern.

2240 *Meyer-Abich* 1999, 309. Für Energietechniken werden dort vier Kriterien für Akzeptabilität genannt: Wirtschaftlichkeit, internationale Verträglichkeit, Umweltverträglichkeit und Sozialverträglichkeit (311 ff.).

2241 Vgl. *Weber* 1976, 28: „Macht bedeutet jede Chance, innerhalb einer sozialen Beziehung den eigenen Willen auch gegen Widerstreben durchzusetzen, gleichviel worauf diese Chance beruht. Herrschaft soll heißen die Chance, für einen Befehl bestimmten Inhalts bei angebbaren Personen Gehorsam zu finden."

2242 *Lucke* 1995, 104; s.a. die Nachweise bei *Kollmann* 1998, 38 ff.

2243 *Lucke* 1995, 216 ff., insbes. 230; vgl. des Weiteren *de Bakker*, ZfRSoz 2003, 219, 232 ff.

2244 *Lucke* 1995, 106.

tion,[2245] Legitimität „die allgemeine Bezeichnung dafür, dass Herrschende, politische Bewegungen und Institutionen aufgrund ihrer Übereinstimmung mit Gesetzen, Verfassungen, Prinzipien oder aufgrund ihrer Leistungsfähigkeit für allgemein anerkannte Ziele *akzeptiert*, positiv bewertet und für rechtmäßig gehalten werden".[2246]

Beiden Richtungen ist gemein, dass sie sich gegen den Versuch abgrenzen, Akzeptanz als Eigenschaft eines Objekts zu verstehen. Unter dem Einfluss von Ablehnungsphänomenen bei der Einführung neuer Technologien war Akzeptanz zunächst als „die Eigenschaft einer Innovation, bei ihrer Einführung positive Reaktionen der davon Betroffenen zu erreichen", begriffen worden.[2247] Demgegenüber wird aufgrund der erläuterten Definitionen deutlich, dass Akzeptanz keine unveränderliche Eigenschaft eines Objekts ist, sondern Ergebnis des Zusammenspiels von Faktoren des (nicht) zu akzeptierenden Objekts, der dieses (nicht) akzeptierenden Subjekte sowie des beide umschließenden Kontextes. So können unter Umständen die Eigenschaften des Objekts völlig in den Hintergrund treten und seine Akzeptanz kann zur Funktion der Einstellungen der handelnden Subjekte oder der äußeren Faktoren werden. Individuen können deshalb dasselbe Objekt unterschiedlich akzeptieren und in dieser Hinsicht getroffene Entscheidungen wieder revidieren.[2248] Außerdem ist Akzeptanz kein statischer Prozess, sondern kann durchaus einen längeren Konflikt beinhalten, bei dem das jeweilige Objekt den bisherigen Gegebenheiten angepasst und damit verändert wird.

7.2 Akzeptanz als Rechtsproblem?

Bevor auf sozialwissenschaftliche Aspekte der Akzeptanz des digitalen Personalausweises, der elektronischen Gesundheitskarte und des JobCard-Verfahrens und die Frage ihrer politischen Durchsetzbarkeit eingegangen wird, ist zunächst zu erörtern, ob es sich bei der Akzeptanz auch um ein originär rechtliches Phänomen handelt. In diesem Fall müsste die rechtliche Bewertung eines durch Akzeptanz hoch beeinflussten Projekts diesen Faktor mit einbeziehen.

7.2.1 Ausgangspunkt

Gelingt es der Soziologie und anderen wissenschaftlichen Disziplinen überzeugend, den Akzeptanzbegriff für die Forschung in ihren jeweiligen Kern- oder Grenzbereichen fruchtbar zu machen, so gibt es in der Rechtswissenschaft deutliche Vorbehalte und Abgrenzungsbemühungen.[2249]

An diesen wird die Problematik einer im strengen Sinn juristischen Betrachtung des Akzeptanzphänomens deutlich. Denn aus dieser Perspektive betreffen akzeptorische Faktoren nur den tatsächlichen Aspekt der Frage nach Beachtung und Einhaltung rechtlicher Regeln. Recht unterscheidet sich nämlich von anderen gesellschaftlichen Normen dadurch, dass es durch Befehl und Zwang durchgesetzt werden kann.[2250] Das impliziert Rechtsgel-

2245 *Lucke* 1998, 18; *Rehbinder* 2003, 30, 155; zum Verhältnis von Legitimation und Akzeptanz *Lucke* 1995, 54 ff.; *de Bakker*, ZfRSoz 2003, 219 ff.

2246 *Fuchs-Heinitz/Lautmann/Rammstedt/Wienold* 1995, 396 (Hervorhebung hinzugefügt).

2247 *Endruweit* 1989, 9.

2248 *Lucke* 1998, 18.

2249 Diese sind mitunter massiv, s. z.B. *Hattenhauer* 1998, 91 ff.; *Kaltenbrunner* 1986, 14 (hinter dem Wort Akzeptanz, das ein Widerstandsrecht der Betroffenen gegen den demokratischen Rechtsstaat unterstelle, verberge sich eine „nur notdürftig verschleierte Führungsschwäche").

2250 Von den Autoren zur Akzeptanz: *Herzog* 1984, 128 m.w.N.; *Hill*, JZ 1988, 377; zum soziologischen Rechtsbegriff vgl. *Rehbinder* 2003, 48 ff. m.w.N.

tung auch ohne Akzeptanz der Rechtsunterworfenen. Bereits nach der Vorstellung *Kants* ist das Recht von den individuellen Beweggründen, es einzuhalten, abgeschnitten.[2251] Gesetze sind danach nicht aus Neigung, sondern aus Pflicht zu befolgen, nämlich aus der Achtung vor dem Gesetz. Nach herkömmlicher Konzeption haben sich die Auslegung von Recht und die Rechtsfortbildung an den Maßstäben der Rechtsordnung zu orientieren.[2252] Die Geltung und Rechtmäßigkeit einer Norm oder einer Entscheidung auf judikativer oder administrativer Ebene hängt von der Erfüllung der jeweils einschlägigen formellen und materiellen Voraussetzungen ab. Betont wird, daneben sei auf der Rechtmäßigkeitsebene kein Raum für ein Akzeptanzkriterium.[2253]

Von einem obrigkeitlichen Staatsverständnis ist aufgrund dessen das Vorliegen oder Nichtvorliegen von Akzeptanz sogar ohne jeden Belang.[2254] Im Grundsatz wird dies auch für den modernen demokratischen Staat als gültig angesehen, da dieser Entscheidungen auch und gerade in gesellschaftlich konfliktträchtigen Fragen über Legitimationsmechanismen wie Wahlen und parlamentarische Mehrheitsentscheidungen fälle.[2255] Die Frage der Konsenssicherung in diesen Verfahren sei praktisch-politischer, nicht aber rechtlicher Natur.[2256] Neben der Legitimation von Rechtsakten als originär rechtlichem Problem sei Akzeptanz als Kategorie des öffentlichen Rechts sogar suspekt: sie sei entweder Empirie in Form der Untersuchung von Meinungsbildung und faktischer Zustimmung, und damit aus rechtlicher Sicht bedeutungslos. Oder aber Akzeptanz werde staatlicherseits hergestellt. In diesem Fall kehre sie jedoch das Konzept der Staatsgewalt um, die nach Art. 20 Abs. 2 GG vom Volke ausgehe.[2257] Ein Bezug zwischen Akzeptanz und Legitimation wird damit strikt abgelehnt.

Des Weiteren wird der „Akzeptanz des Rechts" die „Notwendigkeit eines besseren Politikmanagements" zugeordnet.[2258] Meist herrscht die Meinung vor, Akzeptanz sei ein individual- und sozialpsychologisches[2259] oder sozialwissenschaftliches[2260] Problem. Diesem sei der normativ begründete, verfassungsstaatliche Gesetzesgehorsam gegenüberzustellen. Sofern dem Recht Akzeptanzphänomene nicht in bestimmten Formen und anderen Terminologien (Verkehrssitte, Rücksichtnahme, Treu und Glauben) schon immer vertraut gewesen seien, sei in der rechtlichen Betrachtung kein Raum für die Berücksichtigung von Akzeptanzfragen. Der Rechtsstaat verlange von seinen Bürgern nicht, eine Regelung als gerecht oder angemessen zu akzeptieren, sondern lediglich, sie zu befolgen.[2261] Andernfalls bestehe die Gefahr, dass Nichtakzeptanz belohnt werde und zu Nachahmungen führe. Außerdem sei dem Risiko einer Politisierung nach Ende des parlamentarischen Entscheidungsprozesses entgegenzuwirken. Schließlich ließe sich ein Verstoß gegen das Mehrheitsprinzip beobachten: jenseits eines verfassungsmäßigen Grundkonsenses komme es nicht auf Konsens, sondern auf Mehrheit an.[2262] Im Ergebnis müsse jeder „Kampagne für

2251 Vgl. die Darstellung bei *Roellecke*, JZ 1997, 577, 578.
2252 Vgl. *Larenz* 1979, 152 ff.; *ders*. 1991, 210.
2253 *Hoffmann-Riem*, AöR 1990, 400, 415.
2254 *Hill*, JZ 1988, 377.
2255 *Würtenberger*, Sonderheft 39/1999 der KZfSS, 380, 381.
2256 *Schmidt-Aßmann*, AöR 1991, 329, 371.
2257 *Czybulka*, Die Verwaltung 1993, 27, 34.
2258 So der Titel eines Aufsatzes von *Hill* (JZ 1988, 377).
2259 *Würtenberger* 1987, 81; *ders*., NJW 1991, 257, 258; *ders*., Sonderheft 39/1999 der KZfSS, 380, 394.
2260 *Schmidt-Aßmann*, AöR 1991, 329, 371.
2261 *Röken*, DÖV 1989, 54, 56.
2262 *Röken*, DÖV 1989, 54, 58.

Akzeptanzverhalten eine Gegenkampagne für Gesetzesgehorsam entgegengesetzt werden".[2263]

Die Beschreibung der normativen Gültigkeit des Rechts unabhängig von seiner Akzeptanz bleibt allerdings unvollständig, solange die rechtspraktische Frage des Grundes der tatsächlichen Geltung von Rechtsnormen ausgeklammert wird. Hier hingegen wird deutlich, dass die Masse der Bürger in der Masse der rechtlich relevanten Lebenssituationen das Recht nicht deshalb befolgt, weil hinter diesem der staatliche Zwangsapparat steht, sondern weil sie die durch Rechtsregeln vorgegebene Lösung auf freiwilliger Basis für vernünftig erachtet – das heißt akzeptiert. Erst diese Situation verschafft dem Recht faktische Geltung, weil staatliche Repression allein auf Dauer nicht in der Lage ist, allgemeine Rechtsbefolgung zu erzwingen.[2264] *Herzog* hat das plastisch so ausgedrückt: „Wenn ein Staat...erst hinter jeden zweiten Bürger einen Polizisten stellen muss, um seinen Gesetzesgehorsam zu erzwingen, braucht er hinter jedem dritten Polizisten auch noch den vierten, der auf die drei anderen aufpasst, die ja auch nur Glieder der Gesellschaft sind."[2265] Ganz allgemein gilt deshalb, dass Kooperations- und Implementationsbereitschaft in jedem Gemeinschaftssystem nicht allein durch die Beachtung der Rechtsbindung und die Drohung mit Sanktion erreichbar sind.[2266] Will ein Staat nicht Gesetzesbefolgung um ihrer selbst willen, sondern zur Erreichung der Ziele, die der jeweiligen Norm zugrunde liegen, so ist er vor allem auf Billigung, Akzeptanz und freiwillige Befolgung dieser Norm angewiesen. Dieser Zusammenhang wird auch von den Autoren betont, die sich gegen eine rechtliche Fassbarkeit der Akzeptanz wenden.[2267]

7.2.2 Berücksichtigung von Akzeptanz bei der Rechtssetzung und -anwendung?

Erkennt man jedoch an, dass erst die auf Akzeptanz gegründete Rechtsbefolgung der Rechtsordnung wahre Geltung verschafft, so ist jede Rechtstheorie unzureichend, die das Recht von den betroffenen Bürgern abzukoppeln versucht.[2268] Daraus folgt unmittelbar die Frage, ob es zur Beschreibung des Akzeptanzphänomens nicht doch einer im strengen Sinn juristischen Begriffsbildung bedarf. Ansatzpunkte hierfür könnten sich aus verfassungsrechtlichen Grundsätzen wie dem Demokratieprinzip, der Gesetzesbindung der Gerichte und der Stellung der Abgeordneten ergeben.

Aus dem Demokratieprinzip leiten einigen Autoren Anforderungen an die Berücksichtigung von Akzeptanzerwägungen im gerichtlichen Prozess[2269] und im Verwaltungsverfahren[2270] ab. Ob und in wieweit dies zutreffend ist, kann nur eine Analyse von Art. 20 Abs. 2 GG erweisen. Legitimation staatlicher Herrschaft unter dem Grundgesetz muss nach Art. 20 Abs. 2 Satz 1 GG stets durch eine Rückführung auf das Volk als dem alleinigen Träger

2263 *Röken*, DÖV 1989, 54, 58.

2264 S. *Herzog* 1984, 128; *Kindermann* 1986, 65; *Hill*, JZ 1988, 377, *ders*., DÖV 1988, 666, 667; *Raiser* 1998, 109; *Würtenberger* 1987, 83; s.a. *Rehbinder* 2003, 30 f.; *Rüthers* 2005, 236 ff.

2265 *Herzog* 1984, 128.

2266 *Hoffmann-Riem*, AöR 1990, 400, 415; *Kindermann* 1986, 65.

2267 S. etwa *Herzog* 1984, 128; *Hill*, JZ 1988, 377, *ders*., DÖV 1988, 666, 667; *Würtenberger* 1987, 83.

2268 *Würtenberger* 1987, 83; gegen die aus einem derartigen Ansatz folgende Entfremdung von Bürger und Recht wendet sich bereits *v. Kirchmann* 1848, etwa 34 ff., 45.

2269 *Benda* (DÖV 1983, 305, 307) leitet aus Art. 20 Abs. 2 GG eine Verpflichtung der Rspr. ab, „mit den Vorstellungen in der Gesellschaft in Einklang" zu stehen; ähnlich *Perelman* 1982, 240.

2270 *Würtenberger*, NJW 1991, 257, 261, dort auch zum Bezug zur Idee der „responsiven Demokratie", nach der sich die Bürger in den grundlegenden Entscheidungen des Parlaments wiederfinden können sollen.

der Staatsgewalt begründet werden.[2271] Hierfür hat sich überwiegend der Begriff der „ununterbrochenen demokratischen Legitimationskette“ durchgesetzt.[2272] Unterschieden wird dabei – neben der funktionellen und institutionellen Dimension, die den verschiedenen Staatsgewalten je eigene Funktionen und Organe zuweist[2273] – zwischen zwei Legitimationsformen. Die personelle Legitimation wird durch eine Legitimationskette zwischen dem Volk und jedem einzelnen Amtswalter hergestellt.[2274] Sachliche Legitimation bezieht sich demgegenüber auf das Handeln des Amtswalters selbst.[2275] Sie entsteht zum einen durch dessen Bindung an das Gesetz, zum anderen durch Aufsicht und Weisung. Die Formen demokratischer Legitimation stehen allerdings nicht nebeneinander, sondern wirken zusammen und ergänzen sich gegenseitig.[2276]

Der Zusammenhang von Legitimation staatlicher Entscheidungen und ihrer Akzeptanz ist schwierig zu bestimmen. Zu einfach ist es, mit dem Postulat einer Dichotomie von Rechtfertigung und Hinnahme von Herrschaft jeden Bezug der beiden Kategorien zu leugnen.[2277] Vielmehr besteht zumindest Verwandtschaft zwischen Legitimation und Akzeptanz, da letztere sich etwa damit beschreiben lässt, es gehe „um eine *Legitimation* der öffentlichen Verwaltung durch eine Erledigung von Verwaltungsaufgaben, die vom Bürger anerkannt wird“.[2278]

Ein Beispiel aus den Niederlanden kann den Zusammenhang weiter verdeutlichen:[2279] Dort wurde im Zuge der Ölkrise im Jahre 1973 aus Energiespargründen trotz einer formal geltenden Höchstgeschwindigkeit auf Autobahnen von 120 km/h an die Bevölkerung appelliert, nicht schneller als 100 km/h zu fahren. Da dieser Grund für die Bürger einsichtig war, wurde die Empfehlung akzeptiert und weitgehend befolgt. Als nach Ende der Ölkrise jedoch ein Gesetz das niedrigere Tempolimit auch formell festschrieb, reagierten die Niederländer mit einer massenhaften Überschreitung der Höchstgeschwindigkeit. Allen Bemühungen der Polizei zum Trotz gelang es nicht, diese durchzusetzen. Interessanterweise blieb der Großteil der Fahrer aber weiterhin unter dem zuvor gültigen Limit von 120 km/h. Da die Regierung die Durchsetzung des Gesetzes für undurchführbar hielt und gleichzeitig durch eine Begrenzung auf 120 km/h keine höheren Gefahren für die Verkehrssicherheit zu befürchten waren, wurde die zulässige Geschwindigkeit wieder auf 120 km/h heraufgesetzt. Entscheidendes Argument war dabei die Nichtakzeptanz der Norm.[2280]

Das Phänomen einer derart massenhaften Normablehnung, die sich außerdem in permanenter Gebotsüberschreitung manifestiert, stellt unter demokratietheoretischen Gesichtspunkten die Legitimität staatlichen Handelns in diesem Einzelfall grundsätzlich in Frage. Ausgangspunkt ist das Erfordernis der Legitimierung aller staatlichen Gewalt durch das

2271 Zur Legitimation allgemein s. etwa Sachs-*Sachs*, Art. 20 Rn. 28 ff.; v. Mangoldt/Klein/Starck-*Sommermann*, Art. 20 Rn. 137 ff.

2272 Im Anschluss an *Böckenförde*, HdbStR II (2004) § 24 Rn. 11 ff., s.a. HdbStR I (1987), § 22 Rn. 11 ff.; vgl. zu diesem Ansatz und seinem Anschluss an die Demokratiekonzeption *C. Schmitts* z.B. *Hanebeck*, DÖV 2004, 901, 902 f. (s.a. ebd., 903 zu weiteren Vertretern dieser Auffassung).

2273 Diese Dimension begründet eine grundsätzliche Legitimation zur Ausübung staatlicher Gewalt, ersetzt jedoch nicht die personelle und sachliche Legitimation, s. *Böckenförde*, HdbStR II (2004) § 24 Rn. 15.

2274 BVerfGE 47, 253 (275); *Böckenförde*, HdbStR II (2004), § 24 Rn. 16 ff.; M/D-*Herzog*, Art. 20 Rn. 53 ff.; AK GG-*Stein*, Art. 20 Abs. 1-3 III Rn. 38; Jarass/Pieroth-*Pieroth*, Art. 20 Rn. 9 ff.

2275 BVerfGE 9, 268 (281 f.); 93, 37 (67); *Böckenförde*, HdbStR II (2004), § 24 Rn. 21 f.

2276 BVerfGE 83, 60 (72); 93, 37 (67); v. Mangoldt/Klein/Starck-*Sommermann*, Art. 20 Rn. 163 ff.; AK GG-*Stein*, Art. 20 Abs. 1-3 III Rn. 40.

2277 So aber *Schmidt-Aßmann*, AöR 1991, 329, 369 ff.

2278 *Würtenberger*, NJW 1991, 257, 258 (Hervorhebung hinzugefügt).

2279 Vgl. *Sagel-Grande*, ZRP 1990, 26 ff.

2280 Begründung des Beschlusses v. 21.4.1988 zur Änderung der Reglement Verkeersregels en Verkeerstekens, Staatsbl. 1988, 175 (zitiert nach: *Sagel-Grande*, ZRP 1990, 26).

Volk, wie sie im Demokratieprinzip des Art. 20 Abs. 2 Satz 1 GG ihren Ausdruck gefunden hat. Dessen theoretische Fundierung liegt einerseits in der Identität von Regierenden und Regierten: Nach der Definition *Pufendorfs* ist Demokratie die Gesellschaftsordnung, „wo derjenige, der befiehlt und derjenige, der gehorcht, derselbe ist".[2281] Gleichzeitig gründet dieses Prinzip aber auch in der Menschenwürde: „Demokratie ist die organisatorische *Konsequenz* der Menschenwürde".[2282] Vor diesem Hintergrund kann ein Demokratiemodell, das sich selbst ernst nimmt, nicht die Ablehnung einer staatlichen Maßnahme durch die überwältigende Mehrheit der Mitglieder des Volkes ignorieren.

Das wird auch im Vergleich des beschriebenen Phänomens mit der von der herrschenden Meinung geforderten Legitimation im Wege einer „ununterbrochenen Legitimationskette" deutlich. Diese besteht beispielsweise dann, wenn das Volk einen Bundestag und dieser einen Bundeskanzler wählt, welcher einen Minister vorschlägt, der vom Bundespräsidenten (der selbst indirekt über eine andere Kette legitimiert ist) ernannt wird, später eine Rechtsverordnung erlässt, die einen vor dreißig Jahren eingestellten Beamten mit Befugnissen ausstattet und dieser lange Zeit später unter einer neuen Regierung tätig wird. Die Vorstellung, die am Ende dieser Kette ausgeübte Staatsgewalt ginge tatsächlich vom Volk aus, ist mit Recht verschiedentlich als empirisch nicht haltbar und irreführend kritisiert worden.[2283] Auch die Konzeption eines „Volkswillens", soweit sie ein kollektives Entscheidungssubjekt unterstelle, entbehre schon immer der gesellschaftlichen Grundlage.[2284] Dieser Kritik liegt ein „selbstverwaltungsfreundliche[s], partizipative[s] Demokratieverständnis" zugrunde, das sich gegen die „Idee einer allein auf den parlamentarischen Wahlakt fixierten Demokratiekonzeption" wendet.[2285] Ihren Vertretern zufolge ist beispielsweise – im Unterschied zur Rechtsprechung des Bundesverfassungsgerichts und der herrschenden Meinung in der Literatur – ein Ausländerwahlrecht[2286] und eine Arbeitnehmermitbestimmung in öffentlichen Einrichtungen der Verwaltung auch bei Entscheidungen, die für die Erfüllung hoheitlicher Aufgaben von Bedeutung sind,[2287] zulässig.

2281 Zitiert nach *Neumann* 1998, 60.

2282 *Häberle*, KritV 1995, 298, 303 (Hervorhebung im Original); ähnlich *Maihofer* 1994, 490 ff.; *Rinken*, KritV 1996, 282, 295.

2283 *Blanke*, KJ 1998, 452, 465 ff. et passim; *Rinken*, KritV 1996, 282, 292 ff.; in dieser Richtung auch OVG NW, PersR 1996, 249, 254. Die Entscheidung wurde durch BVerwGE 106, 64 aufgehoben, das relevante Gesetz Ende 2002 vom BVerfG (E 107, 59) aber für verfassungsmäßig erklärt; s.u. Fn. 2287.

2284 *Maus*, KJ 1991, 137. Vertreter dieser Auffassung können sich auf *Max Weber* berufen: „Begriffe wie ‚Wille des Volkes', wahrer Wille des Volkes usw. ...sind *Fiktionen*." (zitiert nach: *Neumann* 1998, 53, Hervorhebung im Original). Nach *Maus*, KJ 1991, 137, 150 ist auch das „Volk" selbst ein fiktiver Begriff.

2285 *Blanke*, PersR 1997, 329, 459; s.a. *Roßnagel*, KritV 1986, 343 ff.; man kann schlagwortartig zwischen diesem „pluralistischen" Konzept und dem „monistischen" der h.M. unterscheiden, s. *Hanebeck*, DÖV 2004, 901 ff.; s. zu den Vertretern der erstgenannten Richtung auch die weiteren Nachweise ebd., 903.

2286 Das BVerfG (E 83, 37; 83, 60) hatte das Stimmrecht von Ausländern auch auf kommunaler Ebene für verfassungswidrig erklärt (zur Kritik *Bryde*, Staatswissenschaften und Staatspraxis 1994, 305 ff.). Daraufhin wurde im Zuge der „Maastricht-Novelle" des Grundgesetzes v. 21.12.1992 (BGBl. I, 2086) Art. 28 Abs. 1 Satz 3 GG entsprechend geändert.

2287 Nach BVerfGE 93, 37; VerfGH NW, DVBl 1986, 1196; HessStGH, PersR 1986, 148 ff.; VerfGH RP, PersR 1994, 269 ff. darf es aufgrund mangelnder demokratischer Legitimierung der Arbeitnehmervertreter bei diesen Entscheidungen keine Mitbestimmung geben; kritisch *Rinken*, KritV 1996, 282 ff.; *Blanke*, PersR 1997, 329 ff.; zur Gegenkritik vgl. v. Mangoldt/Klein/Starck-*Sommermann*, Art. 20 Rn. 182 ff. Das BVerfG hat zuletzt allerdings – bezogen auf die Arbeitnehmermitbestimmung außerhalb der unmittelbaren Staatsverwaltung und der gemeindlichen Selbstverwaltung – Abweichungen vom Erfordernis lückenloser personeller demokratischer Legitimation zugelassen, s. BVerfGE 107, 59 ff.; hierzu *Musil*, DÖV 2004, 116 ff.; *Unruh*, JZ 2003, 1061 ff.; *Becker*, DÖV 2004, 910 ff.

Diesen Problemen kann hier nicht im Einzelnen nachgegangen werden. Vergleicht man aber die Ausübung von Herrschaft durch „das Volk“, vermittelt über eine Vielzahl von Zwischenstufen, mit dem Fall der realen Nichtakzeptanz einer staatlichen Maßnahme durch die überwältigende Mehrheit der Bürger, so erscheint letztere als eine viel deutlichere und unmittelbarere Ausdrucksform der in Art. 20 Abs. 2 Satz 1 GG postulierten Herrschaft des Volkes. Auch aus dem rechtlichen Blickwinkel heraus hängen damit Akzeptanz- und Legitimationstheorien eng zusammen.[2288]

Ist mit Art. 20 Abs. 2 Satz 1 GG ein verfassungsrechtlicher Anknüpfungspunkt gefunden, so begegnet die Berücksichtigung von Akzeptanzfaktoren doch einer Reihe von gravierenden Bedenken. Zwar könnte rein begrifflich eine massenhafte Nichtakzeptanz wie im niederländischen Beispiel das Ausgehen (beziehungsweise in diesem Fall das Verhindern des Ausgehens) von Staatsgewalt durch das Volk im Sinne einer demokratischen Legitimation sein. Diese Form des Ausdrucks der Herrschaft des Volkes würde aber Art. 20 Abs. 2 Satz 2 GG widersprechen, der insoweit nur drei spezifische Formen kennt, nämlich die Ausübung durch Wahlen, Abstimmungen und durch besondere Organe der Gesetzgebung, der vollziehenden Gewalt und der Rechtsprechung. Hier ist eindeutig kein Raum für die Einbeziehung von Akzeptanzgesichtspunkten. Zwar ließen sich diese – zumindest hinsichtlich der oben angesprochenen massenhaft manifestierten Nichtakzeptanz – in ein allgemeines Demokratiemodell einfügen. Maßstab der rechtlichen Betrachtung kann jedoch nicht ein abstraktes, sondern nur das konkrete Modell des Grundgesetzes sein, weil in Anbetracht der Vielfalt der unterschiedlichen Auffassungen über den Inhalt des Demokratieprinzips „die verfassungsrechtlich maßgebliche Bedeutung des Begriffs nur anhand der konkreten Ausformung der Demokratie durch die Verfassung gewonnen werden“ kann.[2289] In der Verfassungsordnung des Grundgesetzes verfügt aber auch das Volk nur über begrenzte Kompetenzen und Handlungsmöglichkeiten, zu denen die Bundestagswahl und bestimmte Abstimmungen gehören, nicht jedoch weitere – rechtlich verbindliche – Einwirkungen auf den Bundestag.[2290] Divergenzen zwischen Volkswillen und Abgeordnetenhandeln können nur auf dem Wege ausgetragen werden, den das Grundgesetz vorgibt: nämlich durch unterbleibende Neuwahl eines Abgeordneten oder seiner Partei.[2291]

Ein zweiter denkbarer Ansatzpunkt findet sich in der Gesetzesbindung der Gerichte nach Art. 20 Abs. 3 GG. Aus dieser wird geschlossen, die Judikative müsse bei ihren Entscheidungen Akzeptanzgesichtspunkte berücksichtigen, weil sich im Gesetz die Rechtsüberzeugungen der Gesellschaft spiegelten, wie sie mit Abschluss des parlamentarischen Verfahrens für akzeptabel erklärt würden.[2292] Problematisch ist, dass in dieser Konzeption die Variante, dass sich die allgemeinen Akzeptanzgesichtspunkte – objektiv oder zur Überzeugung des Richters – gerade nicht im Gesetz spiegeln, nicht vorkommt. Grundsätzlich ist fraglich, ob die Pflicht, im Gesetz festgeschriebene Akzeptanzüberzeugungen zu berücksichtigen, neben der Gesetzesbindung des Richters eine selbständige Bedeutung hat. Ist die Beurteilung der Kongruenz von Gesetzesinhalt und gesellschaftlicher Akzeptanz nicht Aufgabe der Gerichte, so ist die Aussage, diese seien an die Akzeptanz einer Maßnahme, wie sie im Gesetz Ausdruck gefunden habe, gebunden, gleichbedeutend mit einer schlichten Bindung an dieses Gesetz. Wenn schließlich der „Akzeptanzhorizont“ der Gesellschaft

2288 *Czybulka*, Die Verwaltung 1993, 27, 28; *Sagel-Grande*, ZRP 1990, 26, 29; zum Zusammenhang von Legitimation und Akzeptanz auch *Würtenberger* 1987, 82 ff., s.a. oben Fn. 2245.

2289 *Hesse* 1995, Rn. 127; zu den durch Art. 20 Abs. 2 Satz 2 GG vorgegebenen Grenzen auch *Schmidt*, JZ 1978, 293, 294.

2290 Sachs-*Magiera*, Art. 38 Rn. 8.

2291 V. Mangoldt/Klein/Starck-*Achterberg/Schulte*, Art. 38 Rn. 32.

2292 *Benda*, DÖV 1983, 305, 307; kritisch *Limbach* 1998, 260 ff.

in der Verfassung verortet wird,[2293] so ist festzustellen, dass ein derartig verobjektivierter, mit der kodifizierten Verfassung identischer Akzeptanzbegriff weder theoretisch notwendig noch praktisch relevant ist.

Der Einfluss von Akzeptanzkriterien auf Entscheidungen der Gerichte ist darüber hinaus auch nicht erstrebenswert. Denn zum einen besteht die Gefahr, dass die Gerichte das, was sie selbst für akzeptabel halten, als allgemeinen Akzeptanzhorizont bezeichnen. Es darf aber keine Umdeutung von Gesetzen, und schon gar nicht der Verfassung, nach tagespolitischer Akzeptanz geben.[2294] Überdies trüge eine Orientierung an der gesellschaftlichen Akzeptanz einer Entscheidung Gefahren für die Unabhängigkeit der Gerichte in sich. Damit würde aber das Ziel einer volksnäheren Rechtsprechung doppelt konterkariert. Zum einen, weil das Schielen auf kurzfristigen Beifall notwendigerweise zur Diskontinuität der Rechtsprechung und damit im Ergebnis zu weniger Akzeptanz einer einzelnen Entscheidung führen würde – diese erhielte den Makel der Beliebigkeit. Und zum anderen, weil eine derart in ihren Ansprüchen „korrumpierte" Justiz selbst in der Akzeptanz der Bevölkerung sinken würde.[2295] Akzeptanzfragen sind deshalb an erster Stelle nicht vom Richter, sondern – politisch – vom Gesetzgeber zu lösen.[2296]

Hinsichtlich einer Akzeptanzbindung des Gesetzgebers ist angemerkt worden, Art. 38 Abs. 1 Satz 2 GG sei eine „Vorschrift, auf die sich sowohl die Akzeptanzlehre wie auch ihre Gegner berufen können".[2297] Nach dieser Norm sind die Abgeordneten des Bundestages – außer der Verfassung[2298] – nur ihrem Gewissen unterworfen. Die Relevanz von Akzeptanz für das Handeln der Abgeordneten ließe sich damit begründen, dass diese Vertreter des Volkes sind und deshalb dessen Willen berücksichtigen müssen. Dieser Wille drückt sich zwar in Wahlen aus, dort aber eben nur in sehr groben politischen Richtungen, während die Akzeptanz einer konkreten Maßnahme ein viel unmittelbarer Ausdruck des Volkswillens ist, dem sich dessen Vertreter nicht entziehen können. Aus Art. 38 Abs. 1 Satz 2 GG folgt auch eine Pflicht der Abgeordneten, Allgemeininteressen zu berücksichtigen.[2299] Das demokratische Repräsentationsprinzip des Grundgesetzes fordert schließlich als notwendige Ergänzung der periodischen Wahl die permanente demokratische Kommunikation zwischen Volk und Parlament, um die staatliche Willensbildung im Parlament an die politische Willensbildung im Volk zu binden.[2300]

Es ist indes sehr zweifelhaft, ob sich diese Überlegungen zu einer Pflicht zur Berücksichtigung von Akzeptanz im Gesetzgebungsprozess verdichten. Zunächst wirken dem einige Elemente des Art. 38 Abs. 1 Satz 2 GG selbst entgegen. Ziel der Norm ist gerade die Unabhängigkeit von Fremdbestimmung mittels der Übertragung eines „freien" oder „repräsentativen" Mandats.[2301] Auch die Akzeptanz oder Nichtakzeptanz einer Maßnahme

2293 So ausdrücklich *Benda*, DÖV 1983, 305, 307.

2294 So auch *Benda*, DÖV 1983, 305, 308; zu weitgehend deshalb *Perelman* 1982, 240, wonach der Richter „das Gesetz flexibel gestalten [muss], damit das Recht, das er spricht, akzeptiert werde".

2295 *Benda*, DÖV 1983, 305, 309.

2296 *Achterberg* 1986, § 7 Rn. 51.

2297 *Röken*, DÖV 1989, 54, 55 (allerdings ohne nähere Begründung).

2298 Die sprachliche Formulierung von Art. 38 Abs. 1 Satz 2 GG („nur" ihrem Gewissen unterworfen) bedeutet nicht, dass die Abgeordneten nicht auch an die Verfassung gebunden sind, vgl. v. Mangoldt/Klein/Starck-*Achterberg/Schulte*, Art. 38 Rn. 39 m.w.N.

2299 Sachs-*Magiera*, Art. 38 Rn. 45.

2300 *Magiera* 1979, 148 ff.

2301 Die Begriffsbildung ist insoweit uneinheitlich: für „frei" Sachs-*Magiera* Art. 38 Rn. 46; *Stern* 1984, 1070; AK GG-*Schneider*, Art. 38 Rn. 39 ff.; Jarass/Pieroth-*Pieroth*, Art. 38 Rn. 26; für „repräsentativ" v. Mangoldt/Klein/Starck-*Achterberg/Schulte*, Art. 38 Rn. 33. In der Sache besteht aber weitgehend Einigkeit.

durch die Rechtsunterworfenen lässt sich als eine Form von Fremdbestimmung fassen, weil die Verfassungsordnung des Grundgesetzes über das Repräsentationsprinzip so organisiert ist, dass der Staatswille rechtsverbindlich autonom im Parlament gebildet wird.[2302] Die aus Art. 38 Abs. 1 Satz 2 GG folgende Pflicht zur Wahrnehmung von Allgemeininteressen impliziert schließlich nicht, dass diese Interessen gerade auf der Basis von Akzeptanzverhalten festgelegt werden. Eine rechtlich abgesicherte Bindung des Bundestages an die öffentliche Meinung gibt es deshalb im Ergebnis nicht.[2303] Allerdings ist die Rückkopplung an den durch die Akzeptanz oder Ablehnung zum Ausdruck gebrachten Volkswillen Teil der Gewissensbindung der Abgeordneten nach Art. 38 Abs. 1 Satz 2 GG. Fühlen sich diese nicht dementsprechend verpflichtet, besteht die Gefahr einer Abkopplung der Volksvertreter vom Volk. Dieser Aspekt ist aber nicht rechtlich fassbar und schon gar nicht justiziabel.

Zudem ist unklar, wie Akzeptanz (oder ihr Fehlen) in einem rechtlichen Verfahren festgestellt werden könnte. Eine Abstimmung käme in Frage, wäre aber gerade eine direkte und ausdrückliche Legitimation durch das Volk und damit keine Akzeptanzfrage mehr.[2304] Im Übrigen kämen Gutachten, Erhebungen oder die Inanspruchnahme der Demoskopie in Betracht.[2305] Neben dem Problem der Genauigkeit derartiger Instrumente würden sich auch Fragen der Gewichtung stellen.[2306] Es müsste geklärt werden, welcher Anteil der Betroffenen eine Maßnahme akzeptieren müsste, und ob auch der lautstarke Protest einer Minderheit ausreichen könnte. Diese könnte die Gefühle einer schweigenden Mehrheit ausdrücken, was aber nicht notwendigerweise der Fall ist. Diese Schwierigkeiten sind kaum lösbar.

Schließlich gerät eine Berücksichtigung von Akzeptanzfaktoren auch in Widerspruch zu Verfassungswerten. Soll die Nichtakzeptanz durch eine – eventuell massiv auftretende – Minderheit ausreichen, eine Maßnahme zu verhindern, so ist ein Konflikt mit dem Demokratieprinzip die Folge. Auch wenn eine (wie auch immer festgestellte) Mehrheit erforderlich wäre, stünde zumindest die Repräsentativität des momentanen Systems entgegen. Daneben stellen sich aber auch noch Probleme aus dem Grundrechtsbereich. Selbst die mehrheitliche Ablehnung einer staatlichen Entscheidung kann deren Rechtmäßigkeit nicht in Frage stellen, wenn die Maßnahme wegen der Schutzbedürftigkeit einer Minderheit oder eines Einzelnen verfassungsrechtlich geboten ist. Umgekehrt wird ein verfassungsrechtlich unzulässiger Eingriff in Grundrechtspositionen eines Bürgers nicht dadurch rechtmäßig, dass eine Mehrheit der Rechtsunterworfenen ihn unterstützt.

Wenn man aber konstatiert, dass Akzeptanz oder ihr Fehlen weder verfassungsrechtliche Verfahrens- und sonstige Regeln, noch einfaches Recht, noch die Rechtmäßigkeit von Gerichts- und Verwaltungsentscheidungen in Frage stellen kann, dann ist es tatsächlich nicht möglich, Akzeptanz als solche in das vorhandene rechtliche Kategoriensystem unter dem Grundgesetz zu integrieren. Denn um ein Rechtsproblem würde es sich nur dann handeln, wenn die Beantwortung der Frage, ob eine bestimmte Maßnahme akzeptiert wird,

2302 Sachs-*Magiera*, Art. 38 Rn. 46.

2303 V. Mangoldt/Klein/Starck-*Achterberg/Schulte*, Art. 38 Rn. 20. Die Ausführlichkeit der dortigen Begründung ist allerdings schwer nachvollziehbar, da ein derartiger rechtlich verbindlicher Einfluss – soweit ersichtlich – von niemandem behauptet wird. Auch ansonsten wird von Akzeptanzkritikern bisweilen ein argumentativer Gegner bekämpft, den es realiter nicht gibt; s. z.B. *Röken*, DÖV 1989, 54 ff.

2304 Zur Diskussion um die Zulässigkeit von Volksabstimmungen unter dem GG vgl. etwa AK GG-*Stein*, Art. 20 Abs. 1-3 III Rn. 51 f.; v. Mangoldt/Klein/Starck-*Sommermann*, Art. 20 Rn. 156 ff. m.w.N.

2305 *Benda*, DÖV 1983, 305, 309.

2306 *Röken*, DÖV 1989, 54, 58.

auf deren Rechtmäßigkeit oder Rechtswidrigkeit Einfluss hätte. Das ist nach dem Vorstehenden nicht der Fall. Zwar sollte nicht übersehen werden, dass direkte Aktionen der Nichtakzeptanz historisch eine wichtige Funktion bei der Durchsetzung der meisten Institutionen der heutigen freiheitlichen Demokratie gehabt haben.[2307] Eine organisierte Akzeptanzverweigerung kann deshalb nicht nur ein Mittel zur „Technikgestaltung von unten“,[2308] sondern auch zur Gestaltung des Rechts sein. Das ändert die Betrachtung de lege lata jedoch nicht.

Wegen der aufgezeigten grundsätzlichen Probleme erscheint es darüber hinaus auch schwer vorstellbar, de lege ferenda eine rechtliche Kategorie der Akzeptanz einzuführen. Nichtsdestotrotz fallen vielfältige Bezüge und Überschneidungen mit originären Rechtsfragen auf. So wird sich etwa die Handhabbarkeit einer per Gesetz eingeführten neuen Technik für ältere und behinderte Mitbürger stark auf ihre Akzeptanz auswirken. Gleichzeitig ergeben sich hier aber auch grundrechtliche Anforderungen an die Vermeidung von Benachteiligungen aus den allgemeinen und besonderen Gleichheitssätzen des Art. 3 GG. Die Einhaltung der jeweiligen, durch Verfassungs- oder einfaches Recht vorgegebenen Verfahrensvorschriften unterliegt der juristischen Betrachtung im eigentlichen Sinn; diese Mechanismen haben aber auch Einfluss auf die Akzeptanz des durch diesen Prozess gewonnenen Ergebnisses – sei es, weil sie auf die Berücksichtigung, oder zumindest die Artikulation, von Minderheitspositionen angelegt sind, sei es, weil sie unabhängige Verfahren ohne Ansehung der jeweiligen Person garantieren. Ein weiteres Beispiel ist die Struktur von Rechtsregeln: Ein übersichtlich gestaltetes, jedermann verständliches Gesetz wird leichter auf Akzeptanz stoßen; gleichzeitig ist das Gebot der Normenklarheit über das Rechtsstaatsprinzip verfassungsrechtlich verankert.[2309] Schließlich ist eine angemessene Information über Gesetzgebungsverfahren und Gesetzesinhalt sowohl ein akzeptanzfördernder Faktor als auch durch das Demokratieprinzip des Grundgesetzes geboten, weil Information eine Voraussetzung für die Ausübung staatspolitischer Bürgerrechte ist.[2310]

Überlappen sich damit Akzeptanz- und Rechtsfragen in vielen Bereichen, so dürfen beide Sphären dennoch nicht vermengt werden. Die Erkenntnis, dass die Beachtung oder Nichtbeachtung rechtlicher Anforderungen an eine Maßnahme Auswirkungen auf deren Akzeptanz hat, ist für sich genommen relativ banal. Die Einhaltung verfassungsrechtlicher Anforderungen kann sich auch auf andere Bereiche auswirken (beispielsweise das Abstimmungsverhalten bei nachfolgenden Wahlen oder die Investitionsbereitschaft ausländischer Konzerne), ohne dass derartige Folgen deshalb selbst zu rechtlichen Problemen würden. Von der Feststellung, dass Recht und Akzeptanz sich wechselseitig beeinflussen, kann deshalb nicht darauf geschlossen werden, dass Akzeptanz eine allgemeine rechtliche Kategorie bildet.

7.2.3 Ergebnis

Die Akzeptanz einer staatlichen Maßnahme ist im Ergebnis weder ein allgemeiner Faktor für die Rechtsanwendung, noch gibt es in der Rechtsordnung eine ausdrückliche An-

2307 AK GG-*Stein*, Art. 20 Abs. 1-3 III Rn. 55 ff.

2308 Dazu *Roßnagel/Wedde/Hammer/Pordesch* 1990, 278.

2309 Vgl. Sachs-*Sachs*, Art. 20 Rn. 123 ff. Das BVerfG hat etwa in BVerfGE 1, 14 (45) festgestellt, dass Gesetze widerspruchsfrei sein müssen, während die Entscheidungen BVerfGE 14, 13 (16); 47, 239 (247) die Verständlichkeit für den Adressaten betonen. Nach BVerfGE 17, 306 (318) ist es unzulässig, den Regelungsgehalt zu verschleiern; auf Probleme der Gesetzgebungstechnik (oder „-kultur“) weist auch *Hill*, DÖV 1988, 666, 667 f. hin.

2310 *Hill*, DÖV 1988, 666, 669.

ordnung an den Rechtsanwender, Akzeptanzkriterien zu berücksichtigen. Die richterliche Rechtsfortbildung kann indes dazu beitragen, dass das Recht nicht akzeptanzblind wird. Gerade im Bereich des Verfassungsrechts ist eine hinreichend verdichtete gesellschaftliche Akzeptanz für die Auslegung allgemeiner Begriffe relevant. So führten beispielsweise die veränderten Auffassungen in der Gesellschaft über die Gleichberechtigung von Frau und Mann auch zu einer Änderung der Rechtsprechung des Bundesverfassungsgerichts zu dieser Frage.[2311] Wenn in derartigen Bereichen ein hoher Grad von Übereinstimmung in der Gesellschaft festgestellt werden kann, so wird diese Form der Akzeptanz in aller Regel Einfluss auf die Rechtsentwicklung nehmen. Dies bringen Urteilsformulierungen zum Ausdruck, die auf Maßstäbe wie das „allgemeine Rechtsbewusstsein" oder „fundierte allgemeine Gerechtigkeitsvorstellungen" rekurrieren.[2312] Dieser Einfluss ist, sofern er sich im Rahmen der anerkannten Auslegungsregeln bewegt, im Grundsatz positiv zu bewerten, da er eine Abkoppelung des Rechts von seinen tatsächlichen Wirksamkeitsbedingungen verhindert.

Gegenwärtig lassen sich darüber hinaus Versuche beobachten, das formal-juristische Konfliktlösungsinstrumentarium durch den Einsatz mediativer Prozesse im gerichtlichen Verfahren zu ergänzen.[2313] Sollte diese Tendenz anhalten, könnten Akzeptanzfaktoren in Zukunft für die Tätigkeit der Juristen eine zunehmende Bedeutung erlangen, weil im Rahmen der Mediation – anders als im bisherigen Prozess – die Akzeptanz des Ergebnisses durch die Konfliktbeteiligten schon im Ausgangspunkt durch den Mediator anzustreben und zu berücksichtigen ist.

Das allgemeine Verhältnis von Akzeptanz und Recht bleibt dagegen bei allen wechselseitigen Beziehungen das zweier voneinander getrennter Bereiche. Am klarsten lässt sich das beschreiben, wenn man Akzeptanz nicht als normativen oder Rechtsbegriff, sondern als eine Frage der faktischen Vorraussetzungen des Rechts begreift.[2314] Das Recht selbst kann seine eigene Verwurzelung in der Gesellschaft nicht sehen und Normakzeptanz nicht erkennen.[2315] Wohl kann dies der Jurist und Rechtsanwender. Dieser darf eine konkrete Entscheidung jedoch nicht abgekoppelt vom Gesetz mit dem begründen, was er selbst für sich oder für andere als akzeptabel erachtet. Die Blindheit des Rechts für Akzeptanzfaktoren resultiert unter anderem daraus, dass Akzeptanz und Rechtsbewusstsein in einem persönlichen Bereich wurzeln, den das Recht bewusst ausnimmt und auch gar nicht erreichen

2311 Dabei wurde etwa 1954 das Nachtarbeitsverbot für Frauen durch BVerfGE 5, 9 (11 f.), und noch zu Beginn der 80er Jahre des vorherigen Jahrhunderts von anderen Gerichten (VG Berlin, NJW 1980, 1066 f.; OVG Berlin, NJW 1982, 66) für verfassungsgemäß erklärt, bis das BVerfG 1992 seine Rspr. änderte (BVerfGE 85, 191); zur Entwicklung vgl. v. Münch/Kunig-*Gubelt*, Art. 3 Rn 84 ff.; v. Mangoldt/Klein/Starck-*Starck*, Art 3 Rn. 295 ff.

2312 *Benda*, DÖV 1983, 305, 307 f. unter Hinweis auf BVerfGE 10, 59 (66); 37, 67 (81); 39, 148 (153); 39, 169 (186); 42, 64 (72); 45, 187 (259).

2313 Eines der wichtigsten Modellprojekte ist das des Landes Niedersachsen; vgl. hierzu die Informationen unter http://www.mediation-in-niedersachsen.de/index.html; s.a. *Hager*, ZKM 2003, 52 ff.; *Wolf/Weber/Knauer*, NJW 2003, 1488 ff.; *Koch*, NJ 2005, 97 ff.

2314 *Roellecke*, JZ 1997, 577.

2315 *Roellecke*, JZ 1997, 577, 579. Hier klingen – bei aller Vorsicht – Parallelen zur Rechtstheorie von *H. L. A. Hart* (1973, insbesondere 135 ff., 142 ff.) an, in dessen System zwei Regeltypen existieren, nämlich primäre (Verpflichtungs-)Regeln, die sich an die Individuen richten, und sekundäre (Erkenntnis-) Regeln, die sich mit der Gültigkeit von Regeln beschäftigen. Die höchste Erkenntnisregel, also etwa die der Gültigkeit der Verfassung, ist danach notwendigerweise keine Rechtsregel mehr, sondern existiert nur „als komplexe, aber normalerweise koordinierte Praxis der Gerichte, Beamten und Privatpersonen, wenn sie mit Hilfe gewisser Kriterien identifizieren, was Recht ist" (*Hart* 1973, 155). Diese Art von Faktizität ähnelt der Aussage, das Recht könne seine eigene Verwurzelung in der Gesellschaft nicht sehen.

kann.[2316] Zwar sind Recht und Normakzeptanz über die unterschiedlichen Rollen der Akteure miteinander verbunden: Jeder Richter ist gleichzeitig ein mit einem Rechtsbewusstsein ausgestatteter Bürger und verfügt überdies über Zusatzwissen aus anderen, nichtrechtlichen, Sozialzusammenhängen. Jenseits dieser personalen Verbindung handelt es sich aber um nebeneinander stehende Systeme. Daraus folgt auch, dass für die originär rechtliche Bewertung von Chipkartenausweisen deren Akzeptanz außer Betracht bleiben muss.

Diese Trennung zwischen der normativen und der faktischen Sphäre ist allerdings kein Nachteil. Vielmehr bietet gerade sie die Möglichkeit einer umfassenden Betrachtung der Voraussetzungen und Auswirkungen der Einführung von Chipkartenausweisen. Unter politikpsychologischen wie rechtssoziologischen Gesichtspunkten stellen sich im Bereich der Akzeptanz entscheidende Fragen, die für die Umsetzbarkeit zu beantworten sind. Eine sorgfältige Akzeptanzanalyse ist insbesondere dann erforderlich, wenn es um Vorhaben geht, die wie der digitale Personalausweis und die elektronische Gesundheitskarte über ein hohes Konfliktpotential verfügen. Derartige Analysen sind ein wichtiges Mittel der Rechtspolitik.

7.3 Einflussfaktoren für die Akzeptanz von Chipkartenausweisen

Die Akzeptanz von Chipkartenausweisen wird zum Teil von denselben allgemeinen Faktoren beeinflusst wie die Akzeptanz jeder anderen staatlichen Maßnahme. Mit der Volkszählung und der Einführung des maschinenlesbaren Personalausweises gibt es in Deutschland überdies zwei Akzeptanzbeispiele, die in Fallstudien für die zu erwartende Debatte fruchtbar gemacht werden können. Schließlich lassen sich einige Besonderheiten der einzelnen Ausweise und ihrer Funktionen herausarbeiten.

7.3.1 Allgemeine Einflussfaktoren für die Akzeptanz staatlicher Maßnahmen

7.3.1.1 Bisherige Kategorisierungen

In der Literatur wird eine Reihe allgemeiner Einflussfaktoren für die Akzeptanz staatlicher Maßnahmen genannt.[2317] Ein ausdifferenziertes System unterschiedlicher Akzeptanzfaktoren findet sich zunächst bei *Würtenberger*.[2318] Die Akzeptanz einer staatlichen Maßnahme kann danach hervorgerufen werden durch:

- Autonome Entscheidung. Dabei wird das Recht auf der Basis individueller Wertungsdispositionen als ein „Akt der Selbstgesetzgebung“ und „natürlich richtig“ empfunden. Eine derartige Einstellung entspringt der Gewissensentscheidung und dem Rechtsgefühl.
- Tradition und Kontinuität. Hergebrachtes Recht hat die Vermutung der Richtigkeit für sich, während Rechtsänderungen rechtfertigungsbedürftig sind. Gleichzeitig schlägt sich der Schutz von Dispositionen („Investitionen in die Rechtsordnung“) nieder.
- Konsensbildendes Verfahren. Ein offener Meinungsbildungsprozess bereits im frühen Stadium des Verfahrens der Normfindung kann die Akzeptanz des Ergebnisses erhöhen. Dazu muss die politische Mehrheit, insbesondere bei weitreichenden Ent-

2316 *Roellecke*, JZ 1997, 577, 581.
2317 Vgl. zusammenfassend *Roßnagel/Hornung*, in: Reichl/Roßnagel/Müller 2005, 306.
2318 Sonderheft 39/1999 der KZfSS, 380, 386 ff.; *ders*. 1987, 84 ff., 92 ff.; s.a. *ders*. 1996, 73 ff.; 98 ff.; *ders*., NJW 1991, 257 ff.

scheidungen, Minderheitspositionen mit einbeziehen. Möglichkeiten hierfür finden sich im parlamentarischen Verfahren, aber auch im Verwaltungsprozess. Konsensbildende Verfahren führen nach diskurstheoretischen Ansätzen außerdem nicht nur zur Akzeptanz, sondern auch zur rechtlichen Richtigkeit des Ergebnisses. Zu beachten ist allerdings, dass wegen eines zu beobachtenden Vertrauensverlusts in demokratische Prozesse und Institutionen Gesetze nicht schon deshalb akzeptiert werden, weil sie verfassungsrechtlich korrekt zustande gekommen sind. Es geht damit auch um die Integrität des Verfahrens selbst, etwa das Zurückdrängen des Einflusses von Lobbyisten.

- Rationalität. Dabei fragt der Betroffene, ob das verfolgte politische Ziel mit der Maßnahme tatsächlich erreichbar ist. Das Ziel selbst kann allerdings kaum mit dem Maßstab der Rationalität, sondern nur im Wege politischen Wertens überprüft werden.
- Egalität. Dem liegt die Erkenntnis zugrunde, dass die Gleichheit vor und durch das Gesetz einem allgemeinen Verlangen nach Gleichbehandlung entspringt, das anthropologisch tief verwurzelt ist.
- Flexibilität. Auf Akzeptanz kann eine rechtliche Regelung stoßen, die auf die Besonderheiten alternativer Lebens- und Verhaltensweisen Rücksicht nimmt.
- Konkretisierung der Verfassung. Gerade in Deutschland genießen Konkretisierungen des Grundgesetzes eine hohe Akzeptanz, die durch den verbreiteten „Verfassungspatriotismus“ und das Vertrauen in das Bundesverfassungsgericht bedingt ist.
- Autorität der Rechtssetzungsinstanz. Die Wertzumessung gegenüber dem rechtssetzenden Organ hat direkte Auswirkungen auf die Akzeptanz der von ihm erlassenen Regeln. Das gilt in ähnlicher Art und Weise für die Autorität einer Instanz, die – wie das Bundesverfassungsgericht – über die Verfassungsmäßigkeit dieser Regeln entscheidet.
- Rechtssicherheit und Rechtsfrieden. Eine für den Bürger unabdingbare Funktion des Rechts ist die Gewährung von (Rechts-)Frieden und Ordnung. Außerhalb von Krisensituationen trägt dies allerdings allenfalls unterschwellig zur Rechtsakzeptanz bei.
- Orientierung am Zeitgeist. Das betrifft vor allem die richterliche Rechtsfortbildung, die im Rahmen der Auslegung von Begriffen wie ’Sittengesetz’, ’öffentliche Ordnung’ oder ’gute Sitten’ die Möglichkeit hat, auf veränderte Wertvorstellungen in der Gesellschaft einzugehen.

Neben diesen Faktoren betont *Würtenberger*, dass auch Normen selbst akzeptanzbildend wirken können; dies gelte zumindest teilweise unabhängig von ihrem Inhalt.[2319]

Etwas größere Gruppen werden demgegenüber gebildet von *Hill*.[2320] Einflussfaktoren auf die Akzeptanz sind danach:

- Gesellschaftliche Rahmenbedingungen. Diese führen bedingt durch den wachsenden Vertrauensverlust in das politische System, die Zunahme individualistischer und pluralistischer Wertorientierungen, den Anstieg der allgemeinen Problemkom-

2319 S. *Würtenberger*, Sonderheft 39/1999 der KZfSS, 380, 386: „Im demokratischen und pluralistischen Staat hat die Rechtssetzung und Rechtsfortbildung durchaus auch eine rechtsbewusstseinsbildende Funktion“. Gegenläufige Effekte werden demgegenüber dem Einfluss einer „geeinten Subkultur“ beigemessen. Das hierzu angeführte Bsp. der Volkszählung (*Würtenberger* 1987, 79) ist allerdings kaum das einer Subkultur, sondern eines breiten Protestes verschiedener Bevölkerungsschichten, s.u. 7.3.2.1.1.

2320 *Hill*, JZ 1988, 377 ff.; *ders*., DÖV 1988, 666, 668 ff.

plexität und die Ambivalenz des technischen Fortschritts zu einer Erhöhung der „Akzeptanzschwelle“ für staatliche Maßnahmen.[2321]

- Die Transparenz der Rechtsentstehung. Wegen der geringen Möglichkeiten unmittelbarer Einflussnahme im repräsentativen System werden das Anstoßen gesellschaftlicher Diskussionen, die rechtzeitige Vorinformation des Bürgers und die Prüfung von Alternativvorschlägen umso wichtiger. Die Aufnahme von Bedenken und Anregungen und deren gewissenhafte Prüfung, die Abschätzung der Gesetzesfolgen und die Offenlegung von relevanten Daten können Kommunikationsmechanismen stimulieren, die zur Akzeptanz der gefundenen Lösungen beitragen.
- Die Zustimmung zum Rechtsinhalt im Sinne von inhaltlicher Übereinstimmung mit vorhandenen Überzeugungen.
- Weitere Faktoren aus dem prozesshaften Charakter der Rechtsentstehung wie der Eindruck vertretbarer Konfliktschlichtung, Gleichheitsgesichtspunkte, das Bedürfnis nach Rechtsfrieden, Kompromissfähigkeit, die Berücksichtigung der Sozialverträglichkeit (etwa über Technikfolgenabschätzung) und das Vertrauen in die Integrität des Rechtsstabs.
- Die Darreichungsform des Rechts im Sinne von Verständlichkeit, Normenklarheit und Voraussehbarkeit.
- Die Art der Rechtsvermittlung, wobei sich das schlichte Problem des Zugangs zum Gesetz, aber auch Fragen eines so genannten „Gesetzes-Marketings“ stellen.
- Die Art des Rechtsvollzugs, insbesondere die Praktikabilität der Umsetzung.

Als Probleme für die Akzeptanzbildung werden demgegenüber die zunehmend fehlende Überschaubarkeit der Rechtsordnung, vor allem aber der Niedergang der Gesetzgebungskultur genannt.[2322] Das betrifft zum einen die Strukturen und Prozesse der Rechtssetzung und das Erscheinungsbild der Gesetzgebung aus Sicht des Bürgers (insbesondere den Eindruck des hohen Einflusses von Interessengruppen), zum anderen den Zustand und das Erscheinungsbild der Gesetze selbst. Weitere Faktoren sind der Verlust der Autorität staatlicher Institutionen und der Glaubwürdigkeit von Politik und Politikern.

Czybulka nennt als Gründe für Akzeptanzprobleme die „Inflation“ des Gesetzgebungsumfangs, die Unübersichtlichkeit der Rechtsordnung und die Hypertrophie der Verwaltung.[2323] Darüber hinaus stelle sich das Problem der ökologischen Herausforderung, die irreversible Entscheidungen auf der Basis des Mehrheitsprinzips fragwürdig werden lasse. Schließlich lasse das Vertrauen in die Effektivität verwaltungsgerichtlichen Rechtsschutzes rapide nach. Faktoren für eine positive Einstellung zu staatlichen Maßnahmen sind nach *Czybulka* im Wesentlichen nicht-materieller Art, wie allgemeine Konsensvorstellungen und die Verständlichkeit der Rechtsordnung.[2324]

Vergleichbare Faktoren wie bei den bisher genannten Autoren werden auch von *Herzog* angeführt.[2325] Danach wirken sich die Einsicht in die Notwendigkeit und Vernünftigkeit eines Gesetzes sowie dessen Überschaubarkeit und Verständlichkeit positiv auf die Akzeptanz aus. Daneben sei die Durchsetzung rechtlicher Normen wichtig: nur durchgesetztes Recht werde auch akzeptiert. Für relevant hält *Herzog* auch die Einsicht in die Notwendig-

2321 Diese Beschreibung der Rahmenbedingungen bezieht sich auf die Zeit des Erscheinens, d.h. Ende der 80er Jahre des vorigen Jahrhunderts. Sie haben sich seitdem in der von *Hill* genannten Richtung weiterentwickelt.

2322 *Hill*, DÖV 1988, 666, 667 f.

2323 *Czybulka*, Die Verwaltung 1993, 27, 30 f.

2324 *Czybulka*, Die Verwaltung 1993, 27, 29.

2325 *Herzog* 1984, 131 ff.

keit einer Rechtsordnung überhaupt, weil das auch die Akzeptanz einzelner Normen einschließe, die man für sich gesehen ablehne.[2326] Als Gründe für Akzeptanzprobleme werden demgegenüber der Abbau ethischer Standards, der Verlust von Wertüberzeugungen und die zunehmend schwerere Greifbarkeit der Anforderungsprofile des Staates an seine Bürger genannt.[2327]

Bezüglich der Akzeptanz von Gerichtsurteilen und Verwaltungsentscheidungen findet sich eine grundlegend andere Konzeption bei *Roellecke*. Danach ist nicht entscheidend, was der Betroffene selbst denkt,[2328] sondern das „normative Miterwarten" des Rests der Rechtsunterworfenen. Die Akzeptanz der Betroffenen wird also entscheidend durch die Einstellung außenstehender Dritter bestimmt: Wird das Ergebnis staatlichen Handelns von diesen miterwartet, akzeptieren es die Betroffenen. Sie protestieren nicht, weil sie nicht damit rechnen können, in der Öffentlichkeit für ihre Proteste Unterstützung zu finden. Die Einflussfaktoren auf das normative Miterwarten werden allerdings nur wenig präzisiert. Es sei maßgeblich in einem empirisch nicht erforschten Bereich der Privatsphäre verwurzelt, jedoch auch durch die staatliche Durchsetzung des Rechts beeinflusst.[2329] Letztlich dringe das Recht jedoch nicht in die individuelle Sphäre des Rechtsbewusstseins vor, da es „ohne Ansehen der Person", das heißt allgemein gelte und sich damit notwendigerweise von der Person als dem Zentrum von Normakzeptanz entferne.[2330]

Bei anderen Verfassern finden sich die Erfordernisse der Publizität des Gesetzgebungsverfahrens,[2331] der Klarheit der Gesetzessprache,[2332] gründlicher Rechtskenntnis[2333] und einer „Erziehung zum Recht"[2334] als Voraussetzungen der Akzeptanz. Zur Akzeptanz von Gerichtsurteilen komme es insbesondere auf einen Interessenausgleich und eine überzeugende Begründung an.[2335] Menschen handelten außerdem vor allem dann normadäquat, wenn sie sich davon Vorteile versprächen. Akzeptanzbemühungen des Staates seien deshalb insbesondere dort relevant, wo Normen keine ethische Basis hätten.[2336]

Bei *Lucke*, einer Autorin mit sozialwissenschaftlichem Hintergrund, findet sich eine Einteilung in drei große Kategorien.[2337] Verallgemeinerbare Umstände sind danach Glaubwürdigkeit („credibility"), Zurechenbarkeit und Verantwortlichkeit („responsability"), sowie Begründbarkeit, Rechtfertigungsfähigkeit und Entschuldbarkeit („accountability") einer staatlichen Maßnahme. Akzeptanzwahrscheinlichkeiten differieren außerdem nach den individuell angenommenen Risiken sowie nach der vermuteten oder tatsächlichen Beeinflussbarkeit und Abwendbarkeit riskanter Situationen.

7.3.1.2 Bewertung

Die Vielzahl und unterschiedliche Gewichtung der genannten Faktoren ergibt sich bis zu einem gewissen Grad aus den verschiedenen Blickwinkeln der einzelnen Autoren bei der Analyse des Akzeptanzphänomens. Die Faktoren lassen sich dennoch in drei große

2326 *Herzog* 1984, 136.
2327 *Herzog* 1984, 134 f.
2328 „Mit dem werden die Gerichte leicht fertig", s. *Roellecke*, JZ 1997, 577, 579.
2329 *Roellecke*, JZ 1997, 577, 581.
2330 *Roellecke*, JZ 1997, 577, 582.
2331 *Rehbinder* 2003, 246 ff.
2332 Eingehend *Kindermann* 1986, 53 ff.
2333 *Pichler* 1996, 24 ff., 35; *Sagel-Grande*, ZRP 1990, 26, 29; s. zum Begriff *Raiser* 1998, 109 ff.
2334 *Lampe* 1998, 99 ff.
2335 *Benda*, DÖV 1983, 305, 309, 307; *Limbach* 1998, 264.
2336 *Sagel-Grande*, ZRP 1990, 26, 29.
2337 *Lucke* 1998, 22.

Blöcke einteilen. Es handelt sich um Umstände, die der zu akzeptierenden Maßnahme, dem akzeptierenden Individuum und dem beide umschließenden Kontext zugeordnet werden können.

Hinsichtlich der Maßnahme selbst lassen sich in rechtspolitischer Sicht prozedurale und inhaltliche Faktoren unterscheiden. Zur Prozessebene gehören die Einflüsse durch ein konsensbildendes Verfahren, die Einbeziehung von Minderheits- und Oppositionspositionen, ein Kompromiss zwischen den Akteuren, Informationen im Vorfeld und das Vertrauen in die handelnden staatlichen Akteure auf den Ebenen der Normsetzung und -kontrolle. Auf der inhaltlichen Seite, also dem Ergebnis des Prozesses, werden einerseits formelle Elemente wie die Verständlichkeit und Klarheit einer Maßnahme relevant, andererseits materielle Gesichtspunkte wie die Rationalität des staatlichen Handelns, seine egalisierende Wirkung, Verteilungsgerechtigkeit, Flexibilität und die Berücksichtigung sozialer Gerechtigkeit.

Demgegenüber wird das Akzeptanzverhalten eines Individuums maßgeblich durch autonome Entscheidungen bestimmt, das heißt durch Rechtsbewusstsein und Rechtsgefühl. Beide entstehen wie andere persönliche Überzeugungen im Laufe des Sozialisationsprozesses. Der individuellen Akzeptanz oder Ablehnung einer rechtlichen Maßnahme liegen damit dieselben Einstellungen zugrunde wie der Akzeptanz oder Ablehnung anderer sozialer Normen. Neben diesem Faktor sind der persönlichen Sphäre das Verlangen nach Rechtsfrieden, die Einsicht in die Notwendigkeit einer Rechtsordnung, Fragen rationalen Entscheidens (also das Abwägen zwischen Vorteilen und Risiken von Rechtsbefolgung oder -bruch) und die Kenntnis der Rechtsordnung (oder eines konkreten Rechtsaktes) zuzuordnen.

Bezüglich des Kontextes lassen sich zunächst allgemeine Faktoren wie eine gesellschaftliche Tendenz zur Pluralisierung von Werten, der Verlust an Glaubwürdigkeit des politischen Entscheidungsprozesses, Fragen der tatsächlichen Durchsetzung rechtlicher Normen und die Unübersichtlichkeit der Rechtsordnung insgesamt anführen. Die Akzeptanz der konkreten Maßnahme wird durch Informationen und Werbung beeinflusst. Auch das „normative Miterwarten“ gehört hierher. Daneben kann die Berichterstattung in den Medien eine nicht zu unterschätzende Polarisierungsrolle spielen, etwa durch die Art der Darstellung von Zielen und Alternativen einer Maßnahme oder Berichte über prominente Missbrauchsfälle. Akzeptanz ist damit immer die Akzeptanz einer konkreten Maßnahme in einem konkreten gesellschaftlichen Umfeld und insofern abhängig von den allgemeinen Strömungen der Zeit.

Für den Einfluss der drei Sphären auf eine konkrete Akzeptanzsituation ist zu differenzieren. Die „objektiven“ Eigenschaften des jeweiligen Objekts wirken allgemein, das heißt auf alle Individuen in allen Situationen. Sie sagen aber in einer konkreten Einzelsituation für sich genommen noch nichts über die real zu erwartende Akzeptanz aus. Je nach der Stärke des jeweiligen Kontextes können die tatsächlichen Objekteigenschaften sogar völlig hinter diesen zurücktreten. Um schließlich die subjektive Reaktion der einzelnen Rechtsunterworfenen abschätzen zu können, ist eine Betrachtung der jeweiligen individuellen Wertüberzeugungen erforderlich.

Bewertet man die genannten Faktoren, so sind diese von unterschiedlicher Relevanz und Plausibilität. So trifft es zwar zu (und wird durchweg in den Veröffentlichungen betont), dass zur Akzeptanz einer Maßnahme ihre Kenntnis erforderlich ist. Gerade diese Kenntnis kann andererseits aber auch zur Ablehnung der Maßnahme führen.

Was *Roelleckes* „normatives Miterwarten“ angeht, so bezeichnet dies einen relevanten Faktor für Einzelentscheidungen, ist aber nicht anwendbar, wenn es keine außenstehenden Dritten gibt. Dies ist bei Gesetzen der Fall, deren Inhalt – wie bei der Volkszählung und

dem Personalausweis[2338] – jedermann, oder – wie bei der elektronischen Gesundheitskarte – den ganz überwiegenden Teil der Bevölkerung erfassen. Darüber hinaus ist zweifelhaft, ob die Einstellungen Dritter wirklich schwerer wiegen als eigene Auffassungen.[2339] Hierdurch wird auch der Einfluss von Eigenschaften des Objekts auf seine Akzeptanz geleugnet: man dürfe die Analyse von Normakzeptanz und Rechtsbewusstsein „nicht von Inhalten abhängig machen".[2340] Von *Roelleckes* Standpunkt aus ist das zwar konsequent, weil er von einem in der Wirklichkeit unentscheidbaren Konflikt verschiedener Werte in der Gesellschaft ausgeht und auch die Gerechtigkeit (etwa einer Maßnahme) nicht als übergeordnetes Prinzip, sondern als einen Wert unter vielen begreift.[2341] Dennoch ist der Verzicht auf inhaltliche Kriterien für das Akzeptanzverhalten unbefriedigend.

Auch andere der genannten Beispiele sind nicht zweifelsfrei. So wird oftmals der Einfluss von Elementen der Konsensbildung im Entscheidungsfindungsprozess betont. Eine solche inhaltliche Übereinstimmung dürfte zwar hinsichtlich eines gewissen Basiskonsenses (etwa bezogen auf staatliche Fundamentalprinzipien) noch herzustellen sein. Bei politischen Sachentscheidungen stellt sich die Situation hingegen schwieriger dar, und dies verschärft sich noch bei stark umstrittenen Problemen. Gerade hier aber kommt es auf die Akzeptanz an.

Andere Faktoren erscheinen wiederum in ihrer realen Wirkung fragwürdig. Auf einer extremen Makroebene mögen etwa das Verlangen nach Rechtsfrieden oder die Einsicht in die Notwendigkeit einer Rechtsordnung an sich akzeptanzbeeinflussend sein. Warum dies jedoch die Akzeptanz einer im Einzelfall als falsch oder ungerecht empfundenen Maßnahme begünstigen soll, ist nicht einsichtig, weil Menschen nicht die Notwendigkeit einer beliebigen, sondern einer gerechten Rechtsordnung einsehen. Genau diese Einsicht kann aber im Einzelfall gerade dazu führen, eine Maßnahme abzulehnen. Ein derartiges Verhalten kann sich – zumindest subjektiv – auch als Verteidigung einer solchen gerechten Rechtsordnung darstellen.

Die genaue Analyse der tatsächlichen Relevanz der genannten Bereiche steht im Übrigen bislang noch aus. Insbesondere gibt es so gut wie keine empirische Fundierung der oben aufgeführten Thesen hinsichtlich der verschiedenen Einflussfaktoren.[2342] Im Ergebnis gründen sich die Ausführungen – inklusive der hier vorgeschlagenen Kategorisierung – lediglich auf ihre jeweilige inhaltliche Plausibilität. Damit wird die tatsächliche Relevanz der Einzelfaktoren nicht bestritten. Man sollte aber im Blick behalten, dass einige der angeführten Punkte im Einzelfall vermutlich ohne messbare Wirkung sein werden.

2338 Eine Ausnahme besteht nach § 1 Abs. 1 Satz 1, 2. Halbsatz PersAuswG für Inhaber eines Reisepasses. Es besteht aber in jedem Fall eine Pflicht zum Besitz eines staatlichen Identifikationsdokuments.

2339 So *Roellecke*, JZ 1997, 577, 579: ob außenstehende Dritte eine Rechtsnorm normativ erwarten, sei wichtiger als das „abstrakte Bewusstsein" des Betroffenen.

2340 *Roellecke*, JZ 1997, 577, 580.

2341 *Roellecke*, JZ 1997, 577, 579.

2342 S. *Pichler* 1996, 12. Dort finden sich erste Ansätze zu empirischer Untersuchung, vgl. 14 ff.; zu soziologischen Forschungsdefiziten s. *Lucke* 1995, 235 ff. Diese unternimmt auch den Versuch einer Operationalisierung zur Messung von Akzeptanz, ebd., 286 ff. Andere Autoren betonen demgegenüber zwar, das Akzeptanzphänomen sei eine soziologische oder psychologische Fragestellung (s. *Würtenberger*, Sonderheft 39/1999 der KZfSS, 380, 381), erwähnen jedoch nicht, dass dann konsequenterweise zur Überprüfung ihrer eigenen Hypothesen auch die empirischen Instrumente der Soziologie und Psychologie anzuwenden wären.

7.3.2 Frühere Akzeptanzphänomene: Fallstudien aus Deutschland

Die Probleme, die durch Chipkartenausweise aufgeworfen werden, sind in ihren speziellen Ausprägungen zwar neuartig, gleichzeitig aber nicht ohne Vorläufer. Das gilt insbesondere für Akzeptanzfragen. Aus diesem Grund wird im Folgenden ein näherer Blick auf zwei rechtspolitisch hoch umstrittene staatliche Projekte geworfen, bei denen neben Aspekten des Datenschutzrechts auch Akzeptanzfragen eine wichtige Rolle gespielt haben.[2343] Die Volkszählung dient dabei als Beispiel für die Mobilisierungswirkung, die staatliche Maßnahmen bei der Datenverarbeitung im hoheitlichen Bereich auslösen können, während die Einführung des derzeitigen maschinenlesbaren Personalausweises für die vorliegende Arbeit selbstredend von Interesse ist.[2344]

7.3.2.1 Fallstudie 1: Die Volkszählung

7.3.2.1.1 Die Geschichte der Volkszählung

Das Gesetz über eine Volks-, Berufs-, Wohnungs- und Arbeitsstättenzählung (Volkszählungsgesetz 1983)[2345] wurde am 25. März 1982 vom Bundestag beschlossen.[2346] Die Verabschiedung erfolgte einstimmig.[2347] Die Wortmeldungen in der Debatte bezogen sich ganz überwiegend auf die mit der Volkszählung verbundenen Kosten.[2348] Anmerkungen zum Datenschutz fehlten fast vollständig; die allgemeine Einschätzung war wohl, es ginge „nur um Statistik".[2349] Als Hauptargument für die Zählung wurde die Planungsfähigkeit des Staates angeführt.[2350] Für die Durchführung wurde die aufschiebende Wirkung von Widerspruch und Anfechtungsklage ausgeschlossen (§ 80 Abs. 2 Nr. 3 VwGO).

Völlig überraschend für Regierung und Opposition formierte sich ab dem September des Jahres 1982 eine Gegenbewegung zur Volkszählung.[2351] Ihr Schwerpunkt lag zunächst in Hamburg, wo sich auch das Koordinierungsbüro befand. Anfang März des Jahres 1983 gab es bundesweit bereits 400 Initiativen. Im Unterschied zu anderen Fällen der Akzeptanzverweigerung lehnten nicht nur eng begrenzte Gruppen, sondern Bürger aus unterschiedlichsten sozialen Zusammenhängen, verschiedenen Alters und Bildungsgrads die Volkszählung ab.[2352] Die breite Diskussion überraschte sogar die Datenschutzbeauftragten. Wesentliche Argumente gegen die Volkszählung waren die grundsätzliche Ungeeignetheit statistischer Verfahren für eine bürgernahe und soziale Politik, die Gefahren des Daten-

2343 Vgl. schon *Roßnagel/Hornung*, in: Reichl/Roßnagel/Müller 2005, 301 ff.

2344 Andere Bsp. wie das Atomkraftwerk Brokdorf, die Startbahn West oder die Wiederaufbereitungsanlage Wackersdorf bleiben hier außer Betracht, weil sie keinen Bezug zum Datenschutzrecht aufweisen.

2345 BGBl. I S. 369. Der Entwurf eines Volkszählungsgesetzes war zuvor in der 8. Legislaturperiode an unterschiedlichen Auffassungen über die Verteilung der Kosten zwischen Bund und Ländern gescheitert; zu den historischen Hintergründen des statistischen Instruments der Volkszählung vgl. *Grohmann*, Berliner Statistik – Monatsschrift 2000, 216 f.

2346 S. zum Folgenden bereits *Roßnagel/Hornung*, in: Reichl/Roßnagel/Müller 2005, 301 ff.

2347 Schon in der ersten Lesung stimmte auch die oppositionelle CDU/CSU zu, vgl. BT-Drs. 9/1068, 17.

2348 Vgl. das Protokoll der Beratung, abgedruckt bei *Taeger* (Hrsg.) 1983, 31 ff. Die Kosten wurden auf 371 Mio. Mark geschätzt.

2349 *Hoffmann* 1983, 87; zum Gesetzgebungsverfahren s.a. *Taeger* 1983, 68 ff.; *Würzberger/Stürmer* 1983, 167.

2350 Laut Beitrag des Abgeordneten *Broll* (s. *Taeger* (Hrsg.) 1983, 32 f.) hatte die Fortschreibung der Volkszählung von 1961 auf das Jahr 1970 858.000 Einwohner und 714.000 Wohnungen mehr ergeben, als 1970 dann tatsächlich gezählt wurden.

2351 Zu ihrer Geschichte s. allgemein *Huber* 1983, 254 ff.

2352 *Simitis*, NJW 1984, 398; *Mückenberger*, KJ 1984, 1.

missbrauchs und der Vorwurf, der Einsatz staatlicher Kontrolle statt Bürgerbeteiligung offenbare ein grundsätzlich falsches Demokratieverständnis.[2353] Die nach der Bundestagswahl im März des Jahres 1983 im Amt bestätigte Regierung aus CDU/CSU und FDP hielt jedoch an dem Projekt fest. Die Durchführung der für den 27. April 1983 geplanten Volkszählung wurde schließlich am 13. April 1983 durch eine einstweilige Anordnung des Bundesverfassungsgerichts bis zur Entscheidung über die gegen das Gesetz anhängigen Verfassungsbeschwerden ausgesetzt.[2354]

Das Urteil in der Hauptsache erging am 15. Dezember 1983.[2355] Die unmittelbar gegen das Volkszählungsgesetz gerichteten Verfassungsbeschwerden wurden trotz des noch fehlenden Vollzugsaktes für zulässig erklärt, weil wegen der Anordnung des Entfallens der aufschiebenden Wirkung eines Widerspruchs und wegen des sehr knappen Zeitraums von zwei Wochen zwischen Austeilung und Einsammlung der Erhebungsbögen eine Überprüfung im Wege des vorläufigen Rechtsschutzes vor den Verwaltungsgerichten nicht möglich gewesen wäre.[2356]

In der Begründetheitsprüfung lehnte das Gericht zunächst Verletzungen von Art. 4 Abs. 1, Art. 13 Abs. 1 und Art. 5 Abs. 1 GG ab.[2357] Danach formulierte es mit der bereits beschriebenen Argumentationslinie[2358] das Grundrecht auf informationelle Selbstbestimmung. Im Ergebnis erklärte das Bundesverfassungsgericht die Volkszählung für im Prinzip verfassungsgemäß. Damit befand es sich in einer Linie mit der Europäischen Kommission für Menschenrechte, die die britische Volkszählung des Jahres 1980 in einer Entscheidung aus dem Jahre 1982 für zulässig befunden hatte.[2359] Das Bundesverfassungsgericht stellte für die Datenerhebung zu statistischen Zwecken erleichterte Regeln auf, nämlich die Möglichkeit einer (anonymisierten) Vorratsspeicherung, den Verzicht auf eine konkrete Zweckumschreibung und die erweiterte Zulässigkeit von Datenübermittlungen.[2360] Die Gebote der Normenklarheit und Verhältnismäßigkeit sahen die Richter als erfüllt an.[2361] Letzteres gelte allerdings nur, solange nicht mildere, gleich geeignete Mittel aus der statistischen Methodik verfügbar seien.[2362]

Auch wenn die Volkszählung damit im Grundsatz verfassungsrechtlich zulässig war, verlangte das Urteil doch ergänzende verfahrensrechtliche Vorkehrungen für die Durchführung und Organisation der Datenerhebung.[2363] Das betraf Aufklärungs- und Belehrungspflichten, die frühestmögliche Löschung von Identifizierungsmerkmalen, die Vermeidung von Interessenkonflikten auf Seiten der Zähler und die Übereinstimmung der

---

2353 S. *Appel* 1986b, 267 ff.; ausführlich unten 7.3.2.1.2.

2354 BVerfGE 64, 67. Die Entscheidung erging mit 5 zu 3 Stimmen. Die Mehrheit der Richter argumentierte im Rahmen der Folgenabwägung (§ 32 Abs. 1 BVerfGG), eine Durchführung der Volkszählung würde im Falle ihrer Verfassungswidrigkeit die Rechte aller Bürger in einer Art und Weise verletzen, die aufgrund der einsetzenden Verwertung nicht wieder rückgängig zu machen sei. Demgegenüber war die Aussetzung der Zählung nur eine kurze Verschiebung, die die Hauptsache nicht vorwegnahm.

2355 BVerfGE 65, 1; vgl. etwa *Podlech*, Leviathan 1984, 85 ff.; *Simitis*, NJW 1984, 398 ff.; *Schlink*, Der Staat 1986, 233 ff.; *Mückenberger*, KJ 1984, 1 ff.; *Konferenz der Datenschutzbeauftragten*, DÖV 1984, 504 ff. und (vor dem Urteil) *Mallmann*, JZ 1983, 651, 653 ff.; aus neuerer Zeit s. *Faber*, RDV 2003, 278 ff.; *Hornung*, MMR 2004, 3 f.; kritischer *Duttge*, NJW 1998, 1615 ff.

2356 BVerfGE 65, 1 (37 f.).

2357 BVerfGE 65, 1 (38 ff.).

2358 S.o. 4.1.1.2.

2359 Bericht der Kommission 9702/81, DR 30, 239 = EuGRZ 1983, 410; dazu *Breitenmoser* 1986, 243 f.; *Gridl* 1999, 108 f.; *Matz* 2003, 113 f.

2360 BVerfGE 65, 1 (47).

2361 BVerfGE 65, 1 (52 ff.).

2362 BVerfGE 65, 1 (55 f.).

2363 BVerfGE 65, 1 (58 ff.).

Ausgestaltung des Fragebogens mit den gesetzlichen Bestimmungen. Für verfassungswidrig erklärt wurde schließlich die Kombination der Volkszählung für statistische Zwecke mit dem Melderegisterabgleich und eine Reihe anderer Übermittlungsregeln an Bundes- und Landesbehörden sowie Kommunen.[2364] Hier sah das Gericht die gebotene Anonymität, Zweckbestimmung und Normenklarheit verletzt. Damit war die Durchführung der Zählung im Jahre 1983 gescheitert.

In der Protestbewegung wurde das Urteil einerseits euphorisch begrüßt, andererseits durchaus kritisch gesehen, weil der Protest dadurch abebbte und im Jahre 1987 nur schwer wieder zu mobilisieren war.[2365] Außerdem wurde eine Tendenz zum Unterlaufen des Urteils beobachtet und kritisiert, das aufgestellte Erfordernis bereichsspezifischer Eingriffsregelungen führe nunmehr zur Legalisierung vorheriger rechtswidriger Praktiken.[2366]

Nach einem erneuten Gesetzgebungsverfahren[2367] wurde die Volkszählung schließlich am 25. Mai 1987 durchgeführt. Das Verfahren wurde teilweise verändert; außerdem verzichtete man auf den Melderegisterabgleich. Die Zählung des Jahres 1987 war allerdings gleichzeitig die letzte ihrer Art in der Bundesrepublik. An der EG-Volkszählung im Jahre 1991 nahm Deutschland nicht mehr teil. Dies lag wohl darin begründet, dass der wissenschaftliche wie politische Wert derartiger Totalerhebungen inzwischen ohnehin sehr umstritten geworden war.[2368]

Im Unterschied zum gescheiterten Versuch im Jahre 1983 wurde die Volkszählung im Jahre 1987 von einer massiven Informationskampagne begleitet, für die allein in den ersten viereinhalb Monaten des Jahres 30 Millionen DM zur Verfügung standen. Die Kampagne umfasste Plakate, Handzettel, Aufkleber, Werbespots, Unterrichtsmaterialien, eine Telephon-Hotline und den medienwirksamen Auftritt des Bundespräsident und einiger Mitglieder der Regierung. Die Argumente konzentrierten sich im Wesentlichen auf die Harmlosigkeit der Fragen und die Notwendigkeit der Zählung für die staatliche Planung. Es gab aber auch Hinweise auf die Strafbarkeit der Verweigerung, und in der heftigen Debatte wurde von Seiten des Bundeskanzlers *Kohl* einmal sogar der Vorwurf einer „faschistischen Gesinnung" der Verweigerer erhoben.[2369]

Auch im Jahre 1987 gab es Widerstand, diesmal von ca. 900 Boykottinitiativen, in denen sehr unterschiedliche gesellschaftliche Gruppen vertreten waren.[2370] Ihre Argumente ähnelten denen der Verweigerungskampagne des Jahres 1983. Sie gaben etwa Tipps für Zähler, ihrer Pflicht zu entgehen, sowie Hinweise für Bürger im Umgang mit den Zählern.[2371] Im Ergebnis war ihr Effekt im Jahre 1987 deutlich geringer als im Jahre 1983, was allerdings teilweise mit der Furcht vor Repressionen erklärt wurde.[2372] Unter den Gemeinden stellte sich eine gewisse Abneigung gegen die Zählung ein, da sie diese unter ver-

2364 BVerfGE 65, 1 (63 ff.).
2365 *Pötzl* 1985, 28.
2366 *Pötzl* 1985, 33 ff., 43; s.a. *Simitis*, NJW 1984, 398, 400; vgl. zu den Gesetzen, auf die sich das Volkszählungsurteil unmittelbar im Sinne einer Revisionsbedürftigkeit auswirkte, *Konferenz der Datenschutzbeauftragten*, DÖV 1984, 504, 506 ff.
2367 Dieses mündete in das Gesetz über eine Volks-, Berufs-, Gebäude-, Wohnungs- und Arbeitsstättenzählung (Volkszählungsgesetz 1987) v. 8.11.1985 (BGBl. I S. 2078); zum Inhalt des Gesetzes s. *Mallmann*, NJW 1986, 1850 ff. Neben den Regierungsfraktionen stimmte auch die oppositionelle SPD zu.
2368 *Appel/Hummel* 1988, 9; s.a. *Simitis*, NJW 1984, 398, 403 f. m.w.N.; *Sietmann*, c't 19/1999, 268, 274 ff. Allerdings werden in der EU nach wie vor Volkszählungen durchgeführt; s. etwa zur Zählung des Jahres 2001 in Österreich http://www.statistik.at/gz/vz.shtml.
2369 S. *Sietmann*, c't 19/1999, 268, 273.
2370 *Appel/Hummel* 1988, 21 f.
2371 *Ziegler* 1987a, 37 ff.; *ders*. 1987b, 46 ff.
2372 *Appel/Hummel* 1988, 19.

schärften Verfahrensbedingungen durchführen mussten, wegen des Verbots des Melderegisterabgleichs aber nur sehr eingeschränkt profitieren konnten.[2373]

Die Verfassungsmäßigkeit der Volkszählung, deren Gesamtkosten sich schließlich auf etwa 1 Milliarde DM beliefen, war auch in ihrer revidierten Version umstritten.[2374] Verfassungsbeschwerden gegen die Zählung wurden im Jahre 1987 durch das Bundesverfassungsgericht nicht zur Entscheidung angenommen.[2375] Das Gericht richtete dabei den Fokus auf die individuelle Ebene des einzelnen Betroffenen, statt wie im Jahre 1983 auf die Gesamtperspektive abzustellen. Es erklärte etwaige Missbrauchsgefahren und Verfahrensfehler als für die Verfassungsmäßigkeit der Volkszählung selbst unbeachtlich.

7.3.2.1.2 Wesentliche Argumentationslinien

Im Folgenden soll ein näherer Blick auf die in der rechtspolitischen Diskussion vorgebrachten Argumente geworfen werden.[2376] Das Hauptanliegen der Befürworter war es, die Planungsfähigkeit des Staates auf eine sichere Grundlage zu stellen. Die Ergebnisse der Statistik als einer der vielseitigsten Informationsquellen seien unverzichtbar für die Beobachtung der gesellschaftlichen und wirtschaftlichen Situation und ihrer Entwicklung sowie für die Vorbereitung und Kontrolle von Entscheidungen, Maßnahmen und Planungsvorhaben.[2377] Verwiesen wurde auf entsprechende Empfehlungen der Vereinten Nationen[2378] und der Europäischen Gemeinschaft.[2379] Als Anwendungsbeispiele für die gesammelten Daten wurden genannt: der Zuschnitt von Wahlkreisen, Finanzausgleichsberechnungen, künftige Schulanfängerzahlen, Berechnungen der Rentenversicherung, Erkenntnisse über Frauenerwerbstätigkeit und über das Ausscheiden von Berufstätigen aus bestimmten Berufen, die Planung des öffentlichen Personennahverkehrs und die Wohnungsbauförderung.[2380] Zur Totalerhebung gebe es keine Alternative, weil die Zusammenführung vorhandener Datenbanken oder Erhebungen auf Stichprobenbasis keine vergleichbar zuverlässigen Daten lieferten.[2381] Grundsätzlich verteidigt wurde das Modell des systematisch planenden Staates, dessen Planungsvorteile letztlich allen dienten.[2382] Soweit in die Privatsphäre des Einzelnen eingegriffen werde, sei der Eingriff von geringer Intensität, weil die Erhebung keine Daten des Intimbereichs erfasse und die Fragen auch in ihrer Kumulierung keine wesentliche Beeinträchtigung der Persönlichkeitssphäre ergäben.[2383]

2373 *Grohmann*, Berliner Statistik – Monatsschrift 2000, 216, 218.

2374 Vgl. einerseits *Hauck-Scholz*, NJW 1987, 2769 ff. (verfassungswidrig), andererseits *Schenke*, NJW 1987, 2777 ff. (bis auf Marginalien verfassungsmäßig).

2375 Z.B. BVerfG, NJW 1987, 1689; NJW 1987, 2219.

2376 Dabei wird nicht zwischen den beiden Diskussionen der Jahre 1983 und 1987 differenziert, weil die Argumente inhaltlich weitgehend übereinstimmen; vgl. bereits *Roßnagel/Hornung*, in: Reichl/Roßnagel/Müller 2005, 303 f.

2377 So die Bundesregierung und die Mehrheit der Landesregierungen vor dem BVerfG, s. BVerfGE 65, 1 (22); s.a. *Sietmann*, c't 19/1999, 268 f.

2378 Vgl. *Würzberger/Stürmer* 1983, 164. Die UN empfehlen den Staaten seit 1950, alle zehn Jahre eine Volkszählung durchzuführen, s. *Grohmann*, Berliner Statistik – Monatsschrift 2000, 216 f.

2379 Richtlinien des Rates v. 22.11.1973 zur Synchronisierung der allgemeinen Volkszählungen, 73/403/EWG, ABl. EG L 347 (17.12.1973), S. 50.

2380 *Würzberger/Stürmer* 1983, 171 ff.

2381 S. die Erläuterungen der Bundesregierung und der Mehrheit der Landesregierungen im Volkszählungsurteil, BVerfGE 65, 1 (26 f., 33 f.). Das wurde vom Gericht genauso gesehen, vgl. ebd., 56 ff.

2382 *Dickhoven* 1983, 195 ff.; *Frank* 1983, 225 ff. Dies wurde durch das BVerfG (in den Ausführungen zur Erforderlichkeit statistischer Erhebungen) im Wesentlichen akzeptiert, s. BVerfGE 65, 1 (47 ff.).

2383 Vorbringen der Bundesregierung und der Mehrheit der Landesregierungen im Volkszählungsurteil, BVerfGE 65, 1 (25).

Hinsichtlich des im Jahre 1983 vorgesehenen Melderegisterabgleichs wurde vorgebracht, allenfalls die Existenz dieser Register selbst sei problematisch, nicht aber der Abgleich der Volkszählungsdaten mit ihnen.[2384] Überhaupt sei die Volkszählung nur ein Katalysator, der zwar Entwicklungen bewusst mache, selbst aber nicht gefährlich sei.[2385] Schließlich seien Datenschutzbeauftragte in die Erarbeitung des Gesetzes einbezogen worden.[2386]

Die Argumente der Gegenseite sind aufgrund der Vielzahl inhomogener Gruppierungen, die sich gegen die Volkszählung engagierten, sehr unterschiedlich und teilweise widersprüchlich.

Zunächst wurde versucht, die prinzipielle Brauchbarkeit des Instruments der Totalerhebung in Frage zu stellen.[2387] Durch die „natürliche Verweigerungsquote" von etwa 5 % und die Gefahr falscher Angaben trotz guten Willens seien die Ergebnisse statistisch unbrauchbar.[2388] Außerdem müsse gerade bei planerisch interessanten Fragen, etwa zum Sozialhilfeempfang, mit vermehrten Falschantworten gerechnet werden. Daneben sei der Fragebogen veraltet, er gehe etwa von einer überholten Sozialstruktur aus.[2389] Etwaige Diskrepanzen zwischen Melderegistern und Volkszählung müssten keineswegs zugunsten der letzteren gelöst werden.[2390] Ohnehin könnten die Daten vernünftigerweise nur für etwa zwei Jahre als valide angesehen werden, die Auswertung dauere aber bereits länger als ein Jahr.[2391] Es sollten lieber andere Erhebungsmethoden verbessert werden, statt das seit der Mitte des 19. Jahrhunderts nicht fortentwickelte Instrument der Volkszählung anzuwenden.[2392] Der Volkszählung des Jahres 1987 wurde schließlich attestiert, sie sei als Totalerhebung unbrauchbar.[2393]

Eine zweite Gruppe von Argumenten betraf datenschutzrechtliche Fragen. Eine Anonymisierung der Daten werde noch nicht einmal ansatzweise verwirklicht.[2394] Aus den 160 Einzelangaben lasse sich mühelos jeder Bürger bestimmen,[2395] außerdem gebe die Kennziffer des Bogens sogar das jeweilige Haus an.[2396] Schließlich würden die Bögen zu lange aufbewahrt.[2397] Als Schwachstelle wurde außerdem bezeichnet, dass die Gemeinden die Daten unanonymisiert erhielten und so kopieren könnten.[2398] Für den im Jahre 1983 geplanten Melderegisterabgleich fehle es bereits an einer Gesetzgebungskompetenz des Bundes. Er hebe überdies die funktionelle Trennung von Statistik und Meldewesen auf und führe zu einem Gebot der Selbstbezichtigung. Dies verstoße gegen das Rechtsstaatsprin-

---

2384 Stellungnahme von *Bull* im Streitgespräch mit *Grass*, in: Taeger (Hrsg.) 1983, 48.
2385 Stellungnahme von *Bull* im Streitgespräch mit *Grass*, in: Taeger (Hrsg.) 1983, 45.
2386 So die Bundesregierung und die Mehrheit der Landesregierungen, BVerfGE 65, 1 (22).
2387 Eine Umfrage des grünen Bundestagsabgeordneten *Ströbele* ergab etwa, dass keine der von ihm befragten Kommunen 1987 ein Projekt angeben konnte, dass deswegen nicht oder schlechter verwirklicht worden war, weil seit 1970 keine Volkszählung stattgefunden hatte, vgl. *Ströbele* 1987, 9.
2388 *Erb* 1987, 83; Stellungnahme von *Grass* im Streitgespräch mit *Bull*, in: Taeger (Hrsg.) 1983, 44.
2389 *Güllner* 1983, 190.
2390 *Güllner* 1983, 188.
2391 *Taeger* 1983, 104; *Tiemann* 1983, 222.
2392 *Güllner* 1983, 187 ff. und die Klagebegründung des Volkszählungsurteils, BVerfGE 65, 1 (18).
2393 *Steinmüller* 1988, 204.
2394 *Brunnstein* 1987, 62 ff.; *Hoffmann* 1983, 88 ff.; *Taeger* 1983, 91; s.a. das Vorbringen der Kläger im Volkszählungsurteil, BVerfGE 65, 1 (17), sowie die Auffassung der Hamburgischen Landesregierung, ebd., 34.
2395 *Ellerbrock* 1983, 13.
2396 Stellungnahme von *Grass* im Streitgespräch mit *Bull*, in: Taeger (Hrsg.) 1983, 52.
2397 *Ellerbrock* 1983, 13.
2398 *Taeger* 1983, 88; Stellungnahme von *Grass* im Streitgespräch mit *Bull*, in: Taeger (Hrsg.) 1983, 51.

zip.[2399] Der Abgleich sei eines der Hauptprobleme und ziehe durchaus persönliche Folgen nach sich, etwa bei Wehrpflichtigen, die in Berlin gemeldet seien, dort aber nicht wohnten.[2400] Höchst problematisch sei schließlich die Möglichkeit der Weitergabe von Daten an Private[2401] sowie die Tatsache, dass dem Bürger jedwede Weitergabe nicht mitgeteilt werde.[2402] Auch erlangten Mitglieder von Familien und Wohngemeinschaften Kenntnis über die gegenseitigen persönlichen Verhältnisse, da der jeweilige Haushaltsvorstand den Bogen auszufüllen habe.[2403] Fragen mit starkem Bezug zum persönlichen Bereich (Bad, Einkommen) seien bereits in sich bedenklich.[2404]

Die nächste Argumentationslinie betonte, der legale Gebrauch der Daten sei sogar noch gefährlicher als ihr Missbrauch, weil tradierter Bilder im Wege empirisch-technokratischer Planung verstärkt würden.[2405] So sei die Frage nach dem Weg zur Arbeit falsch gestellt: dass jemand mit dem Auto fahre, sage nichts darüber aus, ob er nicht lieber die Bahn benutzen würde, dies jedoch wegen des schlechten Angebots nicht tue.[2406] Allgemein sollten statt Tatsachen eher Bedürfnisse abgefragt werden.[2407] Außerdem bestehe die Gefahr, dass ein gut informierter Staat auf Mittel stärkerer Bürgerbeteiligung verzichten zu können glaube.[2408] Daneben führten Datensammlungen tendenziell zu einer Abkoppelung der Exekutive von legislativer Kontrolle, da die Exekutive über mehr Informationsverarbeitungskapazitäten verfüge.[2409] Kritisiert wurde also eine Verquickung von Forschung und Verwaltungsvollzug: statistische Verfahren seien grundsätzlich ungeeignet für eine bürgernahe und soziale Politik.[2410]

Des Weiteren wurden gesetzestechnische Bedenken vorgebracht. Schon der Name des Gesetztes sei verwirrend: es gehe nicht, jedenfalls nicht vorwiegend, um eine Zählung.[2411] Erhebungszweck und Erhebungsprogramm seien im Gesetz nur unzureichend geregelt.[2412] Überdies fehle der Hinweis, dass es keine Pflicht gebe, den Zähler in die Wohnung zu lassen. Außerdem hätten einige Fragen keine Grundlage im Gesetz, sodass es auch keine Pflicht gebe, auf sie zu antworten. Ferner seien sie in wenig verständlichem Beamtendeutsch verfasst.[2413] Schließlich enthalte der Bogen keine Rechtsmittelbelehrung.[2414]

Im Zusammenhang mit dem ersten Volkszählungsversuch im Jahre 1983 wurden der Regierung auch eine mangelnde Information der Öffentlichkeit und ein Verbreiten von

---

2399 Klagebegründung im Volkszählungsurteil, BVerfGE 65, 1 (19) und das dortige Vorbringen der Hamburgischen Landesregierung, ebd., 34.

2400 *Taeger* 1983, 100; s. aus rechtlicher Sicht zum geplanten Melderegisterabgleich *Mallmann*, JZ 1983, 651, 655 ff.

2401 *Taeger* 1983, 44.

2402 Insoweit wurden Verstöße gegen das Bestimmtheitsgebot und die Rechtsschutzgarantie beanstandet, s. *Geulen* 1983, 111; *Taeger* 1983, 94; vgl. auch das klägerische Vorbringen in BVerfGE 65, 1 (19 f.).

2403 *Taeger* 1983, 102.

2404 *Hoffmann* 1983, 89.

2405 *Huber* 1983, 263.

2406 *Appel* 1987, 22.

2407 *Erb* 1987, 84; Stellungnahme von *Hansen*, in: Taeger (Hrsg.) 1983, 52.

2408 *Frank* 1983, 228.

2409 *Frank* 1983, 229 und 231 ff.

2410 *Appel* 1986b, 267 ff.; *Güllner* 1983, 193; *Hoffmann* 1983, 88 ff. *Appel* (1986a, 46) verweist auf *Burkhard Hirsch* (BT-Prot. Nr. 159, 10. Wahlperiode, 11922 f.): „Die Lebenserfahrung zeigt, dass die Kenntnis von Tatsachen nicht dafür garantiert, dass man daraus die richtigen Schlüsse zieht. Außerdem dienen manche Statistiken nicht dazu, Entscheidungen zu finden, sondern sie zu begründen".

2411 *Simon* 1983, 136 f.

2412 So das Vorbringen der Kläger im Volkszählungsurteil, BVerfGE 65, 1 (18).

2413 *Güllner* 1983, 191.

2414 *Taeger* 1983, 103 f.

Halbwahrheiten über datenschutzrechtliche Gefahren vorgeworfen.[2415] Zudem sei es wenig hilfreich, zwar die Strafen für das Nichtausfüllen des Bogens, nicht aber die für Verletzungen des Datenschutzgeheimnisses herauszukehren.[2416]

Als problematisch wurde außerdem die Einbettung der Datensammlung in die allgemein ausufernde öffentliche Datenverarbeitung gesehen.[2417] Darüber hinaus wurden Einzelfälle kritisiert, wie etwa die „Kopfprämie" der Stadt München, die für jeden von Zählern aufgefundenen nicht gemeldeten Deutschen 2,50 DM, für jeden Ausländer hingegen 5,- DM zahlen wollte.[2418] Schlussendlich konnte auf die Gründe des Scheiterns der Volkszählung in den Niederlanden zu Beginn der 80er Jahre des letzten Jahrhunderts verwiesen werden. Die Zählung wurde dort von der Mehrheit der Bevölkerung aus historischen Gründen abgelehnt, weil das zentral kontrollierte Personenregister in der NS-Besatzungszeit Tausende das Leben gekostet hatte, deren Verfolgung sonst viel schwieriger gewesen wäre.[2419]

7.3.2.2 Fallstudie 2: der maschinenlesbare Personalausweis

Die Geschichte der Einführung des maschinenlesbaren Personalausweises war von einer breiten Diskussion um Nutzen und Gefahren gekennzeichnet.[2420] Zu keiner Zeit allerdings entfachte diese ein ähnlich hohes Mobilisierungspotential wie die Volkszählung. Auch löste sie kein wegweisendes Urteil des Bundesverfassungsgerichts aus. Aus der heutigen Wahrnehmung ist die damalige Diskussion fast vollständig verschwunden.[2421] Beides ist umso bemerkenswerter, als der Ausweis ein weitaus höheres datenschutzrechtliches Missbrauchspotential enthält, da er Möglichkeiten permanenter Kontrolle schafft. Zwar erfragte die Volkszählung erheblich mehr persönliche Daten. Bei diesen handelt es sich jedoch um eine Momentaufnahme, was mittelfristig Nutzen wie Gefahren mindert. Das zeigt sich beim Blick auf die heutige Situation: Während es schwer vorstellbar ist, dass die Daten der Zählung des Jahres 1987 heute noch datenschutzrechtliche Probleme aufwerfen, sind die des Ausweises ungemindert.

7.3.2.2.1 Die Geschichte des maschinenlesbaren Personalausweises

Die Zeitspanne von der ersten Konzeption einer Ersetzung des (aus dem Jahre 1960 stammenden) alten Personalausweises bis zur tatsächlichen Umsetzung betrug fast zehn Jahre. Erste Ideen für eine maschinenlesbare Version stammen aus dem Jahre 1977, das heißt, sie wurden auf dem Höhepunkt der terroristischen Aktivitäten der Rote Armee Fraktion (RAF) geboren.[2422] Auf Beschluss der Innenministerkonferenz der Länder richtete das Bundesministerium des Innern im Jahre 1978 eine Arbeitsgruppe ein. Diese wurde unter wenig Beachtung der Öffentlichkeit tätig, sodass der Beschluss des Kabinetts über die Einführung des neuen Ausweises vom 23. Mai 1979 auch die Datenschutzbeauftragten überraschte. Von diesem Zeitpunkt an arbeiteten allerdings einige von ihnen im Gesetzgebungsverfahren mit und in der schließlich beschlossenen Fassung findet sich eine Reihe

2415 *Güllner* 1983, 192.
2416 Stellungnahme von *Hansen*, in: Taeger (Hrsg.) 1983, 52.
2417 *Brunnstein* 1983, 129 und die Kläger im Volkszählungsurteil, s. BVerfGE 65, 1 (17).
2418 Stellungnahme von *Grass* im Streitgespräch mit *Bull*, in: Taeger (Hrsg.) 1983, 43.
2419 *Vieten* 1983, 277.
2420 S. zum Folgenden schon *Roßnagel/Hornung*, in: Reichl/Roßnagel/Müller 2005, 301 ff.
2421 Die Internet-Suchmaschine Google findet am 18.5.2005 auf die Anfrage „maschinenlesbarer Personalausweis" lediglich 42 Treffer, für die Kombination aus „Volkszählung" und „Deutschland" sind es 63.000.
2422 *Pötzl* 1985, 123.

von Normen, die auf diese Mitwirkung zurückzuführen sind. Dazu gehören etwa die Verwendungsbeschränkungen des Ausweises und seiner Seriennummer, das (inzwischen durch das Terrorismusbekämpfungsgesetz aufgehobene) Verbot der Aufnahme verschlüsselter Daten[2423] sowie die ausdrückliche gesetzliche Erwähnung der Maschinenlesbarkeit. Außerdem wurde die automatische Einrichtung und Erschließung von Dateien (mit den Ausnahmen für Gefahrenabwehr- und Strafverfolgungsbehörden in § 3a Abs. 1 Satz 2 PersAuswG) verboten.

Der ursprünglich vorgesehene Einführungstermin (1. Oktober 1981) konnte wegen Kontroversen über die Finanzierung zwischen Bund und Ländern nicht eingehalten werden.[2424] Das neue Ausweisformat wurde in der Folge von der SPD/FDP-Regierung im Jahre 1982 beschlossen. Die SPD rückte allerdings später aus Datenschutzgründen von dem geplanten Vorhaben wieder ab. Der nunmehr avisierte Ausgabetermin, der 1. November 1984, wurde – unter anderem unter dem Einfluss des Volkszählungsurteils – zunächst zugunsten des 28. Februar 1986 aufgegeben.[2425] Dieser Zeitpunkt konnte jedoch ebenfalls nicht eingehalten werden. Die entsprechenden Gesetze wurden schließlich im April des Jahres 1986 verabschiedet und traten am 1. April 1987 in Kraft.[2426] Auch zu diesem Zeitpunkt war Deutschland allerdings im internationalen Vergleich immer noch Vorreiter hinsichtlich der Maschinenlesbarkeit des Ausweises. Der Austausch der Dokumente erfolgte im normalen Verfahren, das heißt über einen Zeitraum von fünf Jahren.

Erstmals wurde der neue Personalausweis durch nur einen Hersteller (die Bundesdruckerei) hergestellt und eine zentrale Datei eingerichtet, wenn auch nach § 3 Abs. 3 PersAuswG nur zum Nachweis des Verbleibs der Ausweise. Für die Personalausweisregister, die in einigen Bundesländern bereits existierten, wurde eine bundeseinheitliche Rechtsgrundlage geschaffen.[2427] Darüber hinaus bestimmte das neue Gesetz eine bis dahin nicht existierende allgemeine Gebühr für die Ausstellung des Ausweises.[2428] Eine solche bestand zuvor bereits für den Reisepass, war für den Personalausweis wegen der Ausweispflicht aber problematisch. Sie wurde mit dem Anfall höherer Kosten begründet.

Die Einführung des neuen Ausweises ist untrennbar verknüpft mit seiner Einbettung in eine Computerisierung der Polizeiarbeit und ein neues polizeiliches Fahndungskonzept, das vermehrt auf ereignis- und verdachtsunabhängige Kontrollen setzte.[2429] Hierzu gehörten etwa die Fahndungsdateien INPOL und NADIS[2430] sowie eine Reihe von Gesetzgebungsverfahren, die – teilweise um die Anforderungen zu erfüllen, die das Bundesverfassungsgericht im Volkszählungsurteil aufgestellt hatte – parallel zur Einführung des Ausweises durchgeführt wurden. So wurden etwa der Bundesnachrichtendienst (BND) und der

2423 Dieses war Ergebnis von Bedenken, es würden verdeckte und für den Inhaber nachteilige Informationen im Ausweis gespeichert, s. *Kauß* 1984, 71.

2424 S. *Schulz*, ZRP 1981, 143, 144 f.

2425 Vgl. *Dippoldsmann* 1986, 171; *Konferenz der Datenschutzbeauftragten*, DÖV 1984, 504, 507; s.a. die Vorlage des Bundesministers des Innern an den Innenausschuss v. 25.4.1984, DuD 1984, 281, 287 ff.

2426 Zweites Gesetz zur Änderung personalausweisrechtlicher Vorschriften v. 19.4.1986 und Bekanntmachung der Neufassung des Gesetzes über Personalausweise v. 21.4.1986, beide in BGBl. I, 545, 548; zur Gesetzgebungsgeschichte vgl. *Medert/Süßmuth* 1998, Einf. Rn. 28 ff.; s.a. die Berichte des Innenausschusses von 1979 (BT-Drs. 8/3498) und 1986 (BT-Drs. 10/5129).

2427 S. *Medert/Süßmuth* 1998, § 2a Rn. 1.

2428 Hierzu, und zur Frage der Rechtmäßigkeit s. VGH Mannheim, NVwZ-RR 2003, 712 f.; *Medert/Süßmuth* 1998, § 1 Rn. 29 ff.

2429 *Kauß* 1984, 48.

2430 S. dazu *Bölsche* 1979, 35 ff.

Militärische Abschirmdienst (MAD), die bis dahin lediglich auf der Basis von Kabinettsbeschlüssen gearbeitet hatten, auf gesetzliche Grundlagen gestellt.[2431]

Ähnlich wie die Neuauflage der Volkszählung im Jahre 1987 wurde auch die Einführung des maschinenlesbaren Personalausweises von einer groß angelegten Informationskampagne der Regierung begleitet, die die Funktionsweise und Vorteile des neuen Papiers zu vermitteln suchte. Das gesamte Planungs- und Implementierungsverfahren wurde zwar von massiver Kritik begleitet. Es gelang den Gegnern des neuen Ausweises jedoch nicht, eine der ersten Volkszählung vergleichbare Bewegung zu initiieren.

7.3.2.2.2 Wesentliche Argumentationslinien

Die (auch in der Informationskampagne verwendeten) Argumente für den neuen Ausweis betrafen im Wesentlichen die drei Bereiche Kriminalitätsbekämpfung, datenschutzrechtliche Unbedenklichkeit und Servicefunktion für den Bürger.[2432]

Zunächst wurde vorgebracht, die Verfälschbarkeit des alten Ausweistyps sei – etwa durch den Diebstahl von Blankovordrucken – massiv gestiegen. Dies sei gerade in Zeiten massiver Terrorismusbedrohung durch die RAF nicht hinnehmbar.[2433] Durch ungezielte Fahndung an der Grenze würden zwar bedeutende Erfolge erzielt.[2434] Die Abfragequote sei aber für ein Kriminalitätstransitland wie die Bundesrepublik zu gering[2435] und beeinträchtige die innere Sicherheit vor allem in den Bereichen des organisierten Verbrechens, des Rauschgifthandels, des Terrorismus und der Verschiebung gestohlener Kraftfahrzeuge.[2436] Betont wurde also die Nutzbarkeit des Ausweises als Fahndungsinstrument.

Daneben stellten die Befürworter die Mitwirkung der Datenschutzbeauftragten am Gesetzgebungsverfahren heraus.[2437] Aufgrund der eingearbeiteten Datenschutzbestimmungen sei der neue Ausweis unter diesem Gesichtspunkt unbedenklich. Eine höhere Fälschungssicherheit berühre die Rechte des Bürgers nicht. Das neue Format des Personalausweises bringe dem Bürger überdies Servicevorteile. Wenn und soweit das Fahndungssystem den Missbrauch personenbezogener Daten ausschließe, verkürze die Maschinenlesbarkeit die Abfertigung, erleichtere die Zügigkeit des Reiseverkehrs und mache den Kontrollvorgang fehlerfrei, weil Verwechslungen des Ausweisinhabers erschwert würden.[2438] Schließlich sei die Maschinenlesbarkeit lediglich ein Vorgriff auf internationale Regelungen, die zwangsläufige Übernahme neuerer technischer Entwicklungen und werde von der ICAO bereits gefordert.[2439]

Die ablehnenden Argumente lassen sich – ähnlich wie bei der Volkszählung – in drei Blöcke unterteilen. Die Kritiker stellten die prinzipielle Brauchbarkeit des neuen Auswei-

---

2431 S. hierzu und zu weiteren Gesetzen *Appel* 1986b, 290 ff.; *Ordemann*, RDV 1986, 60 ff.

2432 S. zum Folgenden schon *Roßnagel/Hornung*, in: Reichl/Roßnagel/Müller 2005, 301 ff.

2433 S. *Taeger* 1984a, 10.

2434 Vgl. *Kauß* 1984, 57.

2435 Die Angaben über die Kontrolldichte vor Einführung des neuen Ausweises schwanken zwischen jedem 120. (*Herold* 1988, 72) und jedem 150. (*Pötzl* 1985, 134) Reisenden. Für das neue Papier wurde sie auf jeden 30. Reisenden prognostiziert (*Pötzl* 1985, 134). Eine Gegenüberstellung mit heutigen Zahlen ist nicht sinnvoll, weil wegen des Wegfalls regelmäßiger Kontrollen an den Binnengrenzen der Mitgliedstaaten des Schengen-Acquis keine Vergleichbarkeit gegeben ist.

2436 S. Computerwoche Nr. 18/85; s.a. *Hoffmann* 1983, 98.

2437 S. *Kauß* 1984, 67.

2438 So etwa der Chef des BKA *Boge* (nach *Pötzl* 1985, 61); s.a. *Taeger* 1984a, 23 und den Bericht in Computerwoche Nr. 18/85.

2439 *Kauß* 1984, 77.

ses in Frage, erhoben datenschutzrechtlich Bedenken und kritisierten das gesetzgeberische Vorgehen.

Vorgebracht wurde zunächst, das Beschaffen eines falschen Ausweises durch Täuschung sei immer noch möglich. Außerdem benutzten Terroristen, wie das Beispiel RAF zeige, ohnehin ausländische Pässe.[2440] Überdies bestünde nach wie vor das Problem der Passersatzpapiere, für die Blankoformulare bei den Behörden verfügbar sein müssten.[2441] Die behauptete Steigerung der Fahndungserfolge sei zu bezweifeln. Ab einer gewissen Zahl von Kontrollen stiegen diese nicht mehr, jedenfalls nicht linear.[2442] Eine Gruppe von Datenschutzbeauftragten erklärte im Jahre 1986, der behauptete Sicherheitsgewinn sei bislang nicht dargetan.[2443]

Auch hinsichtlich der Servicevorteile wurde der Nutzen des Ausweises bestritten. Wegen der bevorstehenden Abschaffung der Kontrollen an den EG-Binnengrenzen sei das Argument einer schnelleren Abfertigung in weiten Bereichen sinnlos.[2444] Außerdem werde der Zeitgewinn durch die Zunahme der Kontrolldichte an den Grenzen wieder aufgezehrt. Im Ergebnis gelte die „Benutzerfreundlichkeit" eher für die Ausweisbehörden.[2445]

Die Argumente im Bereich des Datenschutzes waren sehr umfänglich. Sie führten dazu, dass Pläne fallengelassen wurden, spezifische Datenschutzregeln erst nach Einführung des Ausweises folgen zu lassen.[2446] Diese wurden vielmehr bereits bei der Einführung in das revidierte Personalausweisgesetz integriert.

Zunächst erfuhr die Einsetzbarkeit des Ausweises als „Massenkontrollmittel zur Überwachung großer Bevölkerungsteile" grundsätzliche Kritik.[2447] Schon die objektive Möglichkeit einer allgemeinen Registrierung aller Bürger sei verfassungswidrig.[2448] Außerdem bestehe die Gefahr einer Erfassung nicht nur von Straftätern, sondern von allen abweichenden Lebensformen. Im Ergebnis sei der Ausweis der „Schlüssel zum Daten- und Überwachungsstaat".[2449] Kritisiert wurde auch die Datenspeicherung bei der Bundesdruckerei. Die Einrichtung einer zentralen Datei werde zwar auf die Seriennummern beschränkt. Die damit einhergehende, wenn auch kurzzeitige, zentrale Speicherung der Daten zur Weiterverarbeitung sei aber bedenklich.[2450] Überdies sei es nicht akzeptabel, das Verbot zentraler Dateien auf die Bundesebene zu beschränken: auch landesweite Dateien seien datenschutzrechtlich abzulehnen.[2451] Durch die Maschinenlesbarkeit werde der Ausweis zudem zum Surrogat einer allgemeinen Personenkennziffer.[2452]

Ein weiterer Ansatzpunkt für Kritik war die durch den Ausweis erleichterte datenmäßige Profilbildung, etwa bei Grenzübertritten.[2453] Besonders beanstandet wurden in diesem Zusammenhang die so genannte „polizeiliche Beobachtung" und die Verbindung mit

2440 *Taeger* 1984a, 21.
2441 *Kauß* 1984, 44.
2442 *Kauß* 1984, 61.
2443 Vgl. *Konferenz der Datenschutzbeauftragten*, DÖV 1984, 504, 507; s.a. *Taeger* 1984a, 17.
2444 *Bäumler*, CR 1986, 284, 287; *Holtfort* 1986, 112.
2445 *Steinmüller* 1986, 60.
2446 *Bölsche* 1979, 75.
2447 *Steinmüller* 1986, 68; *Taeger* 1984a, 25; zum Problem der Quantität der Kontrollen auch *Büllesbach* 1984, 132; *Bäumler*, CR 1986, 284, 286.
2448 Angelehnt an die h.M. zur Überwachung von Arbeitnehmern im Betrieb, vgl. *Taeger* 1984a, 32.
2449 *Gössner* 1986, 128.
2450 Vgl. § 3 Abs. 3 PersAuswG; zur Geschichte dieser Norm und der Problematik der Speicherung zur Weiterverarbeitung s. *Büllesbach* 1984, 121.
2451 *Büllesbach* 1984, 131; *Taeger* 1984a, 29.
2452 *Büllesbach* 1984, 115; *Kauß* 1984, 68; *Steinmüller* 1982, 28; s.a. *Stollreither*, DuD 1986, 6; *Der Bundesbeauftragte für den Datenschutz*, DuD 1985, 87.
2453 *Pötzl* 1983, 77; *Taeger* 1984a, 25.

polizeilichen Datenbanken wie INPOL, NADIS, PIOS oder polizeilichen Störerdateien, die schon an sich für problematisch erachtet wurden.[2454] Auch die Regelung der Ausnahmen vom Verbot des automatischen Datenabrufs in § 3a Abs. 1 PersAuswG wurden scharf angegriffen. Die Ausnahme aller Dateien, die der Abwehr von Gefahren für die öffentliche Sicherheit dienten, gehe viel zu weit, da sie im Grundsatz jede polizeiliche Datenverarbeitung erfasse.[2455] Die größte Gefahr liege schließlich im Zusammenhang von personalausweisrechtlichen, melde- und polizeirechtlichen Regelungen.[2456] Der Ausweis sei insoweit grundsätzlich abzulehnen, da er als „Informationsmagnet" im Bedarfsfall zum Abruf auch dezentral gespeicherter Informationen dienen könne.[2457] In die gleiche Richtung zielten Einwände gegen Datentransfers zwischen Polizei und Geheimdiensten.[2458] Der frühere BKA-Chef *Herold* kritisierte den ersten Gesetzesentwurf, da dieser keine datenschutzrechtliche Funktionsteilung enthalte, sondern bisherige Trennungen sogar noch aufgehoben würden.[2459]

In Anlehnung an das Volkszählungsurteil finden sich des Weiteren Anmerkungen zur Gefahr von Einschüchterungseffekten bei der Wahrnehmung demokratischer Rechte.[2460] Die komplette Speicherung der Daten aller Teilnehmer einer Demonstration werde durch den Ausweis ebenso erleichtert wie der Abgleich mit bundesweiten Dateien der Hausbesetzer-, Anti-AKW- und Friedensbewegung.[2461]

Besonderes Augenmerk fand das Problem der Intransparenz. So könne der Bürger bei einer Vorlage des neuen Personalausweises nicht mehr erkennen, ob und wie seine Daten verarbeitet würden.[2462] Auch die vorgesehenen Online-Abfragen verletzten das vom Bundesverfassungsgericht aufgestellte Transparenzgebot. Einhellig forderten die Datenschutzbeauftragten das dann ins Gesetz aufgenommene Verbot, verschlüsselte Daten in den Ausweis einzubringen.[2463] Von anderer Seite wurde dagegen betont, weitere persönliche Daten des Inhabers würden ohnehin – intransparent – in Dateien gespeichert, die für den Bürger unerkennbar, für staatliche Stellen aber über den Personalausweis zugänglich seien.[2464] Vorgebracht wurde auch, die mit dem neuen Ausweis einhergehenden Belastungen seien unverhältnismäßig. Die höhere Fälschungssicherheit und das Ziel vermehrter Fahndungserfolge rechtfertigten nicht die hohen Kosten, den Verwaltungsaufwand, die Datenschutzrisiken und die Masse der Personenkontrollen.[2465] Durch deren Zahl werde überdies die Kontrolle der Datenschutzbeauftragten massiv erschwert.[2466]

Ansatzweise finden sich in der Debatte auch Besorgnisse um die Verwendung des Personalausweises im Ausland wegen des dortigen niedrigeren Datenschutzniveaus[2467] sowie um die Verwendung im privaten Bereich.[2468] Für den staatlichen Sektor wurde auf die

2454 *Gössner/Herzog* 1984, 206 ff.; *Taeger* 1984a, 27.
2455 *Kauß* 1984, 73; *Hoffmann* 1983, 98; *Seifert* 1984, 176.
2456 *Büllesbach* 1984, 117.
2457 *Schnepel* 1984, 146.
2458 *Paech* 1986, 77; *Taeger* 1984a, 30.
2459 Zitiert nach *Pötzl* 1985, 129.
2460 *Steinmüller* 1986, 70.
2461 *Kauß* 1984, 65; *Taeger* 1984a, 28.
2462 *Kauß* 1984, 79; *Steinmüller* 1986, 71.
2463 Vgl. 3 Abs. 1 PersAuswG a.F. (inzwischen durch das Terrorismusbekämpfungsgesetz ins Gegenteil verändert) und *Taeger* 1984a, 20.
2464 *Pötzl* 1985, 131.
2465 *Hoffmann* 1983, 96; *Taeger* 1984a, 33.
2466 *Kauß* 1984, 79.
2467 *Büllesbach* 1984, 140.
2468 *Bölsche* 1979, 86; *Stollreither*, DuD 1986, 6.

Gefahren neuer Technologien nach politischen Machtwechseln hingewiesen.[2469] Überdies gab es Kritik an der Gesetzestechnik, etwa an der mangelhaften Begründung des Gesetzes von 1986.[2470] Unter dem Gesichtspunkt der Wesentlichkeitslehre wurde auch das Fehlen eines Hinweises auf die Maschinenlesbarkeit des Ausweises im ersten Gesetzesentwurf kritisiert.[2471] Als Reaktion auf diese Kritik wurden noch im Gesetzgebungsverfahren Regelungen eingefügt, die die automatische Verwendung des Ausweises im Privatbereich ausschlossen und die Maschinenlesbarkeit regelten.[2472]

Weitere kritische Argumente betrafen Rationalisierungseffekte bei der Polizei[2473] sowie das allgemeine Problem der Absenkung kostenbedingter Kontrollbarrieren.[2474] Dem Staat wurde vorgeworfen, die Polizei werde unter Zuhilfenahme des neuen Ausweises als „gesellschaftliches Diagnoseinstrument“ und zur „allgemeinen Gesinnungskontrolle“ eingesetzt.[2475] Welche Schärfe die Diskussion annahm, zeigt sich an der Warnung, der neue Ausweis werde die Bundesrepublik in „einen Polizeirechtsstaat“ und eine „andere Republik“ verwandeln.[2476]

7.3.2.3 Bewertung

Um die Fallstudien für die anstehende Einführung von Chipkartenausweisen und die um diese geführte rechtspolitische Diskussion fruchtbar machen zu können, sind eine genauere Analyse und ein Vergleich mit den allgemeinen Akzeptanzfaktoren erforderlich.

7.3.2.3.1 Analyse der Fallstudien

Zunächst ist der Versuch der Volkszählung im Jahre 1983 ein Beispiel für eine totale Verkennung der datenschutzrechtlichen Probleme eines staatlichen Projekts und des damit einhergehenden Protestpotentials in der Bevölkerung.[2477] Durch die aus heutiger Sicht schwer nachvollziehbare Unterlassung einer Akzeptanzanalyse im Vorfeld des ersten Zählversuchs formierte sich – anders als bei vergleichbaren Problemfeldern wie der Atomkraft, der Startbahn West oder der Friedensbewegung, bei denen es jeweils Keimzellen im Vorfeld gab – innerhalb weniger Wochen eine Protestbewegung. Die verantwortlichen Stellen wurden vom Widerstand total überrascht und waren auf ihn nicht vorbereitet.[2478] Es ist nicht unwahrscheinlich, dass selbst das Bundesverfassungsgericht sich im Volkszählungsurteil von den massiven Protesten in der Bevölkerung beeinflussen ließ.[2479] Aus der Verkennung des Informationsbedürfnisses der Bürger resultierte im Jahre 1983 eine durchweg schlechte Aufklärung durch die statistischen Ämter. Schließlich leisteten die

2469 Vgl. *Schnepel* 1984, 147: „Wer als Guter ins Töpfchen und als Schlechter ins Kröpfchen kommt, ist eine politische Machtfrage. Die Sortiermaschine steht für alle Fälle bereit.“
2470 *Bäumler*, CR 1986, 284, 287.
2471 *Kauß* 1984, 45; *Konferenz der Datenschutzbeauftragten*, DÖV 1984, 504, 507.
2472 S. *Steinmüller* 1986, 61 (vgl. §§ 1 Abs. 3, 4 Abs. 2, Abs. 3 PersAuswG).
2473 Vgl. *Schnepel* 1984, 148: der „einfache Polizist vor Ort“ werde in erster Linie zum „rein mechanische[n] Karteneingeber“; s.a. *Taeger* 1984b, 216 f.
2474 *Myrell* 1984, 11.
2475 *Schnepel* 1984, 153.
2476 *Bölsche* 1979, 76.
2477 S. zur Analyse schon *Roßnagel/Hornung*, in: Reichl/Roßnagel/Müller 2005, 304 f.
2478 *Duve* 1983, 25.
2479 *Kauß* 1984, 82; *Würtenberger* 1987, 79 m.w.N.; M/D-*di Fabio*, Art. 2 Abs. 1 Rn. 173; *Mückenberger* (KJ 1984, 1, 3) spricht von einem Plebiszit in „ver-gerichtlichter“ Form.

Datenschutzbeauftragten von Bund und Ländern Informationsarbeit, obwohl sie die Volkszählung (oder jedenfalls Teile davon) durchaus kritisch sahen.[2480]

Die Einführung des neuen Ausweises war nicht imstande, auch nur ein annähernd gleiches Protestpotential zu mobilisieren. Das ist umso bemerkenswerter, als der Personalausweis datenschutzrechtlich bedenklicher war (und ist) als die Volkszählung.[2481] Die Akzeptanzsituation um das neue Papier ähnelt eher der bei der letztlich durchgeführten Zählung im Jahre 1987. Bei beiden wurden staatliche Informationskampagnen vorgeschaltet und Datenschutzbeauftragte eingebunden. Die Kampagne zur Volkszählung im Jahre 1987 kann wegen der relativ geringen Verweigerungsquote als grundsätzlich erfolgreich bezeichnet werden. Bedenklich ist aber, dass einigen Umfragen zufolge eine Mehrheit der Bevölkerung die Zählung zwar als ungefährlich, aber unnütz ansah. Sollte es gar zutreffen, dass die geringe Zahl der Verweigerer durch eine Furcht vor Repressionen erzeugt wurde,[2482] so wäre dies sicherlich kein wünschenswertes Ergebnis eines derart massiven staatlichen Informationsaufwands.

Ein wichtiger Faktor in der Diskussion (und Folge des Unterlassens staatlicher Information im Jahre 1983) war, dass es der Gegenbewegung – auch nach Ansicht der Befürworter – gelang, den Begriff „Volkszählung" in der öffentlichen Diskussion negativ zu besetzen. Hierin liegt ein gewichtiger Unterschied zur Einführung des maschinenlesbaren Personalausweises, bei dem dies nicht möglich war. Ein Grund hierfür dürfte sein, dass der Begriff des Personalausweises in Deutschland, anders als in anderen Staaten, keine negativen Konnotationen hat.[2483]

Bei der Analyse der Diskussionsmuster der Volkszählungs- und Personalausweisgegner fällt ein grundsätzlicher Unterschied auf. Ersteren gelang es, ein fundamentales Argument gegen die staatliche Maßnahme zu etablieren, nämlich die Fragwürdigkeit des Nutzens der Datensammlung und des dahinter stehenden staatlichen Planungsmodells. Beides war sogar in Fachkreisen umstritten. Beim Ausweis hingegen vermochte es der Staat, mit der Fälschungssicherheit und der Kriminalitätsbekämpfung zwei unmittelbare und greifbare Vorteile zu vermitteln. Selbst von den meisten Kritikern wurden diese Effekte nicht grundsätzlich, sondern nur dem Grad nach bestritten; sie hielten „lediglich" den dafür zu zahlenden Preis (Kosten, Datenschutzprobleme, höherer Überwachungsgrad) für zu hoch. Dieses waren aber politische Wertungsfragen, die ein signifikant geringeres Mobilisierungspotential entfalteten. Fundamentale Argumente fehlten in der Diskussion um den Personalausweis hingegen fast völlig.[2484] Darin liegt ein gewichtiger Grund für das Unterliegen der Einführungsgegner und die spätere Akzeptanz des Papiers.

Was den Umgang des Staates mit den Volkszählungsgegnern angeht, so finden sich einige Beispiele für überharte und rechtlich zweifelhafte Reaktionen.[2485] So speicherte das baden-württembergische Landeskriminalamt 127 "VoBos" (Volkszählungsboykotteure) in seiner Terroristen-Datei, obwohl das Vergehen juristisch allenfalls eine Ordnungswidrigkeit darstellte. In Berlin wies der damalige Finanzsenator und spätere Bundeswirtschafts-

2480 Die Meinungen über die Volkszählung waren unter den Datenschutzbeauftragten geteilt. So kritisierte etwa der Bundesdatenschutzbeauftragte *Bull* 1983 zwar den Melderegisterabgleich, verteidigte die Zählung aber im Grundsatz als unbedenklich.

2481 S. bereits oben Einl. zu 7.3.2.2.

2482 So *Appel/Hummel* 1988, 19.

2483 Die momentane Diskussion in den USA und in Großbritannien zeigt, dass die grundsätzliche Einstellung zum Institut des Personalausweises und seinem Begriff stark kulturell und historisch bedingt ist; s. näher oben 3.4.1.1, 3.5.2.1.

2484 Eine Ausnahme stellt die Forderung der Fraktion DIE GRÜNEN aus dem Jahre 1986 dar, die Personalausweispflicht völlig abzuschaffen (s. BT-Drs. 10/1316).

2485 S. *Sietmann*, c't 19/1999, 268, 273.

minister *Rexrodt* die zuständige Finanzdirektion an, Bußgelder gegen Volkszählungsgegner vorrangig zu bearbeiten; das Eintreiben von Steuerrückständen hatte demgegenüber zurückzustehen. Die Gegenbewegung sah sich durch die staatliche Repression politisiert und tendenziell sogar eher gestärkt.[2486]

In den heutigen Einstellungen der Bevölkerung zu Volkszählung und maschinenlesbarem Personalausweis bestehen erhebliche Unterschiede. Während die Volkszählung, trotz ihrer letztendlichen Umsetzung im Jahre 1987, als Beispiel für einen gelungenen Widerstand gegen eine staatliche Datenerhebung gilt, ist die Diskussion um den maschinenlesbaren Personalausweis aus dem öffentlichen Bewusstsein fast ganz verschwunden.[2487] Format und Handhabung des Ausweises sind vollständig akzeptiert; auch die im Jahre 1986 neu eingeführte Gebühr wird nicht mehr hinterfragt. Aus staatlicher Sicht stellt der maschinenlesbare Ausweis damit ein Modell für ein erfolgreiches Akzeptanzmanagement dar.

7.3.2.3.2 Vergleich mit den allgemeinen Akzeptanzfaktoren

In einem sehr eingeschränkten Umfang lassen sich auf der Basis der beiden Fallstudien zur Volkszählung und zum maschinenlesbaren Personalausweis einige der oben vorgebrachten Akzeptanzfaktoren empirisch überprüfen.

So kann festgehalten werden, dass eine breite gesellschaftliche Diskussion unter Einbeziehung von Kritikern, die Einbindung von Datenschutzbeauftragten zu einem möglichst frühen Zeitpunkt des Gesetzgebungsverfahrens und eine staatliche Informationskampagne sowohl kurz- als auch mittel- und langfristig starken Einfluss auf die Akzeptanz hatten. Bei der Einführung des neuen Personalausweises spielte außerdem die inhaltliche Plausibilität der seitens des Staates vorgebrachten Argumente eine Rolle. Schließlich war auch der Faktor des Vertrauens der Bevölkerung in das Bundesverfassungsgericht als normkontrollierende Instanz relevant. Das Gericht hatte ja den letztlich im Jahre 1987 durchgeführten Teil der Volkszählung im Urteil des Jahres 1983 für verfassungsgemäß erklärt und der Widerstand war im Jahre 1987 signifikant geringer. Es ist anzunehmen, dass diese Faktoren mehr oder weniger kontextunabhängig wirken und deshalb auch Einfluss auf die künftige Akzeptanz von Chipkartenausweisen haben werden.

Bei anderen der allgemeinen Einflussfaktoren lässt sich dagegen kein Einfluss auf die Akzeptanz feststellen. So trug das Gesetzgebungsverfahren in beiden Fällen wenig zur Akzeptanz bei. Weder die Einhaltung der relevanten Anforderungen an die Normbildung, noch der breite Konsens, mit dem etwa das erste Volkszählungsgesetz im Parlament verabschiedet wurde, vermochten den Protest aufzuhalten. Es wird vielmehr deutlich, dass auch einstimmig verabschiedete Gesetze auf massive Ablehnung stoßen können.

Wenn sich andere Faktoren nicht wiederfinden, so liegt dass zum Teil daran, dass sie keinen Bezug zur Volkszählung und zum Personalausweis haben. Das gilt etwa für Gleichheitsgesichtspunkte, Fragen sozialer Gerechtigkeit und die Unübersichtlichkeit der Rechtsordnung insgesamt. Was die individuelle Seite der Akzeptanz angeht, so ist diese auf Basis der gefundenen Erkenntnisse – mit Ausnahme der deutlich feststellbaren Furcht vor den mit der jeweiligen Maßnahme verbundenen (hier datenschutzrechtlichen) Risiken – kaum zu beurteilen.

2486 *Appel/Hummel* 1988, 23.

2487 S. dazu bereits die Ergebnisse der Internetrecherche, oben Fn. 2421 (S. 405).

7.3.2.3.3 Übertragbarkeit auf die derzeitige Akezptanzsituation von Chipkartenausweisen

Die Volkszählung und die Einführung des maschinenlesbaren Personalausweises sind zunächst im Kontext der allgemeinen gesellschaftspolitischen Diskussionen und Auseinandersetzungen in Deutschland zu Beginn der 80er Jahre des vorherigen Jahrhunderts zu sehen.[2488] In diesem Zusammenhang wurden etwa eine Verstärkung durchschnittlicher Erwartungsnormen und ein erhöhter Anpassungsdruck durch staatliche Beobachtungen und Datensammlungen kritisiert.[2489] Es lassen sich auch Querverbindungen finden: argumentiert wurde beispielsweise, die Einführung des maschinenlesbaren Personalausweises führe mit der Volkszählung zusammen zu einer höheren Kontrolldichte, die einen Normalisierungsdruck erzeuge,[2490] der neue Personalausweis sei damit eine „Volkszählung in Permanenz". Daneben gab es im Jahre 1983 eine Verknüpfung mit der Nachrüstungsdebatte.[2491] Diese Kontextfaktoren stellen sich heute grundlegend anders dar und schmälern die Übertragbarkeit der Ergebnisse.

Gleiches gilt für die Gründe des schnellen Anwachsens der Gegner beim ersten Zählversuch, nämlich das Misstrauen gegen eine zunehmende „Verdatung" des Bürgers, das grundsätzliches Misstrauen gegen den Staat, das sich in den gesellschaftlichen Auseinandersetzungen ab dem Ende der 60er Jahren aufgebaut hatte, das Misstrauen in die Planungswilligkeit und -fähigkeit des Staates (der wegen der Lobbyarbeit von Interessengruppen und der allgemeinen Unsicherheit über die Zukunft gar nicht rational planen könne), sowie die Abwehr des soziologischen Anspruchs der Statistik, die individuelle Lebenswelten ignoriere.[2492] Von diesen Faktoren dürfte kaum einer bestimmend für eine heutige Debatte sein.

Abschließend bleibt auf einen fundamentalen Unterschied der Rahmenbedingungen hinzuweisen. Die zunehmende Verbreitung der elektronischen Datenverarbeitung und der Multimediatechnik hat dazu geführt, dass heute große Bevölkerungsteile mit beiden selbstverständlich umgehen. Dies gilt gerade für die jüngere Generation. Insbesondere junge Menschen stellten jedoch in den 80er Jahren des letzten Jahrhunderts ein großes Protestpotential dar. Heutzutage steht dagegen zu erwarten, dass die grundsätzlichen Bedenken zumindest in den Bevölkerungsgruppen jüngeren und mittleren Alters sich jedenfalls nicht auf den Charakter der geplanten Ausweise als Chipkarte konzentrieren werden.

Die einzelnen zur Volkszählung und zum maschinenlesbaren Personalausweis vorgebrachten Argumente sind damit zwar nicht auf die heutige Situation übertragbar. Dies stellt sich hinsichtlich des Erfordernisses einer Akzeptanzanalyse anders dar. Außerdem sind Parallelitäten in den Argumentationsstrukturen erkennbar. So sind auch für Chipkartenausweise Diskussionen über praktischen Nutzen, datenschutzrechtliche Probleme, den Informationsanspruch des Staates, die Einbindung und Information der Öffentlichkeit sowie eine klare gesetzestechnische Regelung zu erwarten. Dies sind exakt die Punkte, die in der spezifischen Situation der beiden Fallstudien relevant waren. Die damaligen Debatten haben damit auch für die hier untersuchten Chipkartenausweise die relevanten Problem- und Diskussionsfelder abgesteckt.

2488 Vgl. zu diesem Abschnitt *Roßnagel/Hornung*, in: Reichl/Roßnagel/Müller 2005, 304 f.
2489 *Simon* 1983, 140.
2490 *Taeger* 1984b, 216.
2491 Unter dem Slogan „Wenn ihr uns nicht sagt, wo die Raketen stehen, sagen wir euch auch nicht, wo wir wohnen!", s. *Grohmann*, Berliner Statistik – Monatsschrift 2000, 216, 217.
2492 *Duve* 1983, 25.

7.3.3 Anwendung auf einzelne Chipkartenausweise und deren Funktionalitäten

Eine Prognose über die tatsächlich zu erwartende Akzeptanz der verschiedenen Chipkartenausweise ist mit sehr vielen Imponderabilien behaftet, weil die grundsätzliche Akzeptierbarkeit einer Technologie oder staatlichen Maßnahme nicht mit der im konkreten Fall zu erwartenden oder tatsächlich erfolgten Akzeptanz zusammenfallen muss.[2493] Dennoch lassen sich auf der Grundlage der bisher gewonnen Erkenntnisse und der Besonderheiten der einzelnen Ausweise und ihrer Einsatzumgebungen plausible Akzeptanzfaktoren erarbeiten.

7.3.3.1 Faktoren im Rahmen der Einführung biometrischer Verfahren

Die Einführung biometrischer Daten auf allgemeinen verpflichtenden Chipkartenausweisen ist bislang nur für den digitalen Personalausweis geplant.[2494] Da Deutschland hier – im Unterschied zur Einführung des maschinenlesbaren Personalausweises – im internationalen Vergleich nicht Vorreiter ist,[2495] lohnt es sich, einen Blick auf die Akzeptanzsituation in anderen Staaten zu werfen. Außerdem haben die bereits erfolgten gesetzgeberischen Aktivitäten Reaktionen hervorgerufen, die näher zu betrachten sind. Des Weiteren sind die allgemeinen Akzeptanzfaktoren und die Ergebnisse der Fallstudien auf den digitalen Personalausweis anzuwenden. Schließlich gibt es erste Akzeptanzerfahrungen aus anderen Biometrieprojekten im staatlichen und privaten Bereich.

Chipkartenausweise sind im Ausland generell auf relativ wenig Ablehnung gestoßen.[2496] Das gilt auch für die Einführung biometrischer Daten. Eine Übertragung der Erfahrungen anderer Länder ist allerdings nur mit Einschränkungen möglich, weil Akzeptanzfragen stark kulturabhängig sind. Wichtige Unterschiede ergeben sich etwa aus der Verschiedenartigkeit der Rechtssysteme, den unterschiedlichen Entwicklungen des Personalausweiswesens, einer anderen Einstellung der Bevölkerung gegenüber neuen Technologien und einer unterschiedlichen Sensibilität hinsichtlich Fragen des Datenschutzes. Das wird vor allem beim Blick in den angloamerikanischen Raum deutlich, wo – vor dem Hintergrund der fehlenden Ausweispflicht – die Diskussion nicht so sehr um Ausweistyp und Art der gespeicherten Daten, sondern um die Einführung allgemeiner Ausweispapiere an sich geführt wird.[2497]

Was die Aufnahme biometrischer Daten angeht, so ist eine Übertragung auf die Situation in Deutschland sogar noch schwieriger, weil eine Reihe der untersuchten Staaten schon vor der Einführung der jeweiligen Chipkarte über andere Ausweisformate mit diesen Daten verfügten. Das trifft etwa auf Malaysia, Hongkong und Macao zu. In diesen Ländern stellt die Verwendung biometrischer Angaben keine Neuheit dar, sodass auch kaum mit grundsätzlicher Ablehnung zu rechnen ist. In anderen Fällen bestehen andere Verfassungs- und Gesellschaftsstrukturen, in denen die Ablehnung staatlicher Maßnahmen nicht üblich, nicht opportun oder sogar gefährlich ist. Derartiges gilt beispielsweise für autoritäre Systeme (China) oder arabische Monarchien (Brunei, Oman). Beide Faktoren verhindern sinnvolle

2493 *Lucke* 1998, 16.

2494 Der zukünftige Reisepass wird biometrische Daten enthalten (dazu oben 3.1.2 und *Roßnagel/Hornung*, DÖV 2005, i.E.), jedoch nur auf Antrag ausgestellt werden. Technische Lösungen gibt es auch schon für elektronische Gesundheitskarten mit biometrischen Daten, s. http://www.cardtechnology.com/cgi-bin/readstory.pl?story=20040707CTDN607.xml.

2495 S. zur internationalen Entwicklung oben 3.

2496 Vgl. zu diesem Aspekt *Roßnagel/Hornung*, in: Reichl/Roßnagel/Müller 2005, 307 f.

2497 S.o. 3.4.1.1, 3.5.2.1, 3.5.2.2.

Rückschlüsse auf das Akzeptanzverhalten in Deutschland. Immerhin lässt sich aber im Erst-Recht-Schluss die Relevanz frühzeitiger Information der Öffentlichkeit über Verfahren und Risiken und der Einbeziehung von Datenschutzbeauftragten ableiten. Wenn derartiges sogar in den genannten Ländern für erforderlich gehalten wurde, so wird es in einem demokratischen System wie in Deutschland noch wichtiger sein.

In Deutschland haben die Regelungen des Terrorismusbekämpfungsgesetzes eine Reihe von Stellungnahmen von Datenschützern und anderen Gruppen hervorgerufen.[2498] Die überwiegende Zahl dieser Erklärungen befasst sich auch mit den Änderungen des Personalausweisgesetzes zur Einführung „weiterer biometrischer Merkmale". Die ablehnenden Argumente lassen sich wie bei der Volkszählung und dem maschinenlesbaren Personalausweis in drei Kategorien einordnen: Brauchbarkeit der Maßnahme, Datenschutzbedenken und Fragen des Gesetzgebungsverfahrens und der Regelungstechnik.

Für die Brauchbarkeit wird etwa auf die Fehlerraten biometrischer Systeme verwiesen, die einen Masseneinsatz nicht zuließen.[2499] Zu berücksichtigen sei auch der enorme technische und finanzielle Aufwand. Biometrie sei darüber hinaus kein Allheilmittel gegen Identitätstäuschungen und Fälschungen: bisher habe noch jedes neu eingeführte Sicherheitsmerkmal einen Wettlauf mit Fälschern hervorgerufen.[2500] Es finden sich Stimmen, die die Erforderlichkeit einer Veränderung des momentanen Ausweisformats in Bezug auf Fälschbarkeit des Ausweises, Identitätstäuschung und Gefahr von Terrorakten grundsätzlich bezweifeln. Die Regierung sei, was die Erforderlichkeit angehe, ihrer Nachweis- und Begründungspflicht nicht nachgekommen. Der Bundesminister des Innern habe im Bundestag auch auf Nachfragen keine Zahlen über Fälschungen deutscher Personalausweise vorlegen können.[2501]

Auf der datenschutzrechtlichen Ebene gibt es Bedenken gegen zukünftige zentrale wie dezentrale Speicherungen außerhalb des Ausweises, da diese zu Vorratsdatensammlungen und der versteckten Einführung eines Personenkennzeichens führen könnten.[2502] Vorbehalte werden daneben gegen ein Auslesen durch eine Vielzahl öffentlicher und privater Stellen und gegenüber den Gefahren einer allgegenwärtigen Überwachung, insbesondere bei der Gesichtserkennung, geäußert.[2503] Außerdem bestehe das Risiko von Verwechslungen, vor allem bei automatisierten Entscheidungen auf Basis biometrischer Datenabgleiche. Darüber hinaus könne der Bürger aufgrund der Verschlüsselung der Merkmale die Rich-

---

2498 Vgl. etwa *Konferenz der Datenschutzbeauftragten* 2002; *Der Landesbeauftragte für den Datenschutz Brandenburg* 2002, 19 ff., *Chaos Computer Club* 2001; *Kutscha* 2001; *Müller-Heidelberg* 2002; *Lepsius*, Leviathan 2004, 64 ff.; s. ferner die Stellungnahme von Bürgerrechtsorganisationen zur Anhörung des Innenausschusses des Bundestages am 30.11.2001, http://www.cilip.de/terror/atg-stell-281101.pdf und die Sammlung unter http://www.cilip.de/terror/stellung.htm; s. zum Folgenden auch *Roßnagel/Hornung*, in: Reichl/Roßnagel/Müller 2005, 306 f.

2499 Stellungnahme des *Chaos Computer Club*, s. http://www.heise.de/newsticker/meldung/42265; s. zu den Fehlerraten oben 4.2.2.4.1.1.

2500 *Chaos Computer Club* 2001, 2.

2501 *Müller-Heidelberg* 2002, 4; die Bundesregierung konnte auch Anfang Januar 2005 keine konkreten Daten zu der Zahl gefälschter deutscher Pässe nennen, s. die Antwort auf die Kleine Anfrage der FDP-Fraktion, BT-Drs. 15/4616, 2: die Grenzschutzdirektion untersuchte 2002 35 deutsche Pässe und 30 sonstige Ausweise wegen Verdachts auf Verfälschung oder fälschliche Ausstellung. Es gibt keine Angabe dazu, wieviele Fälschungen dabei tatsächlich entdeckt wurden.

2502 *Konferenz der Datenschutzbeauftragten* 2002, unter 4; s. zum Pesonenkennzeichen oben 4.2.1.2.4; 4.2.2.1.2.

2503 *Der Landesbeauftragte für den Datenschutz Brandenburg* 2002, 20 f.; ablehnend gegenüber der Datenerhebung ohne Kenntnis des Betroffenen auch *Konferenz der Datenschutzbeauftragten* 2002, unter 3.

tigkeit der Daten nicht mehr beurteilen.[2504] Schließlich sei ein Verstoß gegen das Verhältnismäßigkeitsprinzip zu beobachten.[2505]

Was das Gesetzgebungsverfahren angeht, so wird eine Verschleierung moniert: viele der Teile des Terrorismusbekämpfungsgesetzes, auch die Änderung im Personalausweisgesetz, hätten in Wahrheit nichts mit Terrorismusbekämpfung zu tun.[2506] Darüber hinaus sei das Verfahren mit völlig überzogener Geschwindigkeit durchgeführt worden.[2507] Insbesondere beim Personalausweisgesetz sei dies unverständlich, da es hier ohnehin noch eines weiteren Gesetzes bedürfe. Überdies habe es dem Gesetzgebungsverfahren an Transparenz gemangelt.

Betrachtet man nach diesem Blick auf die aktuelle Diskussion die allgemeinen Akzeptanzfaktoren, so lassen sich einige als für den digitalen Personalausweis irrelevant ausscheiden. Da es sich bei der Verwendung von Biometrie um eine grundlegende technische Neuerung handelt, kann es kaum Akzeptanzvorteile aufgrund von Tradition und Kontinuität geben. Inwieweit eine Konkretisierung der Verfassung oder ein Einfluss ethischer Wertüberzeugungen vorliegen könnte, ist nicht erkennbar, ebensowenig, dass vom Ausweis eine rechtsbefriedende Wirkung im eigentlichen Sinne ausgehen könnte. Faktoren wie die Unübersichtlichkeit der Rechtsordnung werden keine Rolle spielen, weil es sich um eine einzelne Sachfrage handelt.

Auf der Basis der internationalen Erfahrungen und der Fallstudien ist dagegen zu erwarten, dass ein offener, transparenter Meinungsbildungsprozesses für die Akzeptanz des digitalen Personalausweises mitentscheidend sein wird.[2508] Dazu gehören Informationen auch über Probleme und Risiken, gerade wegen der Neuartigkeit der verwendeten Techniken. Diese müssen in ihrer Funktionsweise erläutert werden, um deutlich zu machen, welche Risiken unbegründet und irrational, aber eben auch, welche in bestimmten Konstellationen begründet sein können. Je früher derartige Informationen angeboten werden, desto kleiner ist das Risiko für den Staat, dass in der öffentlichen Diskussion Begriffe negativ besetzt werden. Kontraproduktiv sind dagegen Geheimhaltungsstrategien wie etwa beim Feldversuch zur Gesichtserkennung am Flughafen Boston, bei dem hohe Fehlerraten über ein Jahr geheim gehalten wurden.[2509] Ein derartiges Verhalten schürt Vorbehalte und Misstrauen in der Bevölkerung und verursacht das Risiko, dass sich die im Grundsatz durchaus positiven Einstellungen zur Biometrie in der Bevölkerung[2510] ins Gegenteil verkehren.

Zu einem offenen Meinungsbildungsbildungsprozess gehört notwendigerweise auch die Einbeziehung von Minderheitspositionen. Wie das Beispiel Volkszählung (massive Ablehnung nach parlamentarischer Einstimmigkeit) gezeigt hat, darf sich das nicht nur auf par-

2504 *Chaos Computer Club* 2001, 2; *Lepsius*, Leviathan 2004, 64, 80.

2505 *Kutscha* 2001, unter 1; *Müller-Heidelberg* 2002, 2 f.; Stellungnahme des *Chaos Computer Club*, s. http://www.heise.de/newsticker/meldung/42265 und der Bürgerrechtsorganisationen zur Anhörung des Innenausschusses (s. Fn. 2498), 6 ff.; nach *Lepsius* (Leviathan 2004, 64, 80) ist der implizite „Generalverdacht" gegen die Bevölkerung nicht zu rechtfertigen.

2506 *Müller-Heidelberg* 2002, 2; *Lepsius*, Leviathan 2004, 64, 66.

2507 *Chaos Computer Club* 2001, 1; *Müller-Heidelberg* 2002, 1; Stellungnahme der Bürgerrechtsorganisationen zur Anhörung des Innenausschusses (s. Fn. 2498), 6 f.; *Sietmann*, c't 5/2002, 146, 147.

2508 Vgl. hierzu und zu den folgenden Faktoren *Roßnagel/Hornung*, in: Reichl/Roßnagel/Müller 2005, 308 ff.; s.a. *LSE* 2005, 91 ff.

2509 S. *Jodda* 2003.

2510 *Behrens/Roth* 2002, 413; *Büllingen/Hillebrand* 2002, 421 f. Die generelle Kenntnis über die Biometrie ist allerdings in Deutschland und Übersee eher gering. So konnten in Kanada im September 2003 nur weniger als 10 % der Bevölkerung den Begriff mit dem Gebrauch von Merkmalen wie Fingerabdruck oder Iris-Scan verbinden, s. *Citizenship and Immigration Canada* 2003, 2. Die Unterstützung für den hoheitlichen Einsatz von Biometrie nimmt allerdings kontinuierlich zu, vgl. ebd., 3 ff.

lamentarische Minderheiten erstrecken, sondern muss auch sonstige Kritiker und Datenschutzexperten umfassen. Positiv wird sich in diesem Zusammenhang ein angemessener Ausgleich zwischen Sicherheitsinteressen und Freiheitsrechten auswirken, in dem sich auch Kritiker wiederfinden können. Ein solcher Kompromiss könnte etwa in einem Verzicht auf verfassungsrechtlich gerade noch zulässige, aber politisch umstrittene Lösungen liegen.

Die Kontrolle durch Datenschutzbeauftragte ist ein bewährtes Instrument bei Erhebungs- und Verarbeitungsprozessen in der Verwaltung, in die der Bürger keinen Einblick hat. Trotz des fortbestehenden Problems der ministeriellen Aufsicht[2511] besteht ein hohes Vertrauen der Bevölkerung in die Unabhängigkeit der Datenschutzbeauftragten. Deswegen könnte durch ihre Einbindung im gesamten Verfahren, nämlich bei der Entwicklung, der Implementierung und dem Einsatz des Ausweises, dessen Akzeptanz gestärkt werden.

Die Faktoren für eine inhaltliche Zustimmung zum digitalen Personalausweis sind relativ schwer abzuschätzen. Es erscheint plausibel, dass sich das Argument der inneren Sicherheit („Terrorismusbekämpfung“) auf die Akzeptanz auswirken wird. Bei der Einführung des maschinenlesbaren Ausweises wurde das rationale Argument der verbesserten Verbrechensbekämpfung zwar in seiner Gewichtung, nicht aber in seiner Existenz angegriffen. Dies ist auch für den digitalen Personalausweis zu erwarten. Erneut sind die Regelungen für das neue Ausweisformat in ein Paket neuer Sicherheitsgesetze[2512] und die allgemeine technische Entwicklung (damals als „Computerisierung der Gesellschaft“[2513] bezeichnet) eingebettet. Zwar besteht gegenwärtig keine vergleichbare allgegenwärtige Terrorgefahr im Inneren, jedenfalls aber keine spezifisch deutsche Terroristenvereinigung wie die RAF. Andererseits ist auffallend, dass damals wie heute die Einführung des neuen Personalausweises mit der Abwehr einer Terrorgefahr (diesmal durch islamistische Gruppen) begründet wird. Dies dürfte sich erheblich auf die Akzeptanz des digitalen Personalausweises auswirken: Laut einer Umfrage aus dem Jahre 2003 schätzten die Befragten das individuelle (!) Risiko des internationalen Terrorismus drei Mal so hoch ein wie die Gefahr, Opfer einer Gewalttat zu werden.[2514]

Vor dem Hintergrund des Fehlens größerer Protestgruppen, die – wie bei der Einführung des maschinenlesbaren Personalausweises – ihr allgemeines Misstrauen gegenüber dem Staat öffentlichkeitswirksam kundtun, ist es möglich, dass die Einführung eines Personalausweises im Chipkartenformat und mit biometrischen Daten weniger suspekt erscheinen wird. Umgekehrt könnten mit zunehmendem zeitlichem Abstand zum 11. September 2001 die Argumente für eine Verbesserung der Sicherheitssituation in der öffentlichen Diskussion an Kraft verlieren.

Möglicherweise werden Teile der Bevölkerung den neuen Ausweis dennoch im Rahmen einer individuellen Kosten-Nutzen-Analyse akzeptieren und Eingriffe in das Recht auf informationelle Selbstbestimmung in Kauf nehmen, wenn sie einen signifikanten Sicherheitszuwachs, etwa im Rahmen der Flugsicherheit, erwarten. So der digitale Personalausweis als sichere Signaturerstellungseinheit eingeführt wird, könnte überdies darauf verwiesen werden, dass das Dokument eine echte Servicekomponente enthält.

2511 Vgl. etwa § 22 Abs. 4 Satz 3 BDSG. Die Aufsicht ist insoweit allerdings nur eingeschränkt gegeben, eine Fachaufsicht findet nicht statt; vgl. Simitis-*Dammann*, § 22 Rn. 15 ff.

2512 Kritisch zur Einbindung des maschinenlesbaren Ausweises in ein solches Gesetzespaket *Rühling* 1986, 11.

2513 *Schnepel* 1984, 144 ff.

2514 S. *Strebling/Burgheim*, Die Polizei 2003, 181, 183.

Ein Problem dürften die intransparenten Inhalte des Chips werden.[2515] Eines seiner wesentlichen Merkmale ist, dass die auf ihm gespeicherten personenbezogenen Daten für den Inhaber nicht mehr visuell erkennbar sind. Konnte sich bislang jeder Bürger persönlich vom Inhalt der Daten (und damit gleichzeitig auch von deren Richtigkeit) überzeugen, so wird dies in Zukunft nur noch mittelbar, durch Zuhilfenahme elektronischer Lesegeräte, möglich sein. Damit werden sowohl der aktuelle Inhalt des Ausweises als auch die Zugriffsmechanismen intransparent. Während der Bürger etwa bei einer Sichtkontrolle durch Polizeibeamte erkennen kann, ob Daten aufgenommen und gespeichert werden, ist dies bei einer Überprüfung durch elektronische Lesegeräte nicht mehr offensichtlich. Es besteht die Gefahr, dass sich in der Bevölkerung Misstrauen aufbaut, weil nicht klar ersichtlich ist, welche Daten auf dem Chip gespeichert sind, wer solche Daten aufbringt, sie ausliest oder verändert. Dem kann teilweise, aber sicher nicht vollständig durch ein System eines individuellen Überprüfungszugriffs des Ausweisinhabers entgegengewirkt werden.

Bei der Auswahl des biometrischen Merkmals werden für die Akzeptanz vor allem die über die reine Identitätsprüfung hinausgehenden Verwendungsmöglichkeiten relevant sein, insbesondere, wenn Daten auch noch an anderer Stelle als auf dem Personalausweis selbst gespeichert werden. Der Befund ist insoweit allerdings uneinheitlich.[2516] So ist der Fingerabdruck ein nicht-flüchtiges Merkmal, das heißt, man hinterlässt ihn in der realen Welt, wo immer man Gegenstände berührt. Das birgt die Gefahr von Rückverfolgbarkeiten in sich. Dieser Faktor spricht zunächst dafür, dass flüchtige Merkmale wie das Gesicht und die Iris auf größere Akzeptanz stoßen. Andererseits kann die Möglichkeit, ein biometrisches Merkmal wie das Gesicht heimlich zu erfassen, ein wesentliches Akzeptanzhindernis sein.[2517] Wenn im Bereich der Gesichtserkennung künftig die präzise automatisierte Erfassung mittels Abgleichs von zentralen Datenbanken auch bei sehr großen Menschenmengen, etwa auf öffentlichen Plätzen, durchführbar sein sollte, würden überdies neue Problemfelder entstehen. Bei der Verwendung der Iris besteht dieses Risiko nicht.

Die Akzeptanz der Biometrie hängt daneben von der Leistungsfähigkeit des verwendeten Systems ab. Produziert dieses zu viele Fehler beim Matching oder ist die Rate fehlerhafter Enrolmentversuche zu hoch, sinkt die Akzeptanz.[2518] Erforderlich ist also eine Robustheit und Alltagstauglichkeit der verwendeten Systeme.[2519] Daneben können Manipulationsmöglichkeiten, Vertraulichkeitsverluste und die mangelnde Kenntnis in der Bevölkerung über die Funktionsweise biometrischer Systeme deren Akzeptanz hemmen.[2520] Zumindest Anfang des Jahres 2000 war der Begriff Biometrie in Deutschland noch weitgehend unbekannt.[2521]

Weiterhin gibt es Faktoren, die nur ein biometrisches Merkmal betreffen. Die Iriserkennung wird bisweilen wegen der – falschen – Annahme abgelehnt, es werde ein Laser eingesetzt.[2522] Dies war ein Grund für die Regierung von Hongkong, stattdessen den Finger-

2515 Vgl. *Roßnagel/Hornung*, in: Reichl/Roßnagel/Müller 2005, 309.
2516 S. ausführlich oben 4.2.2.4.1.2.
2517 *Albrecht* 2002a, 95.
2518 *TAB* 2002, 11.
2519 *Albrecht* 2001, 52, 58; *TAB* 2002, 41; *VZBV* 2002, 39.
2520 *Albrecht* 2001, 38; aus Sicht der Technikfolgenabschätzung ist der Ausschluss von Manipulationen eine der Hauptforderungen an die Verwendung von Biometrie, s. *Büllingen/Hillebrand* 2002, 425.
2521 *Behrens/Roth* 2002, 410; s.a. *Albrecht* 2001, 38. In einer Umfrage am Jahresende 2001 hatte zwar die ganz überwiegende Mehrheit der Befragten den Begriff schon einmal gehört oder gelesen, nähere Kenntnisse waren jedoch nicht vorhanden, s. *Behrens/Roth/Büchner/Heumann/Stäblein/Weber* 2002, 452 ff.; s.a. *LSE* 2005, 91 ff.
2522 *Breitenstein* 2002, 51; *TAB* 2002, 16; zu den direkten medizinischen Implikationen der Biometrie (im Unterschied zur Frage der medizinischen Zusatzinformationen) s. *JRC/IPTS* 2005, 50 f.

abdruck zu wählen. Solchen Befürchtungen dürfte aber durch entsprechende Aufklärungsmaßnahmen entgegengewirkt werden können.

Fingerabdrucksensoren stoßen im öffentlichen Bereich mitunter auf hygienische Bedenken,[2523] wobei dies nach anderen Darstellungen kaum problematisch sein soll.[2524] In jedem Fall sind mittlerweile Systeme verfügbar, die ohne direkte Berührung des Sensors auskommen.[2525] Erfahrungsberichte über biometrische Anwendungen weisen darauf hin, die Verwendung von Fingerabdrucksdaten werde wegen der Assoziation mit der Behandlung von Verbrechern abgelehnt.[2526] Dies erscheint jedoch wenig plausibel. Im Rahmen erkennungsdienstlicher Maßnahmen werden auch Gesichtsaufnahmen gefertigt.[2527] Die Gefahr einer solchen Assoziation besteht überdies bei jeder staatlichen Erhebung biometrischer Daten. Für den digitalen Personalausweis kommt hinzu, dass eine Aufnahme von Fingerabdrucksdaten jeden Bürger gleichmäßig betreffen würde. Eine Stigmatisierung wie bei der bisherigen erkennungsdienstlichen Behandlung wäre somit ausgeschlossen. Sollte der Fingerabdruck außerdem datenschutztechnisch die beste Lösung sein,[2528] so dürfte es unschwer möglich sein, dieses Ergebnis in die öffentliche Meinung zu transportieren.

Sehr wichtig ist die Benutzerfreundlichkeit und Handhabbarkeit des Systems.[2529] Bei der Einführung jeder neuen Technologie besteht die Gefahr, dass bestimmte Bevölkerungsschichten mit der Entwicklung nicht Schritt halten können. Dies ist dann besonders problematisch, wenn die Verwendung eines neuen Verfahrens für jeden Bürger verbindlich vorgeschrieben wird. Genau dies wird beim neuen Ausweis hinsichtlich der Identitätsprüfung der Fall sein.[2530] Eine leicht verständliche Handhabbarkeit des biometrischen Systems ist von entscheidender Bedeutung für eine breite Akzeptanz in der Bevölkerung.[2531] Ist dies nicht gewährleistet, stellen sich darüber hinaus Probleme demokratischer Partizipation. Überforderungserfahrungen können sich negativ auf Persönlichkeit und Selbstwertgefühl der Betroffenen auswirken. Die Wahrnehmung von Betroffenenrechten (wie etwa die Auskunft über den Dateninhalt des Ausweises) muss deshalb auch für Menschen mit Behinderungen und technisch nicht Versierte möglich sein.

Bei der Benutzerfreundlichkeit werden des öfteren Vorteile für die Gesichtserkennung genannt.[2532] „Benutzerfreundlich“ meint in diesem Sinne allerdings lediglich, dass kein aktives Mitwirken des Betroffenen erforderlich ist. Insbesondere vor dem Hintergrund der datenschutzrechtlichen Risiken nicht mitwirkungsgebundener Systeme (Verhaltensüberwachung) erscheint es fraglich, ob dieser Faktor entscheidend sein wird. Zwar überwiegen bislang bei den Nutzern biometrischer Verfahren Bequemlichkeitsfaktoren in der persönlichen Bewertung der Systeme.[2533] Effizienz- und Komfortkriterien dürfen jedoch Daten-

2523 *TAB* 2002, 14.
2524 *Büllingen/Hillebrand* 2002, 424.
2525 Das hat auch Vorteile bei der Lebenderkennung (dazu oben 6.2.2), weil der Sensor nicht durch auf ihm verbleibende Spuren überlistet werden kann.
2526 Z.B. *Breitenstein* 2002, 40; *TAB* 2002, 14; *Bolle/Connell/Pankanti/Ratha/Senior* 2004, 146; s.a. *Rankl/Effing* 2002, 509; *OECD* 2004, 15.
2527 Auch historisch ist die Vermessung von Körpermerkmalen als kriminaltechnische Methode keineswegs auf den Fingerabdruck beschränkt, vgl. *Weichert*, CR 1997, 369.
2528 S. zu dieser Frage oben 4.2.2.4.1.2.
2529 Vgl. *Roßnagel/Hornung*, in: Reichl/Roßnagel/Müller 2005, 310.
2530 Deshalb wird der Akzeptanzfaktor der Freiwilligkeit der Verwendung von Biometrie (s. *Albrecht* 2002a, 94) ohne Bedeutung bleiben.
2531 *Behrens/Roth/Büchner/Heumann/Stäblein/Weber* 2002, 97, 155 ff.; *VZBV* 2002, 40. Die Akzeptanz eines biometrischen Verfahrens ist ohne einen allgemeinen Zugang zu diesem nicht denkbar, s. *Büllingen/Hillebrand* 2002, 429.
2532 Z.B. *Stock* 2002, 6; ähnlich *ICAO* 2004a, 17.
2533 *Büllingen/Hillebrand*, DuD 2000, 339, 340 f.; *TAB* 2002, 24.

und Verbraucherschutz nicht in den Hintergrund drängen, auch wenn (nicht ausreichend informierte) Nutzer dies möglicherweise akzeptieren würden.[2534] Eine solche Vorgehensweise würde zu gerade nicht erwünschten Ergebnissen führen, da bei einer entsprechenden Aufklärung über die Risiken nicht mehr der Komfort, sondern die datenschutzrechtliche Risikominimierung bei den Betroffenen in den Vordergrund tritt.[2535] Das belegen Umfragen unter informierten Nutzern, wonach 80 % der Befragten die Gewährleistung des Datenschutzes bei der Einführung eines biometrischen Systems als wichtig oder sehr wichtig ansehen; dieser Faktor ist damit von größerer Bedeutung als alle anderen Merkmale wie einfache Bedienung, Design, Preis-Leistungsverhältnis und lange Lebensdauer.[2536] Dies dürfte sich noch verstärken, falls sich ein spektakulärer Missbrauchsfall ereignen sollte.

Die Skepsis gegenüber Mechanismen der Datenerhebung und -verarbeitung ist immer dann besonders groß, wenn sie mit Gefahren der Überwachungstätigkeit auf bis dahin unbekanntem Niveau verbunden ist. Dies ist etwa bei der aktuellen Diskussion um die Videoüberwachung in Innenstadtbereichen erkennbar.[2537] Jede neuartige Form der Datensammlung begegnet Bedenken, sie könne an sich oder durch Verknüpfung mit anderen Datenbanken dem „gläsernen Bürger" Vorschub leisten. Insoweit besteht (zu Recht) eine hohe Sensibilität gegenüber Gefahren der Profilbildung durch digitale Datensammlungen.

Insgesamt kann Vertrauen nur eingeschränkt durch rechtliche Sicherungsmechanismen erzeugt werden, weil diese immer auf zwei Ebenen anfällig sind. Zum einen besteht die tatsächliche Gefahr des Verstoßes gegen die gesetzlich geregelten Zugriffsbefugnisse zu Missbrauchszwecken, sei es durch private Angriffe von außen, sei es durch eine unzulässige Datenproliferation zwischen verschiedenen Sicherheitsbehörden. Zum anderen ergeben sich Risiken durch die Möglichkeit einer nachträglichen Zweckänderung durch den Gesetzgeber, um die bereits vorhandenen Daten legal für weitere Zwecke verwenden zu können.

Aus diesen Gründen ist davon auszugehen, dass technische Sicherungsmittel zum Schutz der Daten einen deutlich höheren Akzeptanzwert als rechtliche Instrumente haben.[2538] So zeigen Ergebnisse von Nutzerbefragungen, dass eine Speicherung biometrischer Daten auf einer Chipkarte gegenüber der zentralen Variante bevorzugt wird.[2539]

Schließlich ist eine Akzeptanz ohne Alternativsysteme für ungeeignete Betroffene kaum vorstellbar.[2540] Zwar wird das Ausweisformat im Grundsatz allgemein und für jeden verbindlich eingeführt.[2541] Auf der Kontrollebene sind jedoch flexible Einzellösungen für Bürger möglich, die dauerhaft oder temporär nicht biometrisch erkannt werden können.

Jede Form der Ungleichbehandlung führt zu massiven Akzeptanzproblemen. Bei einigen der bereits im Einsatz befindlichen biometrischen Systeme wurden nur Personen zugelassen, die zuvor eine Sicherheitsüberprüfung durchlaufen hatten. Die US-amerikanischen (INSPASS) und kanadischen (CANPASS-Air und NEXUS-Air) „trusted travellers" Programme schließen Personen mit Vorstrafen explizit aus. Auch bei der ICAO gibt es Bestrebungen, Reisende entsprechend ihres – individuell festgestellten – „risk level" unter-

2534 *TAB* 2002, 25.

2535 *Albrecht*, DuD 2000, 332, 338. Ohne eine solche Aufklärung ist das allgemeine Wissen um die datenschutzrechtlichen Gefahren der Biometrie gering, s. *Büllingen/Hillebrand* 2002, 421.

2536 *Behrens/Roth/Büchner/Heumann/Stäblein/Weber* 2002, 455.

2537 S. dazu z.B. Roßnagel-*v. Zezschwitz*, Kap. 9.3; *Gola/Klug*, RDV 2004, 65 ff., jeweils m.w.N.

2538 Dieser Gedanke ist Grundlage des Konzepts des Systemdatenschuztes, s.o. 4.3.2.2.

2539 *Behrens/Roth/Büchner/Heumann/Stäblein/Weber* 2002, 384 f.

2540 S.a. *Büllingen/Hillebrand* 2002, 423.

2541 Vorbehaltlich der Beibehaltung der bisherigen Ausnahme in § 1 Abs. 1 Satz 1, 2. Halbsatz PersAuswG für Inhaber eines Reisepasses. Da dieser jedoch sogar vor dem Personalausweis um biometrische Daten erweitert werden wird (s.o. 3.1.2), stellt dies keine Ausweichmöglichkeit dar.

schiedlich intensiven Kontrollen zu unterwerfen.[2542] Diese Form der Selektierung nach Gruppen, die in den Augen der Sicherheitsbehörden ein mehr oder weniger großes Sicherheitsrisiko darstellen, wäre auch im Vollbetrieb eines allgemeinen biometrischen Reisedokuments denkbar – mit bislang kaum absehbaren Folgen für dessen Akzeptanz.

Im Ergebnis wird deutlich, dass die Akzeptanz des digitalen Personalausweises hinsichtlich der verwendeten biometrischen Daten stark durch die Aufklärung über Funktionsweise und Risiken beeinflusst werden wird, letztlich jedoch in wesentlichen Teilen eine Funktion von Datenschutz und Datensicherheit ist.[2543] Ein hohes Schutzniveau wirkt in diesen Bereichen risikomindernd und beeinflusst damit die rationale Komponente der Akzeptanz positiv. Durch einen Verzicht auf jede Speicherung außerhalb des Ausweises, die Beschränkung von Zugriffsbefugnissen und deren Absicherung durch Authentisierungs- und Verschlüsselungsverfahren sowie die Einrichtung effektiver Alternativverfahren für zur Erkennung ungeeigneter Bürger wird deshalb nicht nur verfassungsrechtlichen Anforderungen genügt, sondern auch ein wichtiger Beitrag zur Akzeptanz des digitalen Personalausweises geleistet.

7.3.3.2 Faktoren aus dem Bereich des Gesundheitswesens

Für die elektronische Gesundheitskarte sind Akzeptanzüberlegungen von großer Wichtigkeit, weil die Mehrzahl ihrer Applikationen nach § 291a Abs. 3 Satz 3 SGB V freiwillig sein wird. Nur wenn diese in der Bevölkerung akzeptiert werden, ist mit einer größeren Zahl von Entscheidungen für ihren Einsatz zu rechnen. Die Ausgangsbedingungen hierfür sind durchaus positiv: Nach Umfragen können sich bis zu 80 % der Bürger vorstellen, die freiwilligen Anwendungen der Gesundheitskarte zu nutzen.[2544]

Anders als beim digitalen Personalausweis existieren für die elektronische Gesundheitskarte bislang keine aussagekräftigen Erkenntnisse über Akzeptanzfaktoren im Ausland, weil es dort so gut wie keine allgemein ausgegebene Multifunktionskarte gibt, die der geplanten Ausgestaltung der deutschen elektronischen Gesundheitskarte entspricht.[2545] Erste Erkenntnisse aus Österreich sprechen dafür, dass die dortige – bislang in Feldversuchen ausgegebene – Karte von den Patienten positiv aufgenommen wird.[2546] Stellungnahmen zum Einsatz elektronischer Datenverarbeitung im deutschen Gesundheitswesen gibt es demgegenüber zwar in größerer Zahl. Das gilt allerdings nicht für die Regelungen des GKV-Modernisierungsgesetzes zur elektronischen Gesundheitskarte. Die öffentliche Diskussion um dieses Gesetz konzentriert sich auf kontroverse Neuregelungen im Bereich der Zuzahlungsregelungen (insbesondere der Praxisgebühr).[2547]

Die elektronische Gesundheitskarte wird in ein Gesamtsystem der Gesundheitstelematik eingebettet sein. Grundsätzliche Akzeptanzprobleme sind in diesem System immer dann zu befürchten, wenn sensible Gesundheitsdaten wie Angaben über bestimmte Krankheiten für Personen verfügbar werden, die bislang keinen Zugriff auf diese Informationen haben. Das kann durch missbräuchlichen Datenzugriff, aber auch durch eine Ausweitung rechtlich zulässiger Datentransfers geschehen. Die missbräuchliche Verwendung von Gesundheits-

2542 Vgl. http://www.icao.int/icao/en/atb/fal/fal12/documentation/fal12ip007_en.pdf.

2543 Datensicherung als Voraussetzung der Akzeptanz jeder Datenverarbeitung wird schon betont von *Pütter*, DuD 1991, 67 ff. und 227 ff.; s.a. *Hillebrand*, DuD 1998, 218.

2544 S. http://www.aerztezeitung.de/docs/2005/01/20/009a0403.asp?cat=/politik/gesundheitssystem_uns.

2545 Das gilt mit Ausnahme der Gesundheitskarte Taiwans, s.o. 3.2.2.6.

2546 Vgl. http://www.heise.de/newsticker/meldung/57412.

2547 S. dazu aus juristischer Sicht *Butzer*, MedR 2004, 177, 182; *Hiddemann/Muckel*, NJW 2004, 7, 12 f.

daten birgt die Gefahren von Diskriminierung und Ausgrenzung.[2548] Eine zunehmende Transparenz des Patientenverhaltens kann dazu führen, dass Krankheit als „selbstverschuldeter Makel“[2549] begriffen wird. Während eine vorsichtige Verhaltenssteuerung hin zu einem gesundheitsbewussten Lebensstil ein legitimes Anliegen der Gesellschaft ist, würde eine weitgehende Beobachtung und Dokumentation des Lebenswandels des Einzelnen zu Akzeptanzschwierigkeiten führen. Ähnlich wie beim digitalen Personalausweis entsteht auch bei der elektronischen Gesundheitskarte überdies ein Transparenzproblem: Sowohl die Speicherung auf der Karte selbst als auch die auf Servern führt zu einer Sammlung von Patientendaten, deren Art und Umfang dem Karteninhaber nicht unmittelbar ersichtlich und zugänglich ist.[2550]

Die Gesundheitstelematik wird nur dann akzeptiert werden, wenn die Verantwortlichkeiten für die Datenverarbeitung exakt definiert und die daraus resultierenden Haftungsfragen geklärt sind.[2551] Der Einsatz von Telematik kann zu einer Verbesserung der Gesundheitsversorgung führen, birgt jedoch auch Schadenspotentiale, die nicht ungeregelt bleiben dürfen. Die Auslagerung medizinischer Aufgaben an externe Stellen kann eine flächendeckende Verfügbarkeit ärztlichen Fachwissens bewirken, aber auch eine Abgabe von Aufgaben an weniger qualifizierte Personen mit sich bringen.[2552] Bei der Einrichtung dezentraler Versorgungsstrukturen besteht die Gefahr eines Verlusts von Kontextwissen, das in Folge der standardisierten Datenformate nicht mitübermittelt werden kann.[2553] Eine zunehmende Überwachung der ärztlichen Tätigkeit würde schließlich nicht nur bei den Patienten, sondern auch bei den Leistungserbringern Akzeptanzprobleme hervorrufen, da diese ihre Therapiefreiheit gefährdet sehen könnten.[2554] Es ist heute kaum abzuschätzen, was der Einsatz von Telematik im Gesundheitswesen für das Berufsbild und das Selbstverständnis der Ärzte einerseits und für die Arzt-Patient-Interaktion andererseits bedeuten wird. Umfragen zufolge sieht eine Mehrheit in der Ärzteschaft die Einführung der Gesundheitskarte zumindest skeptisch.[2555] Die Ärzte bemängeln eine mangelnde Information und Beteiligung und befürchten Probleme bei Aufwand und Betriebsablauf sowie im Datenschutzbereich.[2556]

Wichtige Erfordernisse des Datenschutzes und der Datensicherheit müssen beachtet werden. Nur dann, wenn die technischen Infrastrukturen der elektronischen Gesundheitskarte und der Gesundheitstelematik insgesamt Informationen hoch verfügbar und in bester Qualität bereitstellen und gleichzeitig Persönlichkeitsrechtsverletzungen effektiv verhindern,[2557] wird die Karte auf Akzeptanz bei den Versicherten stoßen. Eine Umfrage in der Testregion Flensburg ergab, dass 38 % der Befragten Bedenken wegen eines möglichen

2548 *Elkeles/Rosenbrock* 1995, 12.
2549 *Fuest* 1999, 95; s.a. *Hammer/Roßnagel* 1989, 131; *Iwansky* 1999, 52; *Bertrand/Kuhlmann/Stark* 1995, 122, 130 ff.; *BSI* 1995, 38 f.
2550 *Müller* 2004, 214.
2551 *Bertrand/Kuhlmann/Stark* 1995, 127; *Fuest* 1999, 100; ausführlich zu den Haftungsproblemen vgl. ebd., 118 ff.; *Dierks/Nitz/Grau* 2003, 152 ff.; *Steffen* 2001, 71 ff.; *Pflüger*, VersR 1999, 1070 ff.; s.a. *BSI* 1995, 49 ff.; *Berger & Partner* 1997, 109 f.
2552 *Dierks/Nitz/Grau* 2003, 25 f.
2553 *Hammer/Roßnagel* 1989, 136; *Bertrand/Kuhlmann/Stark* 1995, 120; *BSI* 1995, 36 f.; *Iwansky* 1999, 55.
2554 *Hammer/Roßnagel* 1989, 121; *Roßnagel/Wedde/Hammer/Pordesch* 1990, 191; *Fuest* 1999, 99; auf die Gefahr der Überwachung der Beschäftigten weisen *Bertrand/Kuhlmann/Stark* (1995, 127) hin.
2555 S. http://www.heise.de/newsticker/meldung/56435; http://www.aerztezeitung.de/docs/2005/02/15/027a0104.asp.
2556 Vgl. http://www.aerztezeitung.de/docs/2005/02/16/028a1801.asp?cat=/politik/gesundheitssystem_uns.
2557 *Dierks/Nitz/Grau* 2003, 22 ff. m.w.N., 27 ff.; s.a. *Konferenz der Datenschutzbeauftragten* 2005.

Datenmissbrauchs hegten.[2558] Umgekehrt hält eine Mehrheit der Betroffenen den Schutz für gewährleistet, solange sie selbst bestimmen, wer auf welche Angaben zugreifen darf.[2559]

Ähnlich wie bei der Einführung biometrischer Daten beim digitalen Personalausweis bietet die strikte Einhaltung datenschutzrechtlicher Anforderungen damit ein Instrument zur Verbesserung auch der Akzeptanz der elektronischen Gesundheitskarte. Die dort gefundenen Ergebnisse sind größtenteils auf das Gesundheitswesen übertragbar. Durch die Mitwirkung des Versicherten, die Gewährleistung eines effektiven Auskunftsrechts, die datensparsame Ausgestaltung der Telematik, die Beschränkung der Zugriffsbefugnisse auf das notwendige Maß und die Einrichtung eines im Einzelfall abstufbaren Zugriffsschutzes werden verfassungsrechtliche Anforderungen erfüllt. Gleichzeitig wird die Akzeptanz der elektronischen Gesundheitskarte gefördert.

Das gilt auch für eine Einbeziehung der Versicherten in den Prozess der Entwicklung, Ausgestaltung und Implementierung der Karte. Hier ist bemängelt worden, dass sich die handelnden Akteure nur mit den technischen Spezifikationen beschäftigten, ohne sich um Vermittlung und Außendarstellung zu bemühen.[2560] Wie beim digitalen Personalausweis ist schließlich damit zu rechnen, dass die Einbeziehung von Datenschutzbeauftragten im gesamten Verfahren der Akzeptanz förderlich sein wird. Die Bundesregierung hat sich bemüht, Verbraucherschutzorganisationen und Selbsthilfegruppen chronisch kranker und behinderter Menschen in die konzeptionellen Arbeiten einzubinden.[2561]

Die konkrete Ausgestaltung des technischen Zugriffsmanagements darf keinesfalls technisch nicht Versierte überfordern. Andernfalls besteht die Gefahr, dass Teile der Bevölkerung von ihrem Recht auf Geheimhaltung de facto keinen Gebrauch machen können.[2562] Ein zu komplexes Zugriffssystem führt im Ergebnis nicht zu mehr, sondern zu weniger informationeller Selbstbestimmung, weil es den Betroffenen mangels Handhabbarkeit des Systems doch wieder vor die Wahl stellt, den Zugriff auf den gesamten Datenbestand zu erlauben oder ihn insgesamt zu verweigern. Da letzteres in einer Behandlungssituation unrealistisch ist, wäre das Erfordernis der Mitwirkung des Karteninhabers ohne praktische Wirkung. Um dies zu vermeiden, bietet es sich an, schon im Rahmen der Pilotprojekte zur Gesundheitskarte gezielt ältere und schwer kranke Versicherte als Testpersonen zu rekrutieren.[2563]

Die datenschutzrechtlichen Risiken der Gesundheitstelematik können sich negativ auf deren Akzeptanz auswirken. Andererseits werden die offensichtlichen Vorteile ihres Einsatzes (auch) für die Versicherten einen gegenläufigen Effekt haben.[2564] Der Einsatz von Informationstechnologie im Gesundheitswesen erfährt immer dann eine hohe Akzeptanz,

---

2558 Vgl. http://www.aerztezeitung.de/docs/2005/01/20/009a0403.asp?cat=/politik/gesundheitssystem_uns.

2559 Das ist das Ergebnis einer Umfrage der Techniker Krankenkasse, s. http://www.aerztezeitung.de/docs/2005/02/15/027a0404.asp?cat=/politik/gesundheitssystem_uns.

2560 *Brenner* 2004, 221; s. bereits *Bertrand/Kuhlmann/Stark* 1995, 137; *Stark* 1998, 35 ff.

2561 S. die Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten *Sehling*, *Storm*, *Widmann-Mauz*, weiterer Abgeordneter und der Fraktion der CDU/CSU v. 30.3.2004, BT-Drs. 15/2810, 15.

2562 S.o. 6.3.3.1; *Bertrand/Kuhlmann/Stark* 1995, 126; s.a. *BSI* 1995, XV, 62; *Grätzel v. Grätz* 2004c, 127 f.

2563 Dieser Ansatz wurde bei der Gesundheitskarte Schleswig-Holstein verfolgt, s. http://www.aerztezeitung.de/docs/2005/02/14/026a0102.asp?cat=/politik/gesundheitssystem_uns.

2564 *Der Bundesbeauftragte für den Datenschutz* 2002, 146; *BITKOM/VDAP/VHitG/ZVEI* 2003, 5, 14 f.; s.a. die Ergebnisse der Umfrage der Techniker Krankenkasse, http://www.aerztezeitung.de/docs/2005/02/15/027a0404.asp?cat=/politik/gesundheitssystem_uns; s. zu den Motiven im Einzelnen oben 2.1.2.

wenn ein Nutzen für den Patienten erkennbar ist.[2565] Angesichts der immer größer werdenden Bedeutung der eigenen Gesundheit für die Menschen wird das Argument einer verbesserten Versorgung die Akzeptanz der elektronischen Gesundheitskarte positiv beeinflussen. Gleiches gilt für die Vermittlung der Tatsache, dass die Karte zu Kostenersparnissen und mehr Beitragsgerechtigkeit im Gesundheitswesen führt und die Versicherten aufgrund der paritätischen Finanzierung der gesetzlichen Krankenkassen hiervon unmittelbar profitieren werden.

Diese akzeptanzfördernden Effekte dürften aber dann entfallen, wenn keine effektiven Sicherungen der Vertraulichkeit medizinischer Daten und des Vertrauensverhältnisses zwischen Arzt und Patient gewährleistet werden.[2566] Aspekte von Datenschutz und Datensicherheit sind nämlich nach empirischen Erkenntnissen die größten Akzeptanzhürden für den Einsatz von Telematik im Gesundheitswesen.[2567] Im Ergebnis ist deshalb die Vertraulichkeit der Daten Grundvoraussetzung der Akzeptanz jeder Datenverarbeitung, insbesondere aber bei sensiblen Daten wie den Angaben, die im Gesundheitswesen verwendet werden.[2568]

7.3.3.3 Faktoren bei der Einführung elektronischer Signaturverfahren

Die Ausgangssituation für die Akzeptanz elektronischer Signaturverfahren auf Chipkartenausweisen ist vielschichtig. Einerseits ist bislang nicht geplant, einen bestimmten Ausweis zwangsweise in signaturfähigem Zustand an die Bürger abzugeben.[2569] Werden andererseits die Pläne für das JobCard-Verfahren umgesetzt, so wird vom Jahre 2007 an für jeden Antragsteller in der gesetzlichen Arbeitslosenversicherung – perspektivisch für alle abhängig Beschäftigten – die Pflicht bestehen, eine Signaturkarte zu besitzen. Daraus resultiert zwar kein Zwang, diese in anderen Situationen einzusetzen. Die große Verbreitung sicherer Signaturerstellungseinheiten könnte aber durchaus dazu führen, dass die Verwendung qualifizierter Signaturverfahren auch in anderen Lebensbereichen (beispielsweise am Arbeitsplatz) zur Pflicht wird.

7.3.3.3.1 Die Akzeptanz eines signaturfähigen Ausweises

Erfahrungen aus dem Ausland zeigen, dass dort in der Öffentlichkeit keine Einwände dagegen erhoben werden, Signaturverfahren auf breiter Basis durch Chipkartenausweise zur Verfügung zu stellen.[2570] Das scheint selbst dann zu gelten, wenn ein Personalausweis – ohne Wahlmöglichkeit für den Antragsteller – voll signaturfähig ausgegeben wird. Zwar gibt es mit Estland und Macao erst zwei Beispiele für diese Vorgehensweise. Über ablehnende Reaktionen dort ist jedoch nichts bekannt. Allerdings wurde die Einführung des

2565 Vgl. die positiven Stellungnahme von *DGVP* (2003) und *VZBV* (2003, 7 f.); s. für das Bsp. Telemonitoring und „Smart Home Care“ bei älteren Menschen *Böhm/Röhrig/Schadow*, DÄ 2003, B 2743 ff.

2566 Ziel der Einführung von Telematik im Gesundheitswesen muss deshalb der Erhalt dieses Vertrauensverhältnisses sein, s. *Goetz* 2001, 5; *Grätzel v. Grätz* 2004c, 15 ff.

2567 S. *Dierks/Nitz/Grau* 2003, 130 m.w.N.

2568 *Ulsenheimer/Heinemann*, MedR 1999, 197, 202; *Müller* 2004, 214; *Der Bundesbeauftragte für den Datenschutz* 2002, 146; *BITKOM/VDAP/VHitG/ZVEI* 2003, 17; *Konferenz der Datenschutzbeauftragten* 2005.

2569 Das gilt jedenfalls für qualifizierte Verfahren. Die Gesundheitskarte muss gemäß § 291 Abs. 2a Satz 3 SGB V technisch geeignet sein, Authentifizierung, Verschlüsselung und elektronische Signatur zu ermöglichen. Dadurch werden qualifizierte Signaturverfahren zwar erlaubt, aber nicht vorgeschrieben. Nach der „eCard-Strategie“ der Bundesregierung sollen Personalausweis und Gesundheitskarte optional die Möglichkeit qualifizierter Signaturverfahren bieten, s.o. Einleitung zu 5.

2570 S.o. 3; zum Folgenden *Roßnagel/Hornung*, in: Reichl/Roßnagel/Müller 2005, 311 ff.

signaturfähigen Personalausweises durch eine groß angelegte Informationskampagne begleitet.

Die zwangsweise Einführung wie im estischen Modell führt naturgemäß zu einem großen Verbreitungsgrad signaturfähiger Chipkarten. Während in Estland bis Mitte Mai des Jahres 2005 760.000 neue Ausweise abgegeben wurden,[2571] erreichte beispielsweise Finnland bis zum November des Jahres 2004 lediglich die Ausgabe von 53.000 Karten. Dass das neue Format freiwillig gewählt und der alte Typ parallel weiter verwendet werden konnte, verhinderte eine größere Verbreitung.[2572]

Ein Zwangsmodell nach estischem Vorbild ist für Deutschland nicht geplant. Solange die qualifizierte Signaturfunktion eines digitalen Personalausweises oder einer elektronischen Gesundheitskarte allerdings freiwillig sind und Kosten verursachen, wird sich an dem grundlegenden Problem der Einführung der elektronischen Signatur nichts ändern:[2573] Wegen der Kosten (Signaturfunktion, Chipkartenleser, Software, jährliche Zertifikatsgebühren) müssten schon sehr attraktive Anwendungen vorhanden sein, um eine freiwillige Verbreitung der Signaturfunktion des Ausweises zu bewirken; ohne ein hinreichende Zahl von Signaturkarten am Markt gibt es jedoch keinen Anreiz für Wirtschaft und Verwaltung, entsprechende Anwendungen bereitzustellen. Staatliche Ausweise mit Signaturfunktion weisen eine Reihe von Vorteilen gegenüber anderen Signaturkarten auf.[2574] Sie werden jedoch ohne entsprechende Strategien auf der Anwendungsseite allein nicht zu einer allgemeinen Verbreitung der elektronischen Signatur führen.

Die Akzeptanz der Signaturfunktion eines konkreten Chipkartenausweises wird auch von den jeweiligen Zugangsmöglichkeiten und damit vom Ausgabemodell abhängen. Der Ausweisinhaber wird die Funktion umso eher annehmen, je geringer sein zeitlicher und finanzieller Aufwand ist. Konkret sollten die Prozesse für die Ausgabe des Ausweises und der Signaturfunktion unter Verbreitungsgesichtspunkten möglichst weitgehend miteinander verbunden werden.[2575] Das betrifft insbesondere die Registrierung, die Unterrichtung und die Ausgabe der sicheren Signaturerstellungseinheit. Demgegenüber dürfte der Verfahrensablauf zwischen Antragstellung und Ausgabe (also die Fragen der Funktionsteilung oder -zusammenführung bei Schlüsselerzeugung, Personalisierung, Zertifikatserstellung, Verzeichnis- und Sperrdienst) nachrangig sein, weil diese Prozesse für den Ausweisinhaber weder Erleichterungen noch Erschwernisse verursachen.

Neben den Hauptfaktoren der Kosten, der attraktiven Anwendungen und des Zugangs gibt es noch weitere Akzeptanzfaktoren für die Signaturfunktion. Diese wird nur eine weite Verbreitung finden, wenn eine einfache Handhabbarkeit gewährleistet ist, also keine größeren technischen Vorkenntnisse erforderlich sind. Allerdings erscheint es unwahrscheinlich, dass insbesondere ältere und/oder technisch ungeübte Mitbürger die Möglichkeiten zur Teilnahme am elektronischen Rechtsverkehr in nennenswertem Umfang nutzen werden. Dies entspricht jedoch der allgemeinen Situation bei der Einführung einer neuen Technik.

Ein wichtiger Faktor aus Akzeptanzsicht ist schließlich die Stärkung des Verbraucherschutzes durch die elektronische Signatur, Authentisierung und Verschlüsselung. Der

2571 Der jeweils aktuelle Stand ist unter http://www.id.ee/pages.php/0303 abrufbar; s. näher oben 3.2.1.2.
2572 S.a. oben 3.2.1.1.
2573 S.o. 2.1.1.
2574 S. näher oben 2.1.1.
2575 Zu den Möglichkeiten des Zusammenwirkens unterschiedlicher Instanzen im Rahmen von Zertifizierungsdiensten s.o. 5.2.2; speziell zu den Integrationsmöglichkeiten beim digitalen Personalausweis *Strasser/Müller/Roßnagel/Gitter*, in: Reichl/Roßnagel/Müller 2005, 260 ff., 268 ff.; *Gitter/Strasser*, DuD 2005, 74, 76 f.

Einsatz dieser technischen Verfahren wird die Zurechenbarkeit von Handlungen im Rechtsverkehr verbessern und damit einen Beitrag zu dessen Eindeutigkeit leisten. Soweit Bedenken gegen die Haftungsrisiken bestehen, die durch die elektronische Signatur hervorgerufen werden, kann dem über Mittel zur Risikominderung wie eine Beschränkung des qualifizierten Zertifikats[2576] entgegengewirkt werden.

Da nicht geplant ist, alle Zertifizierungsdienstleistungen durch den Staat zu erbringen, ist schließlich bedeutsam, ob eine Ausgabe von Signaturkarten unter Einbeziehung staatlicher Stellen von der Wirtschaft akzeptiert wird.[2577] Die Bündelung der Antrags- und Ausgabeverfahren bei Personalausweisbehörden oder Krankenkassen setzt eine Vereinheitlichung der Prozesse der Anbieter voraus. Daraus dürfte sich jedoch kein Ablehnungspotential ergeben, weil die Unterschiede in der Praxis nicht unüberwindlich sind. Auch verbleiben den bestehenden (und künftigen) Zertifizierungsdiensteanbietern substantielle Geschäftsfelder. Antrags- und Ausgabeverfahren werden schon bisher nur von den wenigsten Anbietern selbst erledigt, weil diese im Regelfall über keine flächendeckende Infrastruktur verfügen. Es macht dann aber keinen Unterschied, ob Antrag und Ausgabe über die Personalausweisbehörde oder etwa über die Post abgewickelt werden.

Ein staatlicher Ausweis mit Signaturfunktion stellt damit keine Konkurrenz für die bisherigen Zertifizierungsdiensteanbieter dar, weil diese in die Prozesse mit einbezogen werden. Dagegen besteht ein echter Wettbewerb mit den Signaturkarten der Banken, falls diese Karten nach der Änderung des Signaturgesetzes[2578] im reinen Online-Verfahren beantragt und ohne persönlichen Kontakt ausgegeben werden. Hier bleibt abzuwarten, ob die Banken tatsächlich in großem Umfang in den Signaturkartenmarkt einsteigen werden, und ob sich einer der beiden Verbreitungswege allein durchsetzen wird. Für die Bankenlösung spricht der vereinfachte Verteilungsprozess; indes verschafft die Sicherheit der persönlichen Identifikation durch die Personalausweisbehörde dem digitalen Personalausweis einen Vorteil für die Authentizität der mit ihm erstellen Signaturen.[2579]

7.3.3.3.2 Potentielle Veränderungen durch das JobCard-Verfahren

Die Einführung des JobCard-Verfahrens wird die Verbreitung elektronischer Signaturverfahren in Deutschland beschleunigen und damit auch deren Akzeptanz grundlegend beeinflussen. Zum einen wird entscheidend sein, ob die Bürger, die aufgrund des neuen Antragsverfahrens in der Arbeitslosenversicherung über eine Signaturkarte verfügen müssen, diese freiwillig auch für andere Anwendungen einsetzen werden. Zum anderen fragt sich, ob der Teil der Bevölkerung, der nicht vom JobCard-Verfahren erfasst ist, sich dennoch freiwillig eine Signaturkarte beschaffen wird.

Diese Entscheidungen der Bürger werden nach wie vor von der Bereitstellung attraktiver Anwendungen abhängen. Das JobCard-Verfahren ändert jedoch die Rahmenbedingungen für solche Anwendungen. Es ist zwar im Ausgangspunkt für die Akzeptanz der Signaturkarte problematisch, einen Großteil der Bevölkerung zu ihrem Besitz zu verpflichten. Der positive Effekt dieser zwangsweisen Verbreitung liegt aber darin, dass hierdurch der Anreiz zur Entwicklung von Anwendungen im Electronic Commerce und im Electronic Government massiv gesteigert wird.[2580] Wirtschaft und Verwaltung werden Gewissheit darüber haben, dass Millionen von Antragstellern in der gesetzlichen Arbeitslosenversiche-

2576 Dazu *Fischer-Dieskau/Gitter/Hornung*, MMR 2003, 384 ff.
2577 S. *Roßnagel/Hornung*, in: Reichl/Roßnagel/Müller 2005, 313 f.
2578 S.o. 5.1.2.
2579 S.o. 5.2.2.
2580 S. *Hornung/Roßnagel*, K&R 2004, 263, 265.

rung – und perspektivisch alle sozialversicherten Menschen in Deutschland – über eine Signaturkarte verfügen. Sollten die (bislang nicht verabschiedeten) gesetzlichen Grundlagen einen definitiven Starttermin nennen, hätten Entwickler und Integratoren sogar vor diesem Termin eine entsprechende Planungssicherheit. Da der weit überwiegende Teil der erwerbstätigen Bevölkerung in Deutschland die Signaturverfahren (bei Verfügbarkeit der sonstigen Infrastruktur, insbesondere eines Internetanschlusses)[2581] unmittelbar nutzen kann, wird aller Voraussicht nach eine enorme Steigerung der Anwendungsmöglichkeiten erfolgen.

Sind diese Anwendungen verfügbar, so werden die Nutzer des JobCard-Verfahrens die – dann ohnehin vorhandene – Signaturkarte auch ansonsten verwenden. Werden Signaturverfahren von vielen genutzt, vergrößert sich ihre Attraktivität auch für diejenigen Bürger, die nicht am JobCard-Verfahren teilnehmen. Die positiven Verbreitungseffekte des Verfahrens werden also in der gesamten Bevölkerung spürbar sein. Das gilt umso mehr, als aufgrund der großen Nachfrage nach Signaturanwendungskomponenten durch das JobCard-Verfahren erhebliche Kostendegressionseffekte gegenüber den derzeitigen Aufwendungen in Höhe von etwa 100 Euro für die Anschaffung von Signaturkarte, Kartenlesegerät und Software und etwa 40 Euro für die jährlichen Zertifikatsgebühren zu erwarten sind. Eine Überwälzung der Kosten für die Signaturkarte auf den Arbeitnehmer würde dennoch zu einer unausgewogenen Kostenverteilung innerhalb des Gesamtprojekts führen.[2582] Nicht nur aus verfassungsrechtlichen Gründen, sondern auch um die Akzeptanz des JobCard-Projekts zu stärken, sollten die Kosten nicht einseitig den Antragstellern auferlegt, sondern die Arbeitgeber in angemessenem Umfang beteiligt werden.

Ein potentielles Akzeptanzhindernis könnte sich ergeben, wenn einige Bürger aufgrund des JobCard-Verfahrens über eine Signaturkarte verfügen müssen, der Sicherheit des Signaturverfahrens jedoch grundsätzlich misstrauen und deshalb Haftungsrisiken befürchten. Für diesen Fall stellt das geltende Recht aber eine Ausweichmöglichkeit zur Verfügung. Nach § 7 Abs. 1 Nr. 7 SigG kann die Nutzung des Signaturschlüssels auf „bestimmte Anwendungen nach Art oder Umfang“ beschränkt werden. Hinsichtlich des Inhalts macht das Signaturgesetz keine Vorgaben.[2583] Deshalb ist auch eine Beschränkung der Nutzung auf den Datenabruf im Rahmen des JobCard-Verfahrens möglich.

Das Verhältnis des JobCard-Verfahrens zu signaturfähigen Chipkartenausweisen ist komplementär: Das Verfahren ist darauf angewiesen, dass diejenigen, die zum Besitz einer (beliebigen) Signaturkarte verpflichtet werden, auch die faktische Möglichkeit haben, diese zu erhalten. Wenn Signaturverfahren durch private Zertifizierungsdiensteanbieter sowohl auf dem digitalen Personalausweis (in Zusammenarbeit mit den Personalausweisbehörden) als auch auf anderen Karten (EC-Karten oder in vergleichbare Form) angeboten werden, stehen diese Lösungen miteinander in Konkurrenz. Daraus ergeben sich jedoch keine prinzipiellen Probleme. Die parallelen Verbreitungswege sind sogar positiv zu sehen. Eine ausschließliche Lösung mittels des digitalen Personalausweises hätte nämlich den Nachteil, dass alle durch das JobCard-Verfahren verpflichteten Bürger einen neuen Ausweis benötigen würden. Das könnte gerade in der ersten Phase der Einführung zu erheblichen Problemen führen.

2581 Aus den faktischen Bedingungen für den privaten Einsatz der Signaturkarte (insbesondere der Verfügbarkeit von PC und Internet-Anschluss) ergeben sich Einschränkungen für die erwartbare Verbreitung der Verfahren. Derzeit dürfte eine optimistische Schätzung etwa im Bereich von 5 Mio. potentiellen Nutzern liegen, s. *Roßnagel/Hornung*, in: Reichl/Roßnagel/Müller 2005, 313.

2582 *Hornung/Roßnagel*, K&R 2004, 263, 265 und oben 4.2.4.2.

2583 Näher *Fischer-Dieskau/Gitter/Hornung*, MMR 2003, 384, 385.

7.3.3.4 Faktoren aus der Zusammenführung mehrerer Funktionalitäten in einer Karte

Werden auf einem Chipkartenausweis mehrere Funktionalitäten vereint, so überlagern sich auch deren Akzeptanzeffekte.[2584] Das erschwert die Prognose. Wenn etwa der digitale Personalausweis oder die elektronische Gesundheitskarte die Möglichkeit zur elektronischen Signatur bieten, so könnte sich dies dann positiv auf ihre Gesamtakzeptanz auswirken, wenn in Zukunft mit der zunehmenden Verbreitung elektronischer Signaturverfahren die Nachfrage nach den Funktionen der Identifizierung, Authentisierung, Integrität, Verbindlichkeit und Vertraulichkeit steigt. Auf der anderen Seite ist die Vermittlung dieses Vorteils deshalb schwierig, weil Anwendungsmöglichkeiten für die neue Technik bislang noch nicht im nennenswerten Umfang bestehen. Ob die Aussicht auf eine lediglich zukünftige Verwendbarkeit die Akzeptanz des jeweiligen Chipkartenausweises in der Einführungsphase zu steigern vermag, erscheint unsicher.

Beim digitalen Personalausweis besteht allerdings umgekehrt die Möglichkeit, dass dieser der elektronischen Signatur zu Akzeptanzvorteilen verhelfen könnte, nämlich durch das höhere Vertrauen in die beteiligten staatlichen Stellen und durch eine verbesserte Identifizierungssicherheit.

Nach Umfragen werden elektronische Signaturverfahren dann leichter akzeptiert, wenn sie mit einem schon verbreiteten Trägermedium kombiniert werden.[2585] Der Personalausweis ist ein solches anerkanntes Medium. Staatlichen Institutionen wird in Deutschland außerdem mehr vertraut als privaten Zertifizierungsdiensteanbietern. Wo dies im Ausland ähnlich ist, wird dieser Effekt genutzt. In Hongkong werden die Zertifikate ausschließlich von der HK Post, einer staatlichen Behörde, ausgegeben.[2586] Als Grund dafür wird das höhere Vertrauen der Bürger in eine staatliche Zertifizierungsinstanz genannt. Dieser Aspekt überwog geäußerte Bedenken hinsichtlich einer unumkehrbaren Monopolbildung. In der Schweiz wird diskutiert, bestimmte Anwendungsbereiche wegen der höheren Sicherheit und des höheren Vertrauens einem staatlichen Zertifikat vorzubehalten. Dazu gehören etwa E-Voting, elektronischer Strafregisterauszug oder Geschäfte, die für das organisierte Verbrechen von Interesse sind.

Für die Identifizierungssicherheit ist wesentlich, dass die Befugnisse der Personalausweisbehörden zur Identifizierung eines Antragstellers erheblich weiter reichen als die Möglichkeiten der Zertifizierungsdiensteanbieter nach § 3 Abs. 1 SigV.[2587] Diese Zuverlässigkeit der Identifizierung kann sich positiv auf die Akzeptanz der elektronischen Signatur auswirken, weil eine höhere Verbindlichkeit der signierten Erklärung und damit eine verstärkte Rechtssicherheit erreicht werden.

7.4 Die Beeinflussbarkeit der Akzeptanz durch den Staat

Sowohl die Betrachtung der allgemeinen Akzeptanzfaktoren als auch die Analyse der konkreten Chipkartenausweise machen deutlich, dass Staat und Regierung in einigen Bereichen direkten oder indirekten Einfluss auf das Akzeptanzverhalten in der Bevölkerung nehmen können. Es lassen sich drei Bereiche unterscheiden. Zunächst richtet sich die Akzeptanz einer Maßnahme notwendigerweise nach ihrem Inhalt, der bei den hier behandelten Ausweisen letztlich durch den Staat bestimmt wird. Dann ist die Art und Weise des

2584 Vgl. zum Folgenden (für den digitalen Personalausweis) *Roßnagel/Hornung*, in: Reichl/Roßnagel/Müller 2005, 314 f.

2585 S. *Strasser/Müller/Roßnagel/Gitter*, in: Reichl/Roßnagel/Müller 2005, 266 m.w.N.

2586 S. zum dortigen Modell oben 3.2.2.3.

2587 Vgl. ausführlich oben 5.2.2.

Zustandekommens der Entscheidung von Einfluss. Schließlich gibt es Möglichkeiten im Bereich von Aufklärung und Werbung.

Für die inhaltliche Seite einer Maßnahme sind allgemeine Aussagen – jenseits der oben genannten Faktoren der Rationalität, Flexibilität und egalisierenden Wirkung staatlichen Handelns und der Berücksichtigung sozialer Gerechtigkeit[2588] – kaum möglich. Es ist vielmehr eine Betrachtung des jeweiligen Kontextes und der Auswirkungen der einzelnen Entscheidung erforderlich, die beispielsweise für Chipkartenausweise die Bedeutung einer datenschutzfreundlichen technischen Ausgestaltung nahelegt. Bei Maßnahmen im grundrechtsrelevanten Bereich kann ein Verzicht auf eine verfassungsrechtlich gerade noch zulässige Lösung deswegen akzeptanzfördernd sein, weil damit deutlich wird, dass der Staat Sicherheits- und Freiheitsinteressen gegeneinander abgewogen hat.

Das Verfahren im Vorfeld einer Entscheidung ist regelmäßig rechtlich festgelegt. Das bedeutet jedoch nicht, dass keine Möglichkeiten für eine akzeptanzfreundliche Ausgestaltung bestünden. Betrachtet man etwa die Regeln des parlamentarischen Gesetzgebungsverfahrens, so bilden diese zwar insgesamt einen unverrückbaren Rahmen. Sie lassen aber durchaus Spielräume zu, etwa hinsichtlich der Beteiligung von Verbänden, aber auch des Auftretens der Abgeordneten innerhalb und außerhalb des Parlaments. Wenn Teile des Gesamtprozesses nicht rechtlich geregelt sind, ergeben sich weitere Möglichkeiten für eine Akzeptanzförderung. Das trifft regelmäßig auf große und durchaus für das Ergebnis wichtige Verfahrensschritte zu, etwa die rechtspolitische Diskussionen in den Medien und die Entscheidungsfindungsprozesse in den politischen Parteien.

Auch Information und Werbung können auf die Akzeptanz einer Maßnahme großen Einfluss ausüben.[2589] Beide Kategorien lassen sich oft schwer voneinander abgrenzen. Theoretisch unterscheiden sie sich darin, dass Information auf die Vermittlung von Tatsachen beschränkt ist, während Werbung darüber hinaus auch an Gefühl und persönliche Wertung appelliert oder auf die Identifikation mit Personen oder Sachen abzielt.[2590]

Die genaue Erläuterung technischer Neuerungen wie Chipkartenausweisen ist vor allem für Bevölkerungsgruppen wichtig, die – wie zum Beispiel ältere und/oder technisch ungeübte Menschen – mit ihnen erfahrungsgemäß ohnehin Schwierigkeiten haben. Eine Informationsoffensive könnte etwa die Vermittlung der Funktionen der elektronischen Signatur, die Erläuterung der auf oder durch die Karte gespeicherten Daten hinsichtlich Inhalt, Zugriffsberechtigungen und Sicherheit und die Beschreibung der allgemeinen Handhabung des Ausweises im Alltag sowie der Auskunfts- und sonstigen Schutzrechte des Inhabers beinhalten.[2591] Die Aufklärung muss zu einem möglichst frühen Zeitpunkt erfolgen. Andernfalls stehen größere Zeitverluste zu erwarten, weil verspätete Informationen nicht zu weniger, sondern zu mehr öffentlichen Protesten führen.[2592]

Diese Maßnahmen können insbesondere helfen, irrationale Befürchtungen abzubauen, die durch mangelnde Information über die tatsächliche Funktionsweise und Risiken eines Chipkartenausweises entstehen. Bestehende Vorbehalte dürfen allerdings nicht vorschnell

---

2588 S.o. 7.3.1.1.

2589 *Hill*, JZ 1988, 377, 380; *ders*., DÖV 1988, 666, 667; *Jentsch*, JZ 1995, 9 ff.; *Würtenberger*, NJW 1991, 257; *ders*., Sonderheft 39/1999 der KZfSS, 380, 394.

2590 Werbung kann definiert werden als „Sammelbegriff für alle Maßnahmen, die auf planmäßige Beeinflussung von Mitmenschen abgestellt sind, um ein freiwilliges Befolgen politischer, wirtschaftlicher, sozialer, religiöser, kultureller u.s.w. Tendenzen zu erreichen“, vgl. *Pelzer* 1961, 881. Dazu gehört insbesondere das Ansprechen der emotionalen Ebene (*Hemmi* 1994, 36).

2591 Eine Reihe dieser Informationen ist bereits durch rechtliche Regelungen (insbesondere § 6c BDSG und Verweisungsnormen wie § 291a Abs. 2 Satz 2 und Abs. 3 Satz 5 SGB V) erforderlich. Diese Verpflichtungen greifen aber erst bei der Ausgabe einer konkreten Karte.

2592 *Würtenberger*, NJW 1991, 257, 260.

als irrational abgetan werden. Dies hieße, Ängste in der Bevölkerung nicht ernst zu nehmen. Werden Aufklärungsakte in ein umfassendes „Akzeptanzmanagement“ eingebunden, das darüber hinaus Elemente parlamentarischer Konfliktschlichtung, offensiver Öffentlichkeitsarbeit der Verwaltung, und – sofern anwendbar – Konfliktschlichtung im Verwaltungsverfahren beinhaltet,[2593] so ergeben sich aus Sicht des Staates Vorteile auch deswegen, weil gerichtliche Nachverfahren auf verfassungs- und verwaltungsrechtlicher Ebene vermieden werden. Dies setzt allerdings voraus, dass auch die Gesichtspunkte offen gelegt werden, die gegen ein konkretes Projekt sprechen. Erforderlich ist der Transport der „sozialen Evidenz und alltagsweltlichen Plausibilität“[2594] einer Maßnahme, was durch eine Popularisierung der Kosten-Nutzen-Analyse, durch vergleichende Risikobewertungen oder durch die Implementierung von Sicherheitsmaßnahmen geschehen kann.

Jenseits dieser pragmatischen Fragen stellt sich das grundsätzliche Problem, inwieweit dem Einfluss des Staates auf die gesellschaftliche Akzeptanz einer Entscheidung tatsächliche und rechtliche Grenzen gesetzt sind. Zunächst dürfen staatliche Aktionen nicht auf Verharmlosung von Risiken und Unterdrückung von zweifelnden Stimmen gerichtet sein. Ein solches Verhalten wäre auch potentiell hochgradig kontraproduktiv. Denn sollten derartige politische Taktiken öffentlich werden, ist mit einem massiven Vertrauensverlust in die handelnden Akteure, aber auch in das Akzeptanzobjekt zu rechnen. Dieser Effekt kann irreparabel sein und auch zur Ablehnung einer Entscheidung führen, die an sich mehrheitlich hätte akzeptiert werden können. Außerdem darf es nicht Ziel einer demokratischen Regierung sein, berechtigte Zweifel an Sinn und Rechtmäßigkeit einer Maßnahme in der Bevölkerung beiseite zu schieben und mit dieser Methode gesellschaftliche Mehrheiten zu produzieren. Im demokratischen Rechtsstaat ist die Staatsfreiheit des politischen Willensbildungsprozesses ein hohes Gut.[2595] Anders ausgedrückt: Akzeptanz kann auch die Akzeptanz des Staates selbst oder seiner Regierenden sein, nämlich hinzunehmen, dass das Volk ein Gesetz oder eine Maßnahme nicht will.

In der Literatur finden sich Stimmen, die für eine stärker werbende Rolle des Staates plädieren. Gefragt sei vor allen Dingen ein so genanntes „Gesetzes-Marketing“; der Gesetzgeber müsse sein Produkt „verkaufen“.[2596] Es sei Aufgabe des Staates, für den Rechtsstaat zu werben,[2597] und das Werben für oberste Rechtsprinzipien des Grundgesetzes könne sogar verfassungsrechtlich geboten sein.[2598]

Dieser Gedanke ist dann zutreffend, wenn hierunter der Einsatz des Staates für die Vermittlung der Wichtigkeit von Grundrechten, fundamentalen demokratischen Prinzipien oder Toleranzgedanken verstanden wird. Das Werben für eine spezifische Maßnahme ist davon aber nicht gedeckt. Ein nicht akzeptables Verständnis des Verhältnisses zwischen Staat und Bürgern wird schließlich postuliert, wenn als Autorität für ein offensives Vorgehen des Staates im Akzeptanzbereich ein Zitat des Kameralisten *Justi* angeführt wird, demzufolge „die wahre Staatskunst…dahin gerichtet sein [muss], die Untertanen von der Güte der Gesetze zu überzeugen“.[2599] Diese Bemerkung ist sogar umgekehrt ein Argument gegen werbende Maßnahmen des modernen Staates. Denn im Unterschied zum Untertanen *Justis* hat der mündige Bürger des demokratischen Rechtsstaats sowohl an der Legitimation der Staatsgewalt als auch am politischen Willensbildungsprozess teil. Deshalb ist es

2593 *Würtenberger*, NJW 1991, 257, 259.
2594 *Würtenberger*, NJW 1991, 257, 260.
2595 *Czybulka*, Die Verwaltung 1993, 27, 32, 34.
2596 *Hill*, JZ 1988, 377, 380; *ders*., DÖV 1988, 666, 667.
2597 *Jentsch*, JZ 1995, 9 ff.
2598 *Würtenberger*, Sonderheft 39/1999 der KZfSS, 380, 394.
2599 *Würtenberger* 1987, 84 (vgl. *Justi* 1771, 367).

unter der Geltung des Demokratieprinzips unzulässig, Methoden absolutistischer Staatsaufklärung zur Legitimation einer staatlichen Tätigkeit zu verwenden, die auf die Herstellung von Akzeptanz gerichtet ist. Ziel muss es umgekehrt sein, eine Maßnahme mit dem Ziel von mehr Akzeptanz zu optimieren.[2600] Damit bekommt diese Maßnahme selbst eine neue Qualität, weil es nicht mehr nur um das Marketing für eine bereits getroffene Entscheidung geht, sondern um die Verbesserung von Verfahren und Inhalt der Maßnahme.

Im Rahmen dieses Prozesses kann die Schaffung ergebnisoffener Meinungsbildungsverfahren, und so paradoxerweise gerade der Verzicht auf werbenden Einfluss auf die Bevölkerung, die Akzeptanz einer Entscheidung erhöhen, weil hierdurch die Einflusswege zwischen Regierung und Bürgern zugunsten einer aktiven Rolle der letzteren umgekehrt werden. Damit ist die Ausgangsfrage möglicherweise falsch gestellt: Unter demokratie- und legitimationstheoretischen Überlegungen kann es nicht um den Einfluss des Staates auf die öffentliche Meinung gehen. Vielmehr ist umgekehrt nach deren Einfluss auf die politische Entscheidung über eine Maßnahme wie die Einführung biometrischer Identifikationssysteme oder von Telematik im Gesundheitswesen zu fragen. Der Einsatz mediativer Prozesse kann deshalb im Ergebnis nicht nur die Implementierung der Projekte entscheidend befördern, sondern auch zu einer Stärkung partizipativer Elemente des demokratischen Entscheidungsprozesses beitragen.

2600 *Hoffmann-Riem*, AöR 1990, 400, 415 f.

8 Schlussbemerkungen

„Wenn die Visionen einiger Informatiker richtig sind, dann wird eine kleine Plastikkarte im Scheckkartenformat unser tägliches Leben grundlegend verändern."[2601] Diese Einschätzung von *Münch* datiert aus dem Jahre 1992. Dreizehn Jahre später füllen kleine Plastikkarten im Scheckkartenformat – zumindest in den Industrienationen – die Portemonnaies der Bürger. Eine grundlegende Veränderung des Alltags kann jede einzelne von ihnen kaum für sich in Anspruch nehmen – wohl jedoch ihre Gesamtheit, was sich bereits an den Unannehmlichkeiten zeigt, die beim Verlust einer Geldbörse mit sämtlichen Chip- und sonstigen Karten einer Person eintreten.

Chipkartenausweise mit leistungsfähigen Mikroprozessoren erzeugen eine neue Qualität dieser Entwicklung, verändern und erweitern bestehende Identifizierungsverfahren und wirken damit potentiell auch auf die Identität der Ausweisträger zurück.[2602] Durch die Erweiterung der Datenmenge, die auf ihnen gespeichert werden kann, und durch die Neuartigkeit der Anwendungen, die sie unterstützen oder erst ermöglichen, beeinflussen sie die Interaktionsprozesse zwischen den Inhabern der Karten und den Instanzen, die ihnen gegenübertreten. Grenzkontrollbeamte, Leistungserbringer im Gesundheitswesen, Mitarbeiter der Arbeitslosenverwaltung und ähnliche Stellen begegnen den Karteninhabern zwar immer noch unmittelbar physisch, sie stützen ihre Handlungen jedoch zumindest partiell auf automatisierte technische Prozesse. Das ist per se kein Nachteil, mit Blick auf die grundrechtlich garantierte autonome Identitätsbildung jedoch eine Entwicklung, die ambivalent zugleich Chancen und Risiken mit sich bringt.

Einerseits ist deutlich geworden, welche Vorteile sich durch eine höhere Identifizierungssicherheit, eine Erleichterung elektronischer Geschäfts- und Verwaltungsprozesse und eine Rationalisierung und damit verbundene Kosteneinsparung (die letztlich allen Beteiligten zugute kommt) ergeben. Gerade im Gesundheitswesen bietet die Verwendung leistungsfähiger Multiapplikationschipkarten enormen Chancen zur Verbesserung der Versorgung und Vorsorge.

Andererseits muss man sich klarmachen, dass die technische Erweiterung von Identifizierungsprozessen zum Teil erhebliche Risiken für die informationelle Selbstbestimmung der Karteninhaber hervorruft, denen adäquat zu begegnen ist. Wenn die Abhandlung sich vor allem mit diesen Risiken beschäftigt hat, so darf dies nicht als einseitige Kritik oder gar Ignoranz gegenüber den Potentialen der Technik missverstanden werden. Diesem Ansatz liegt vielmehr die Erkenntnis zugrunde, dass es zur datenschutzgerechten Ausgestaltung risikobehafteter Technologien keine Alternative gibt, die Berücksichtigung entsprechender Gestaltungsoptionen in der Entwicklungs- und Implementierungsphase jedoch bisweilen zu kurz kommt.

Die Untersuchung hat gezeigt, dass die Einführung von Chipkartenausweisen im Spannungsfeld von rechtlicher, technischer, wirtschaftlicher und politischer Machbarkeit zu verorten ist. Mit Blick auf die in der Einleitung dargelegten Wechselbeziehungen zwischen Identität und Identifizierung lassen sich im Ergebnis hauptsächlich drei Punkte festhalten:

- Erstens können die allgemeinen rechtsstaatlichen Anforderungen des Gesetzesvorbehalts und der Bestimmtheit der Ermächtigungsgrundlage ebenso wie die Ausprägungen des informationellen Selbstbestimmungsrechts (Verhältnismäßigkeit, Zweckbindung, informationelle Gewaltenteilung, Transparenz, Verbot der Profil-

2601 *Münch*, GMD-Spiegel 1/92, 4.

2602 Vgl. zum grundlegenden Zusammenhang zwischen Identität und Identifizierung oben 1.

bildung, staatliche Schutzpflichten) auf die Besonderheiten der jeweiligen Chipkartenausweise hin konkretisiert werden.

- Nur wenn – zweitens – diese rechtlichen Anforderungen in der derzeitigen Phase der Weichenstellungen im technischen Bereich berücksichtigt werden, erscheinen die Risiken für die Identitätsbildung des Einzelnen und für die Gesellschaft beherrschbar. Unter dieser Voraussetzung könnten sich Chipkartenausweise in dem Konflikt zwischen ihrer Verwendbarkeit als „Schild des Bürgers zur Bewahrung, ja möglichen Herstellung seiner Anonymität" und als „Instrument der Herrschenden"[2603] tatsächlich als Mittel zum Schutz informationeller Selbstbestimmung erweisen.
- Drittens ist die Minimierung der jeweiligen Grundrechtseingriffe im allseitigen Interesse. Mit ihr wird nicht nur die Identität des Einzelnen geschützt und verfassungsrechtlichen Anforderungen genügt, sondern auch die Akzeptanz der jeweiligen Projekte befördert, die Voraussetzung einer effektiven Umsetzung und ohne den wirksamen Schutz sensibler personenbezogener Daten nicht denkbar ist.

Bei allen berechtigten Hoffnungen in die Chancen der Chipkartentechnologie ist schließlich die Warnung erforderlich, dass diese – wie andere technische Neuerungen – kein Allheilmittel für die Probleme und Schwierigkeiten des Lebensbereiches sein kann, in dem sie eingesetzt wird. Der behandelnde Arzt wird weiterhin die auf oder mittels der elektronischen Gesundheitskarte übermittelten Daten auf ihre inhaltliche Plausibilität und Vollständigkeit hin überprüfen und bei Zweifeln die Daten neu erheben müssen. Grundsätzlich wird der Einsatz von Informationstechnologie nicht alle strukturellen Probleme im Gesundheitswesen (wie die Misallokation öffentlicher Gelder, die Ungleichheit im Leistungszugriff, die Ineffektivität bei der Leistungserstellung und die explodierenden Kosten durch den technischen Fortschritt)[2604] lösen.

Auch der digitale Personalausweis stellt keine Lösung für die Probleme des internationalen Terrorismus und der grenzüberschreitenden Kriminalität dar. Da mit ihm lediglich in einer bestimmten Kontrollsituation die Zugehörigkeit eines Identitätspapiers zu einer Person bestätigt wird, verbleiben gravierende Probleme. Personen mit kriminellen Absichten vermeiden naturgemäß nach Möglichkeit Kontrollen. Ein erheblicher Schwachpunkt ist der Enrolmentsprozess. Werden durch Bestechung oder Erpressung falsche Daten in das Herstellungsverfahren eingeschleust, so produziert dieses Originaldokumente, die Namen und biometrische Daten enthalten, welche tatsächlich nicht zusammengehören. Für die kontrollierenden Instanzen gibt es dann keinerlei Möglichkeit mehr, dies zu erkennen. Es dürfte aufgrund der „offiziell bestätigten" biometrischen Daten sogar erheblich schwerer als heute sein, die Fälschung nachzuweisen. Schließlich ist es nicht möglich, von der Identität einer Person auf ihre Absichten und Ziele zu schließen. Die Anschläge des 11. September 2001 mögen der Anlass für die massiven Anstrengungen zur Implementierung biometrischer Daten in Reisedokumente gewesen sein; eine Rechtfertigung bieten sie zumindest insofern nicht, als die Existenz derartiger Dokumente zu ihrer Verhinderung wenig beigetragen hätte: Die Attentäter reisten – zumindest überwiegend[2605] – unter ihren wahren Namen und

2603 *Dethloff* 1992, 3 (zitiert nach *Elkeles/Rosenbrock* 1995, 1); s. zu diesem Grundkonflikt oben 1.

2604 *BSI* 1995, 12 f.; s.a. *Grätzel v. Grätz* 2004c, 8 f.

2605 Die Angaben zu der Zahl der Terroristen, die mit echten Pässen reisten, sind widersprüchlich; s. einerseits *Towler*, Law Society Gazette 2004, No. 17, 20 (neun), andererseits *Burchardt*, FR vom 2.12.2004 (alle Attentäter).

begingen am Tag der Anschläge keine Identitätstäuschungen oder Passfälschungen.[2606] Reisepapiere mit biometrischen Daten bieten so gut wie keine Unterstützung für die Terrorismusbekämpfung, solange die staatlichen Behörden nicht wissen, wer die Terroristen sind.[2607] Selbstmordattentäter haben keine Vergangenheit, zumindest keine, die in staatlichen Dateien gespeichert ist: Ihr erster Terroranschlag ist zugleich ihr letzter. Gegen dieses Problem bieten weder biometrische Systeme noch jede andere Form von Identitätskontrollen Schutz.

Die Einschätzung der Verwendungspotentiale von Chipkartenausweisen darf also nicht durch eine übertriebene Technikgläubigkeit bestimmt werden. Die sozialen und wirtschaftlichen Chancen und Risiken der Kartentechnologie für die Gesellschaft insgesamt und ihre Folgewirkungen auf den Einzelnen und seine Identität müssen vielmehr realistisch erfasst und abgeschätzt werden. Dies setzt einen Diskurs unter den mit künftigen Chipkartenausweisen befassten Wissenschaftlern und Praktikern, aber auch in Politik und Öffentlichkeit voraus. Aus grundrechtlicher Sicht mag es letztlich mehrere verfassungsmäßige (wenn auch unterschiedlich verfassungsverträgliche)[2608] technische und organisatorische Lösungen geben; echte demokratische Legitimation wird jede einzelne von ihnen nur nach einem derartigen Diskurs beanspruchen können.

Die rechtlichen, technischen, wirtschaftlichen und politischen Rahmenbedingungen für die Einführung von Chipkartenausweisen sind abgesteckt. Dagegen ist die Fortentwicklung in allen diesen Bereichen noch offen und wenig festgelegt. An die Wissenschaft stellt sich deshalb die Herausforderung der Begleitung, Analyse und Systematisierung. Die vorliegende Arbeit hofft, dazu einen Beitrag geleistet zu haben.

2606 Das wird gerade in der US-amerikanischen Diskussion häufig ignoriert, z.B. von *Woodward/Orlans/Higgins* 2003, 354 f.; *Eaton* (2003) widmet sein Buch *Theodore Martin Hesburgh* mit den Worten „September 11, 2001 might never have happened had this advocacy of biometric ID documents been supported". Angesichts des Fehlens von Identitätstäuschungen seitens der Terroristen ist das schwer nachvollziehbar. Ein mittelbarer Effekt kann sich allerdings insoweit ergeben, als bei Vorbereitungshandlungen derartige Täuschungen wahrscheinlicher sind und durch Identitätsdokumente mit biometrischen Daten erschwert werden könnten.

2607 *Hadley*, EMBO reports 2004, 124, 126.

2608 S. zu dieser Unterscheidung oben 2.5.

9 Handlungsleitende Thesen

Die folgenden Thesen verstehen sich nicht als eine Zusammenfassung aller Resultate der Arbeit. Vielmehr geht es – unter beabsichtigter Ausblendung mehr theoretischer Ergebnisse – darum, die unmittelbar praktischen Konsequenzen für den weiteren Prozess der Gesetzgebung und technischen Fortentwicklung zusammenhängend darzustellen.

9.1 Der digitale Personalausweis

- Die verfassungsrechtliche Eignung der Biometrie für die Anwendung auf eine Bevölkerung von 80 Millionen Bürgern ist bislang nicht nachgewiesen. Es fehlt insbesondere an Tests mit einer repräsentativen, untrainierten Stichprobe aus der Gesamtbevölkerung.[2609] Problematisch ist außerdem, dass mit der Gesichtserkennung dasjenige Verfahren eingeführt wird, welches unter den drei in Erwägung gezogenen (Gesicht, Fingerabdruck, Iris) die höchsten Fehlerraten aufweist.[2610]
- Wegen der grundsätzlich unlöslichen lebenslangen Bindung der biometrischen Daten an eine Person besteht in erhöhtem Maße das Risiko einer Verwendung als allgemeines Personenkennzeichen. Es ist deshalb durch technische und organisatorische Maßnahmen sicherzustellen, dass kein Einsatz zur Datensammlung und Profilbildung erfolgt.
- Nach geltendem Recht ist eine Speicherung biometrischer Ausweisdaten außerhalb des Personalausweises – mit Ausnahme des Gesichtsbildes im Personalausweisregister – unzulässig.[2611] Dieses Verbot ist nicht nur einfachgesetzlich, sondern auch verfassungsrechtlich begründet.
- Der missverständliche Wortlaut von § 3 Abs. 5 PersAuswG (Zweckbestimmung der „verschlüsselten Merkmale und Angaben“ zur Echtheits- und Identitätsprüfung; Auskunftsanspruch des Inhabers) ist verfassungskonform so auszulegen, dass er sämtliche biometrischen Daten des Personalausweises erfasst.
- Auf der Erforderlichkeitsebene weisen alle drei biometrischen Merkmale spezifische Risiken auf. Im Ergebnis ist die Iriserkennung (leicht) vorzugswürdig, weil sie nicht unmerklich durchgeführt werden kann und die Iris keine Spuren in der Umgebung hinterlässt.
- Die Verwendung von Templates ist gegenüber Volldatensätzen ein milderes Mittel. Wenn Templates wegen mangelnder Interoperabilität nicht zum Einsatz in Reisedokumenten geeignet sind, muss der Staat sich für eine Standardisierung einsetzen.
- Wenn Matching-On-Card aus Sicherheitsgründen nicht eingesetzt wird, sind Kontrolleinheiten zu verwenden, die schon rein technisch keine dauerhafte Speicherung

2609 Sollte der digitale Personalausweis erst 2007 eingeführt werden, verbliebe noch genügend Zeit. Problematisch ist aber, dass der enge Zeitplan der Bundesregierung für die Erweiterung des Reisepasses (diese ist für den Herbst 2005 geplant, s. die Antwort auf die Kleinen Anfrage der FDP-Fraktion im Januar 2005, BT-Drs. 15/4616, 5 f.) praktisch keine Möglichkeit für größere Feldtests mehr lässt. Der Bundesbeauftragte für den Datenschutz, *Schaar*, forderte deshalb im April 2005 ein Moratorium bis zum Sommer des darauffolgenden Jahres, s. http://www.heise.de/newsticker/meldung/58735.

2610 Daraus allein folgt allerdings noch nicht die verfassungsrechtliche Unzulässigkeit, weil Faktoren wie internationale Interoperabilität, hohe Kosten, patentrechtliche Situation (Probleme der Iriserkennung) und organisatorische Fragestellungen auch die verfassungsrechtliche Bewertung beeinflussen.

2611 Das gilt im Übrigen auch für den Reisepass, weil die Verordnung (EG) Nr. 2252 v. 13.12.2004 (dazu *Roßnagel/Hornung*, DÖV 2005, i.E. und oben 3.1.2) keine Regelung für nationale Register enthält.

oder anderweitige Übermittlung der vom Sensor kommenden (Roh-)Daten zulassen.

- Biometrische Daten können „besondere Arten personenbezogener Daten“ (§ 3 Abs. 9 BDSG) sein; beim Bezug zu Krankheiten genügt hierzu ein hinreichend hoher statistischer Zusammenhang. Die Regelungen des Bundesdatenschutzgesetzes zu Daten nach § 3 Abs. 9 BDSG werden aber gegenüber einer noch zu schaffenden Bestimmung des Personalausweisrechts subsidiär sein.
- Für Bürger, die temporär oder dauerhaft nicht zur biometrischen Authentifikation geeignet sind, sind effektive und diskriminierungsfreie Rückfallsysteme vorzuhalten.
- § 6a BDSG ist nicht auf biometrische Systeme anwendbar. Wegen der nie auszuschließenden Gefahr einer fehlerhaften Zurückweisung darf dennoch aus verfassungsrechtlichen Gründen keine absolut automatisierte Kontrolle stattfinden.
- Je nach technischer Ausgestaltung werden § 6c BDSG oder verwandte Transparenzvorschriften der Landesdatenschutzgesetze auf den digitalen Personalausweis anwendbar sein. Das das Landesrecht erheblich differiert, ist für den Ausweis eine selbständige Regelung oder – wie für die Gesundheitskarte geschehen – eine Verweisungsnorm zu schaffen. Bei einer Verweisung müsste die Personalausweisbehörde eine Unterrichtung in Textform durchführen und die technische Infrastruktur für die Umsetzung der datenschutzrechtlichen Auskunft vorhalten.
- Nach geltendem Recht ist die Nutzung der biometrischen Daten des digitalen Personalausweises im privaten Bereich unzulässig. De lege ferenda könnte dies geändert werden, wenn der Ausweisinhaber einwilligt, die Freiwilligkeit der Einwilligung gesichert ist und diese technisch überprüft wird.
- Die Integrität der gespeicherten Ausweisdaten ist durch eine elektronische Signatur zu sichern, die (zur sicheren Verbindung mit dem Ausweis) auch die sichtbar gespeicherten Daten umfasst.
- Zum Schutz der Vertraulichkeit der Daten sind technische Sicherungsmechanismen zu implementieren. Die Berechtigung des Lesegeräts ist durch einen Authentisierungs- und/oder Verschlüsselungsmechanismus zu gewährleisten. Das gilt insbesondere bei der Verwendung kontaktloser (RF-)Schnittstellen, die ansonsten dem Transparenzprinzip widerspricht. Eine symmetrische Verschlüsselung bietet zwar wegen des Kompromittierungsrisikos keinen absoluten Schutz, verhindert aber zumindest die jederzeitige Auslesbarkeit.
- Ein digitaler Personalausweis als sichere Signaturerstellungseinheit weist eine Reihe von Vorteilen auf. Es handelt sich um ein allgemein verbreitetes, akzeptiertes Medium und die Personalausweisbehörde könnte standardmäßig einen „elektronischen Personalausweis“ ausstellen. Außerdem garantieren der unmittelbare Kontakt mit den geübten Mitarbeitern der Behörde und deren Befugnisse, die bis zur erkennungsdienstlichen Behandlung reichen, ein Höchstmaß an Identifikationssicherheit.
- Identifikations- und Signaturfunktion des Personalausweises sind technisch vollständig zu trennen. Ist der Ausweis nicht mehr zur Identifikation gültig, können weiterhin rechtsverbindliche Signaturen erstellt werden; wenn der Ausweis zurückgegeben werden muss, sind die Karte oder der Signaturschlüssel nachweisbar zu vernichten. Beim Ablauf des Zertifikats kann dieses – so der Schlüssel noch sicher ist – erneuert werden; die Identifikationsfunktion wird nicht beeinträchtigt. Im Fall der Unsicherheit der eingesetzten Algorithmen und zugehörigen Parameter werden

der Signaturschlüssel und die signierten Ausweisdaten unverwendbar, sodass der Ausweis ausgetauscht werden muss; ein Einsatz als Sichtausweis bleibt unberührt.

- Es ist signatur- und datenschutzrechtlich grundsätzlich für die Personalausweisbehörde zulässig, Antrags-, Unterrichtungs- und Ausgabeprozesse für private Zertifizierungsdiensteanbieter zu übernehmen. Um jedoch die Probleme der individuellen Überwachungsbefugnisse im Rahmen der Auftragsdatenverarbeitung und Zertifikatsvergabe zu vermeiden, sind die Aufgabe der Behörde, ihre Befugnis zur Datenübermittlung und zu treffende Sicherheitsmaßnahmen gesetzlich zu regeln.
- Mit dem Konzept eines „elektronischen Ausweises" gibt es ein Verfahren zur sicheren und datenschutzgerechten Identifizierung des Bürgers auch bei einem Erstkontakt mit einer Behörde. Das Verfahren könnte auch auf normalen Signaturkarten implementiert werden; eine Kombination mit dem digitalen Personalausweis weist jedoch organisatorische Vorteile auf.
- Auf die Personalausweisbehörden kommt ein erheblicher organisatorischer Aufwand zu. Jede Zweigstelle, die Ausweise ausgibt (die genaue Zahl dieser Stellen ist unklar, sie liegt aber erheblich höher als die Zahl der 6.500 Behörden), benötigt unabhängig vom Herstellungsprozess biometrische Erfassungsgeräte, weil die Funktionsfähigkeit und Zuordnung des Ausweises vor der Ausgabe geprüft werden muss.
- Die Kosten des Gesamtprojekts sind derzeit noch nicht abschätzbar. Sie werden maßgeblich durch die technische Ausgestaltung und die Zahl der Ausgabe- und Kontrollstellen bestimmt. Die Kosten der Signaturfunktion dürften gegenüber der Biometrie weniger bedeutsam sein. Eine Verkürzung der Laufzeit auf fünf Jahre – wie von der ICAO vorgeschlagen – könnte alle anderen Kostenfaktoren entscheidend überlagern.
- Die Erfahrungen digitaler Ausweisprojekte im Ausland und die Analysen der Volkszählung und der Einführung des maschinenlesbaren Personalausweises lassen darauf schließen, dass die Akzeptanz des digitalen Personalausweises entscheidend von einer effektiven Umsetzung datenschutzrechtlicher Anforderungen und einem transparenten Entscheidungsprozess abhängen wird.

9.2 Die elektronische Gesundheitskarte

- Die verpflichtende Verwendung der Gesundheitskarte zur Übermittlung der Stammdaten und des elektronischen Rezepts ist zulässig. Bei spezifischen Programmen (beispielsweise für chronisch Kranke) kann eine Vorlage bei allen Behandlungen vereinbart werden. Die obligatorische Offenbarung einer elektronischen Patientenakte bei jedem Arztbesuch wäre dagegen mit der Patientenautonomie unvereinbar.
- Wenn eine sichere Ende-zu-Ende-Verschlüsselung unter Verwendung des öffentlichen Schlüssels der Gesundheitskarte eingesetzt wird, sind sowohl die Speicherung und Übermittlung auf der Karte selbst als auch die auf Servern akzeptabel. Auf eine zentrale Speicherung aller Daten der Versicherten ist jedoch zu verzichten. Der Transport in einem geschützten Speicherbereich der Karte hat für den Inhaber den Vorteil, dass er nicht auf die Sicherheit der Serverinfrastruktur und die Zuverlässigkeit ihrer Betreiber vertrauen muss. Aus speichertechnischen und funktionalen Gründen wird aber für die meisten Anwendungen die Ablage auf der Karte ausscheiden.
- Wenn die Daten auf externen Servern so verschlüsselt werden, dass ein Zugriff ausschließlich unter Verwendung der Gesundheitskarte möglich ist, so stellt sich

das Problem der Abgrenzung zwischen Datenverarbeitung im Auftrag und Funktionsübertragung nicht. Sind die Daten auf Servern dagegen personenbeziehbar, so liegt im Betrieb der Serverarchitektur eine Funktionsübertragung und in der Weitergabe der Daten eine Übermittlung, für die es im geltenden Recht keine Grundlage gibt.

- Jeder Leistungserbringer wird wie bisher für seine ordnungsgemäße Behandlungsdokumentation verantwortlich sein, die er zum Zweck der Leistungsabrechnung und weiteren Behandlung, aber auch zum Nachweis über den Inhalt seiner Tätigkeit, etwa in einem Haftungsprozess benötigt.
- Die Aufklärungspflicht nach § 291a Abs. 3 Satz 2 SGB V umfasst gleichermaßen die freiwilligen und verpflichtenden Anwendungen.
- Der Verzicht auf jeden technischen Schutz der Stammdaten entspricht zwar der heutigen Krankenversichertenkarte, ist aber wegen der Erweiterung um das Datum „Zuzahlungsstatus“ nicht akzeptabel. Dieses ist sensibel, weil es je nach Zusatzwissen Informationen über die Gesundheit preisgeben kann. Der Zugriff könnte – wie beim elektronischen Rezept – an die Verwendung eines Heilberufsausweises gekoppelt werden.
- Der Schutz des elektronischen Rezepts durch den Besitz der Karte entspricht dem bisherigen Ablauf beim papiernen Rezept. Im Verlustfall wird der Versicherte sogar besser gesichert, weil nur mit Hilfe eines Heilberufsausweises ein Zugriff möglich ist.
- § 291a Abs. 4 und 5 SGB V sehen keine abgestufte Freigabe von Daten durch den Karteninhaber vor. Diese ist jedoch aus verfassungsrechtlichen Gründen erforderlich, weil es dem Versicherten möglich sein muss, im Einzelfall bestimmte, selbst als sensibel definierte Angaben zurückzuhalten. Die technische Funktionsweise der Gesundheitskarte muss hierfür eine Möglichkeit bereitstellen, die im Grundsatz für jedermann handhabbar ist. Einzelne Datenfelder verschiedener Behandlungsvorgänge könnten hierbei mit einer zusätzlichen PIN gesichert werden.
- Grundvoraussetzung für ein abgestuftes Zugriffssystem ist die Einführung des elektronischen Heilberufsausweises als qualifizierte Signaturkarte und die Vergabe von Attributzertifikaten, die die Rolleneigenschaft als Leistungserbringer bezeugen.
- Wenn einzelne Gruppen von Leistungserbringern zur Erfüllung ihrer Funktion keinen Zugriff auf bestimmte Datenbereiche benötigen, sind sie von diesem technisch auszuschließen.
- Mit dem Erfordernis einer Zugriffsautorisierung für alle vom Versicherten selbst zur Verfügung gestellten Daten ist dem Gesetzgeber ein Fehler unterlaufen. Wenn in diesem Datenfeld der elektronische Organspendeausweis abgelegt wird, ist bei einem Hirntod des Karteninhabers kein Zugriff mehr möglich. Eine neue Regelung sollte einen geschützten und einen ungeschützten Teil des Speicherbereichs vorsehen und den Zugriff auf letzteren Heilberufsausweisträgern vorbehalten.
- Die Regelung zur Patientenquittung ist nicht überzeugend, weil der Zugriff des Karteninhabers nur in Verbindung mit einem elektronischen Heilberufsausweis erfolgen darf. Sinn und Zweck der Quittung ist jedoch gerade, dem Versicherten den transparenten und ausführlichen Nachvollzug der Behandlung in einer selbstgewählten Umgebung zu ermöglichen. Die Bestimmung sollte deshalb angepasst werden.
- Die Protokolldaten dienen nach dem ausdrücklichen Gesetzeswortlaut der Datenschutzkontrolle. Damit darf der Zugriff nur dem Versicherten und nicht den Leis-

tungserbringern offen stehen. De lege ferenda sollte eine Möglichkeit für den Karteninhaber eingeführt werden, die Daten löschen zu lassen.

- De lege lata besteht ein eigenes technisches Zugriffsrecht des Karteninhabers nur für die selbst zur Verfügung gestellten Daten. Perspektivisch ist eine Erweiterung auf alle Daten wünschenswert; Voraussetzung sind ein sicherer Zugriffsmechanismus und ein normativer Schutz gegen die Ausübung sozialen Drucks durch Dritte.
- Die derzeitige Bindung des eigenen Zugriffs auf die selbst zur Verfügung gestellten Daten an eine eigene (zusätzliche) qualifizierte Signaturkarte des Versicherten ist unsinnig. Zur Absicherung genügt eine PIN der Gesundheitskarte; außerdem werden gegenwärtig Personen, die keine Signaturkarte haben, vom Zugriff ausgeschlossen.
- Die Regelung in § 291a SGB enthält keine hinreichende Grundlage, um einem Vertreter des Versicherten die Freigabe der Daten der freiwilligen Anwendungen zu ermöglichen.
- Eine verschlüsselte Übertragung der Daten durch Dritte verstößt nicht gegen § 203 Abs. 1 Nr. 1 StGB. Der erweiterte Beschlagnahmeschutz in § 97 Abs. 2 Satz 2 StPO bietet für den Versicherten hinreichend Schutz. Ein Wertungswiderspruch besteht, weil die Daten zwar bei Leistungserbringer und externen Dienstleistern, nicht jedoch auf den Übertragungswegen vor einer Beschlagnahme geschützt sind. § 100a StPO ist deshalb entsprechend anzupassen. Die Problematik besteht bei Verwendung einer sicheren Ende-zu-Ende-Verschlüsselung nicht. In diesem Fall müssen nur die Gesundheitskarte und ihr geheimer Schlüssel vor einer Beschlagnahme geschützt werden.
- Die Schutznormen der §§ 291a Abs. 8, 307a SGB V erstrecken sich nicht auf den Stammdatensatz. Das ist mit Blick auf dessen Erweiterung um das Datum „Zuzahlungsstatus“ nicht akzeptabel und damit zu ändern. § 307a SGB V erfasst außerdem die Patientenquittung nicht. Auch dies muss angepasst werden.
- Durch die Verweisung auf § 6c BDSG ist § 291a Abs. 3 Satz 2 SGB V überflüssig. Die Krankenkassen müssen die technische Infrastruktur für die Auskunft über die auf oder mittels der Karte gespeicherten Daten bereitstellen; dabei ist zu verhindern, dass sie selbst Zugriff auf diese Daten erhalten. Falls die Auskunft unter Mitwirkung eines Leistungserbringers umgesetzt wird, schließt § 6c Abs. 2 BDSG die Erhebung einer Praxisgebühr, nicht aber die Vergütung durch die Krankenkasse aus.
- Für den Fall, dass die elektronische Gesundheitskarte perspektivisch zur Erstellung qualifizierter Signaturen geeignet sein wird, stellen sich die Zusammenarbeit der Zertifizierungsdiensteanbieter mit den Krankenkassen, die technische Trennung der Kartenfunktionen und das Problem der verschiedenen Gültigkeitszeiträume ähnlich dar wie beim digitalen Personalausweis.
- Wegen der Gefahr des Ausfalls der Gesundheitskarte, des Heilberufsausweises, der Praxis- oder Apotheken-EDV und der Server muss für Eilfälle – auch und gerade beim elektronischen Rezept – ein sicheres Rückfallsystem vorgehalten werden.
- Die Kosten des Projekts werden derzeit mit ca. 1,2 bis 1,5 Mrd. Euro angegeben. Über die zu erwartenden Einspareffekte gibt es erheblich divergierende Prognosen.
- Ähnlich wie beim digitalen Personalausweis wird die Akzeptanz der Gesundheitskarte entscheidend durch den effektiven Schutz der persönlichen Daten der Karteninhaber, die Aufklärung über Wirkungsweise, Chancen und Risiken der Telematik und die Transparenz des Prozesses der Entscheidungsfindung befördert werden.

- Es ist zulässig, die Anspruchsberechtigten der Arbeitslosenversicherung zu verpflichten, für die Antragsstellung und den Datenabruf eine qualifizierte Signaturkarte einzusetzen. Da die wirtschaftlichen Vorteile hauptsächlich bei den Arbeitgebern eintreten, ist ein Finanzierungsmodell zu entwickeln, dass die Kosten nicht einseitig den Antragstellern auferlegt.
- Nimmt der Gesetzgeber zur Effektivitätssteigerung durch die zentrale Datenspeicherung eine Erhöhung der datenschutzrechtlichen Risiken in Kauf, muss er geeignete Schutzvorkehrungen treffen. Die beste Lösung hierfür wäre eine Ende-zu-Ende-Verschlüsselung, deren Umsetzbarkeit jedoch zweifelhaft ist.
- Für die zentrale Speicherung ist ein differenziertes Konzept zur Löschung der jeweils nicht mehr erforderlichen Daten zu entwickeln. Von laufenden Verfahren abgesehen sind die Daten zu löschen, sobald sie für eine hypothetische Anspruchsberechnung zum jeweiligen Zeitpunkt nicht mehr benötigt würden.
- Statt der Zertifikatsnummer könnte im Vollbetrieb auch ein von dieser abgeleitetes Ordnungskriterium verwendet werden. Dieses bringt jedoch nur unwesentliche datenschutzrechtliche Vorteile.
- Die Ermächtigung der Arbeitsagentur zum Datenabruf ist zeitlich zu beschränken und muss jedenfalls dann enden, wenn eine neue Beschäftigung aufgenommen wird.
- Im Interesse der Integrität und Authentizität der Daten gerade bei der Online-Übertragung sollte auch für die Arbeitgeber die Verwendung qualifizierter elektronischer Signaturen vorgeschrieben werden.
- Es ist zwar im Ausgangspunkt für die Akzeptanz der Signaturkarte problematisch, einen Großteil der Bevölkerung zu ihrem Besitz zu verpflichten. Der positive Effekt dieser zwangsweisen Verbreitung liegt aber darin, dass hierdurch der Anreiz zur Entwicklung von Anwendungen im Electronic Commerce und im Electronic Government massiv gesteigert wird. Sind solche Anwendungen verfügbar, werden sich auch Bürger für Signaturverfahren interessieren, die nicht vom JobCard-Verfahren erfasst werden. Das System könnte so eine erhebliche Wirkung für die Verbreitung der elektronischen Signatur entfalten.

Stichwortverzeichnis

11. September 12 f., 74, 95, 122, 175, 417, 434
Abgestufte Zugriffsrechte (bei der Gesundheitskarte)
- als Akzeptanzfaktor 423
- Anforderungen 224 ff., 226
- Umsetzung 306 f., 339, 368 ff.
Adaptive biometrische Systeme 202
AFIS 149, 194
Akzeptabilität 380, 382
Akzeptanz
- allgemeine Einflussfaktoren 393 ff., 396 ff., 412
- als Rechtsproblem 383 ff.
- Beeinflussbarkeit durch den Staat 428 ff.
- Begriff 380 ff.
- der Biometrie 414 ff.
- der Gesundheitskarte 421 ff.
- der Signaturfunktion 424 ff., 426 ff.
- der Volkszählung 399 ff.
- des maschinenlesbaren Personalausweises 405 ff.
- Fallstudien 399 ff., 410 ff.
- Kontextbedingungen 413 f.
- mehrere Funktionen einer Karte 428
- durch die Wirtschaft 426
- soziologischer Begriff 382
Allgemeine Erklärung der Menschenrechte 132, 136, 167
Alternativverfahren s. Rückfallsysteme
Analogie 236, 270
Anonymisierung / anonyme Daten 35, 88, 231
- als Anforderung 142 ff., 157
- bei Datenübermittlungen 289 f.
- bei einzelnen Karten 249 ff., 367
- Personenbezug
- Volkszählungsdaten 403
Arbeits- und Verdienstbescheinigungen 46, 241
Arbeitsagentur 46, 242 ff., 292, 321, 327, 377 f.
Arbeitsgemeinschaft für Aufgaben der Datentransparenz 252, 367
ArchiSig 366
Arzneimitteldokumentation 62, 207
- generelle Einwilligung 64, 210
- Löschungsanspruch 299
- Speicherungsort 217
- Zugriff durch Apotheker 224 f.
Arztbrief, elektronischer 42, 207
- Begriff 62
- Speicherungsort 217 f.
- verschlüsselte Übermittlung 364
Arzt-Patient-Verhältnis 225, 236, 422
Attribut-Zertifikat
- als Mittel der sicheren Authentisierung 321
- auf einem Heilberufsausweis 308, 326, 368
- Begriff 318
- zum Zugriff auf die Gesundheitskarte 224, 327, 339, 372
Auftragskontrolle 308
Auskunft (-sanspruch)
- als Anforderung 133, 135, 163, 295, 419
- digitaler Personalausweis 296
- Gesundheitskarte 240, 297
- Unentgeltlichkeit 273
- Unterrichtung über (§ 6c BDSG) 267
Ausländer
- Erhalt eines Personalausweises 98, 100, 103, 106, 109, 118
- Regelungen im Terrorismusbekämpfungsgesetz 177
Auslegung
- richtlinienkonforme 132, 277, 278
- verfassungskonforme 178, 221
- völkerrechtsfreundliche 131 f., 157, 163
Ausweis, Begriff des 30
Authentisierung 41
- Anwendbarkeit von § 6c BDSG 260
- elektronischer Ausweis 319 ff.
- Funktionsweise 74 f.
- s.a. gegenseitige Authentisierung
Automatische Einzelentscheidung 282 f.
Automatisches Abrufverfahren 292 ff.
Behandlungsfehler 210, 301, 366
Behandlungsvertrag
- Grundlage der Datenerhebung 59 f.

- Grundlage der Schweigepflicht 219, 229, 232
- Grundlage des Auskunftsanspruchs 297
Berechtigungsnachweis, europäischer 207, 213, 279, 343
- als Sichtausweis / elektronische Speicherung 61, 63
- Motiv 44
- Speicherungsort 216
- Zugriffsschutz 221 f.
- zweckfremde Verwendung 237
Berufskammern 233
- Ausgabe von Zertifikaten 292, 325, 326 ff.
Beschlagnahmeschutz 66, 219, 229, 232 ff.
Besondere Arten personenbezogener Daten 274 ff., 293, 296
- biometrische Daten 276, 282
- Gesundheitskarte 278 ff.
- Protokolldaten im Gesundheitswesen 228
- Zuzahlungsstatus 280
Bestimmtheitsgrundsatz
- Anforderungen 140, 153 ff.
- Gesundheitskarte 211 ff.
- Personalausweis 173 ff., 278
- Volkszählungsgesetz 391
Betroffenenrechte 295 ff., s.a. Auskunft
BioAPI 342
Biometrie
- Akzeptanz 414 ff.
- Angriffe 301
- Authentizität 86, 333 f.
- automatische Einzelentscheidung 282 f.
- Begriff 75
- Einsatz bei der Gesundheitskarte 370
- Einsatz bei der Signaturerstellung 177, 193, 333
- Einsatz in der Praxis 81 ff.
- Ermächtigungsgrundlage 154
- Evaluierung 183
- Flüchtigkeit s. dort
- Funktionsweise 78 ff.
- Kombination mehrerer Merkmale 176, 183, 203, 359
- Langzeitstabilität s. dort
- Lebenderkennung s. dort
- Leistungsfähigkeit 180 ff.
- Matching (-On-Card) s. dort
- Mitwirkungsbindung s. dort
- Merkmalsauswahl 178 ff.
- Rohdaten s. dort
- Rückfallsysteme s. dort
- Sensor s. dort
- Templates s. dort
- Verschlüsselung 197, 199, 350 ff.
- Volldaten s. dort
Biometric Data Interchange Formats 342
biT4health 45
Brute Force Attack 330
Bundesdruckerei GmbH
- als derzeit einziger Hersteller 357, 406
- Auswahl der Sicherheitsmerkmale 173
- Chipkartenherstellung 355 f.
- Datenspeicherung bei der Herstellung 193
- DIGANT-Verfahren s. dort
- Signatur der Daten 346
- Vergütung durch Gemeinden 362
- zentrale Speicherung der Seriennummern 50 f., 307, 408
CBEFF 190, 342
Charta der Grundrechte der EU 133, 135, 136 f., 153, 155, 167, 295
Chicago Convention 94
Chipkarten 66 ff.
- als neue Ausweisgeneration 33 f.
- Aufbau 67 f.
- Einsatzgebiete 69 f.
- Identifizierung mittels 34 f.
- Motive der Einführung 37 ff.
Common Access Card 84, 123
Common Criteria 345
Daten zur Prüfung der Arzneimitteltherapiesicherheit s. Arzneimitteldokumentation
Datenakquisitionsangriff 187, 301, 335
Datenschutzaudit 345
Datenschutzbeauftragte
- Akzeptanzförderung durch Einbindung 415, 417, 423
- Auftragsdatenverarbeitung 287
- Einbindung im Ausland 107, 109
- Umsetzung von Datenvermeidung und Datensparsamkeit 248

Datenschutzrichtlinie 137 f.
- Anforderungen 155, 158, 163, 286
- Automatisierte Einzelentscheidung 282
- besondere Arten personenbezogener Daten 275, 277, 278
- Betroffenenrechte 295, 298
- Datensicherheit 302
- Personenkennzeichen, Zulässigkeit 161
Datensicherheit 300 ff.
Datenübermittlung 283 ff.
- gerichtet/ungerichtet 364
- Nichtabstreitbarkeit 365
- Schweigepflicht 231 ff.
- strafprozessuale Fragen 234 ff.
- Weitergabekontrolle 307
Datenverarbeitung im Auftrag 286 ff.
- Angrenzung zu Funktionsübertragung 286 ff.
- Anwendung auf die Gesundheitskarte 288 ff.
- Datensicherheit 308
Datenvermeidung und Datensparsamkeit 140, 143, 196, 247 ff.
Demokratieprinzip 385 ff., 431, 435
DIGANT-Verfahren 51, 329, 357
Digitaler Personalausweis
- Adressänderung 102, 354
- als sichere Signaturerstellungseinheit 40 f., 313, 325, 358 ff.
- Ausgabeverfahren 50 ff., 355 ff., 358 f.
- Biometrie s. dort
- Einsatz im privaten Umfeld 204 ff., 362
- Gebühr 51, 362, 406, 412
- Inhalt 49
- Kompetenz der EU 96
- kontaktlose Schnittstelle s. dort
- Kosten 359 ff.
- Motive der Einführung 37 ff.
- Musterverordnung 50, 173, 358
- Personalausweisnummer 49, 54, 160, 162, 250, 320, 406, 408
- Personalausweisregister s. dort
- Signatur der Ausweisdaten 346 ff.
- Verwendung 54, 56 ff.
- s.a. maschinenlesbarer Personalausweis
DIN 341
DNA 172
Dokumentation
- als ärztliche Pflicht 59 f. 141, 208
- Beweiserleichterungen 214 f.
- Langzeitaufbewahrung 366 f.
Doppelidentitäten 192
Dual-Interface-Chip 68, 103, 354 f.
Eavesdropping 198
eCard-Strategie der Bundesregierung 37, 41, 46, 47, 313
EER 81, 182, 191
Eignung
- als verfassungsrechtliche Anforderung 156
- biometrische Daten 81, 178 ff., 199 ff.
- manuelle Kontrolle 203, 351
Eingabekontrolle 308
Elektronische Form 314
Elektronische Gesundheitskarte
- als sichere Signaturerstellungseinheit 240, 313
- externe Dienstleister 145, 231 f., 234 f., 284 ff., 288 ff., 364
- Freischaltung mittels Biometrie 370
- freiwillige Anwendungen 208, 214, 215, 220, 223 ff., 278, 290, 294
- Funktionen 42 f., 61 f.
- im Ausland 111, 110
- Inhaber 60 f.
- Kosten 374 ff.
- Löschungsrecht 64, 208, 226, 299
- Lösungsarchitektur 45, 343
- Motive der Einführung 41 ff.
- Organisation 372 f.
- Photo des Inhabers 61, 119, 120, 279, 372, 375
- Protokolldaten s. dort
- selbst zur Verfügung gestellte Daten s. dort
- Stammdaten s. dort
- technische Autorisierung 63, 211, 213, 215, 220 f., 223 ff., 226
- Teledienstedatenschutz 284 ff.
- verpflichtende Anwendungen 61 f., 207 ff., 220 ff., 294
- Vertretungsregelung 212 f.

- Zugriff des Inhabers 240 ff., 298 ff., 371 f.
- Zugriffsbefugnisse 220 ff.
- Zuzahlungsstatus s. dort
- zweckfremde Verwendung 65, 228 ff.

Elektronische Patientenakte 42, 65
- als Funktionsübertragung 288
- als Teledienst 284
- Begriff 62
- Löschungsanspruch 299
- Pseudonymisierung 367
- Schutz bei der Übertragung 236
- sozialer Druck zur Offenbarung 239
- Speicherungsort 217
- Zulässigkeit einer verpflichtenden Einführung 207, 210

Elektronische Signatur
- akkreditierte 315
- Aktivierung mittels Biometrie 333 f.
- Akzeptanz 424 ff.
- Beschränkung des Zertifikats 427
- der Personalausweisdaten 346
- einfache 315
- Formerfordernis 314
- Funktionsweise 72 f.
- fortgeschrittene 315
- Gültigkeit 330
- Identifizierung des Inhabers 318
- im Prozess 314, 334
- kombinierter Einsatz mehrerer 327
- Langzeitaufbewahrung 366, 378
- Problem der Einführung 40, 425
- Pseudonyme 252
- qualifizierte 315, 318
- Rechtsfolgen 316
- Signaturstufen 313 ff.
- Unterrichtung 265
- Zusammenarbeit bei der Ausgabe 291 ff., 323 ff.

Elektronischer Ausweis 306, 319 ff., 325, 332, 348

Elektronischer Heilberufsausweis
- als Mittel der Zugriffskontrolle 308
- als Zugriffsinstrument auf Daten 45, 63, 221, 223, 227, 328, 368
- Ausgabe 292, 326
- Investitionsbedarf 373
- im Ausland 64, 103, 110, 112
- Missbrauch 239
- Mitwirkung bei der Auskunft 299
- Spezifikation 343

Elektronisches Rezept
- als besondere Art personenbezogener Daten 279
- als ungerichtete Kommunikation 365
- Ende-zu-Ende Verschlüsselung 290
- Motiv der Einführung 61
- Speicherungsort 213, 217 f.
- Zugriffsbefugnis 63, 220 f.
- Zulässigkeit der verpflichtenden Einführung 207 f.

EMRK
- als Auslegungsmaßstab 132
- Anforderungen 134 ff., 153 f., 155, 163 f., 167, 172, 275, 296

Ende-zu-Ende-Verschlüsselung s. Verschlüsselung

Enrolment
- als verbleibendes Sicherheitsproblem 434
- Anforderungen 179, 355
- Begriff 78
- FER s. dort
- Kosten 359
- mobiles 356
- Personenbezug 148, 152

Erforderlichkeit
- Anforderungen 156, 249, 306
- biometrische Daten 179, 184, 191 ff., 200
- JobCard-Verfahren 245 ff.
- Gesundheitskarte 207, 224, 237
- Personalausweispflicht 166
- Übermittlung aus dem Personalausweisregister 54
- s.a. Verhältnismäßigkeit

EURODAC 83, 96

Europäische Krankenversichertenkarte 42, 97

Evaluierung 183, 344 f.

Face Recognition Vendor Test 179, 182, 202

Fake Angriff 301, 335, 352

FAR 80 f., 171 ff., 179 ff.

Feldversuch 81, 182 f., 201, 344 f.

FER 78, 201, 418

Fernwartung 230

FINEID 98 ff.

Finger (-abdruckserkennung)
- Akzeptanz 418
- als Kostenfaktor 359
- Enrolment 356
- Fehlerraten 181, 201
- kriminalistische Verwendung 75, 194
- Lebenderkennung 352 ff.
- Sensor auf der Karte 196, 335
- Überschussinformationen 276, 278
- unterschiedliche Erkennungsraten 202
- Verhältnismäßigkeit 187 ff.

Fingerprint Verification Competition 181 f., 202
Flüchtigkeit biometrischer Merkmale 77, 86, 185, 187, 418
„Formaler Gehorsam“ 381
Freies Abgeordnetenmandat 389
FRR 80 ff., 171, 179 ff, 203, 333
Fürsorgepflicht des Arztes, erweiterte 370
Funktionstrennung 305
Funktionsübertragung 286 ff., 289
Gegenseitige Authentisierung
- als Kostenfaktor im Gesundheitswesen 374
- beim Einsatz der Biometrie im privaten Umfeld 205
- Funktionsweise 74, 338
- Gesundheitskarte 221, 328, 364
- Personalausweis 197, 198, 348 f.

Gesellschaft für Telematik 45, 65, 289, 343, 372 f.
Gesetzesbindung 388
Gesetzesvorbehalt
- Anforderungen 133 f., 137, 140, 153 ff.
- Gesundheitskarte 211 ff.
- Personalausweis 173 ff.

Gesicht (-serkennung)
- Abgrenzung zur Iriserkennung 176
- Akzeptanz 415, 418
- als besondere Art personenbezogener Daten 276, 278
- als Kostenfaktor 359
- Eignung 179
- Enrolment 355
- Fehlerraten 182, 201
- Lebenderkennung 335, 352 ff.
- „offenes“ Merkmal 186
- unterschiedliche Erkennungsraten 202
- Verfassungsmäßigkeit 170 f.
- Verhältnismäßigkeit 185 f.

Gesundheitskarte s. elektronische Gesundheitskarte
GKV-Modernisierungsgesetz 41, 58, 60 ff., 211 f., 213, 220, 232, 252, 279, 326, 367, 373, 421
Gleichheitssatz 172, 202 f., 263, 391, 422
Gültigkeitszeiträume, unterschiedliche 330 ff., 351 f.
Haftung des Zertifizierungsdiensteanbieters 324
Hartz-Kommission 46, 243
Heilberufsausweis s. elektronischer Heilberufsausweis
Hillclimbing Angriff 189
ICAO
- als Standardisierungsorganisation 38
- Begriff und Rolle 93 f.
- Forderungen und Empfehlungen 76, 165, 190, 197, 201, 333, 347 f., 353, 361
- DOC 9303 95, 342, 348
- New Technology Working Group 95

Identifikationsmodus s. Verifikation
Identität 29 ff.
- Begriff 30 f.
- als Schutzgut informationeller Selbstbestimmung 139, 158, 159, 433

Informationelle Gewaltenteilung
- Anforderungen 140, 158
- Gesundheitskarte 218
- JobCard-Verfahren 244
- Personalausweis 199
- Personalausweisregister 52
- zwischen mehreren Leistungserbringern 219

Informationelle Selbstbestimmung
- als strukturelle Komponente einer demokratischen Gesellschaft 139
- Herleitung 138 f.
- Zusammenhang mit Identitätsbildung 32
- s.a. Volkszählungsurteil

Institutionskarten 328 f.
Internationaler Pakt über bürgerliche und politische Rechte 132, 133, 153
Iris (-erkennung)

- Abgrenzung zur Gesichtserkennung 176
- Akzeptanz 418
- als besondere Art personenbezogener Daten 276, 278
- als Kostenfaktor 359
- Enrolment 356
- Fehlerraten 181, 201
- Lebenderkennung 335, 352 ff.
- unterschiedliche Erkennungsraten 202
- Verhältnismäßigkeit 187
ISIS-MTT 342
ISO 341
JobCard-Verfahren
- Ablauf 242
- Akzeptanz 426 ff.
- Einsatz qualifizierter Signaturen 378
- Ende-zu-Ende Verschlüsselung 377
- Kosten 243 f., 427
- Langzeitaufbewahrung 378
- Löschung der Daten 245
- Motive der Einführung 46
- Registratur Fachverfahren 242, 321, 376 ff.
- Umsetzung 376 ff.
- Verlust der Signaturkarte 377
- verpflichtende Einführung 243
- Zentrale Speicherstelle 47, 143, 242 f., 245, 321, 328, 376 ff.
Kammern s. Berufskammern
Kartenlesegeräte
- als Kostenfaktor 372 f.
- Auskunft 269, 297
- Auswahl 251, 304
- gegenseitige Authentisierung 348 ff., s.a. dort
- Pflicht zu Bereitstellung 272 ff.
- Sicherheit 338
- Zugriff auf Karten 199, 206
Key Recovery 217
Kontaktlose und kontaktbehaftete Schnittstelle
- als Kostenfaktor 360 f.
- als Transparenzproblem 173
- Anforderungen aus § 6c BDSG 257, 274
- Angriffe 302, 338
- Einsatz bei der Gesundheitskarte 223
- Einsatz beim Personalausweis 197 ff., 354 ff.
- Funktionsweise 68
- Standards 341
Kontrollschleuse, automatische 353, 420
Krankenkasse
- Aufklärungspflichten 62, 241, 264, 266, 274
- Mitwirkung bei der Ausarbeitung der Telematik-Infrastruktur 65, 213
- Wechsel der 41, 330
- Zahl 43
- Zugriff auf die Gesundheitskarte 220, 281
- Zusammenarbeit mit Zertifizierungsdiensteanbietern 325, 372, 426
Krankenversichertenkarte, heutige 220, 221, 313, 330
- Missbrauch 375
Krankenversichertennummer 162, 371
Kriterienkatalog, TeleTrusT 344
Landesdatenschutzgesetze
- Datensicherheit, Terminologie 304
- mobile personenbezogene Speicher- und Verarbeitungsmedien 256 f., 261 ff., s.a. dort
- Verhältnis zum BDSG 141
Landespersonalausweisgesetze
- Behörden, Verfahren 50
- Bezugnahme auf die Bundesdruckerei 358
- Erfordernis einer Transparenznorm 264
- Identifizierungsbefugnisse 325
- Personalausweispflicht 48
- Ungültigkeit des Ausweises 351
- Verlust des Ausweises 269, 307
Langzeitstabilität biometrischer Daten 193, 201, 333, 361
Lebenderkennung, biometrische 335 f., 352 ff., 370
Legitimation 382, 384, 385, 430, 435
Legitimationskette 386
Lesegeräte s. Kartenlesegeräte
Lipobay-Skandal 43
Lügendetektor 169
Man-in-the-middle Angriff 302
Maschinenlesbarer Personalausweis
- Argumentationslinien 407 ff.

- Geschichte der Einführung 405 ff.
- Maschinenlesbare Zone 32, 50, 166, 173, 342, 348, 352, 357, 407
- s.a. digitaler Personalausweis

Matching
- Ausrüstung 357
- Begriff 78
- Erheben von Überschussinformationen 277
- FAR, FRR s. dort
- im Ausland 206
- keine Protokollierung 172
- Ort des 195 ff.
- Personenbezug 148, 150, 152

Matching-On-Card
- Anwendbarkeit von § 6c BDSG 258 f.
- Begriff 79
- Personalausweis im Ausland 206
- Erfordernis beim Einsatz zur Signaturerstellung 335
- Gesundheitskarte 370
- Personalausweis im privaten Bereich 204
- in Hongkong 107
- Personenbezug 151
- Verhältnismäßigkeit 195 f.

Mediation 392

Melderechts-Rahmengesetz 321

Menschenwürde
- als Element medizinischer Behandlung 225
- als Teil des Demokratieprinzips 387
- Biometrie 167 ff.
- Datenverarbeitung 138, 156

Mikrozensus-Urteil 138

Mitteilungspflichten, ärztliche 219

Mitwirkungsbindung biometrischer Verfahren
- Akzeptanz 419
- Begriff 76 f.
- Verhältnismäßigkeit 86, 184 ff.

Mobile personenbezogene Speicher- und Verarbeitungsmedien 141, 164, 253 ff.
- Abgrenzung 264 f.
- Begriff 256 ff.
- biometrische Daten 258 ff.
- Form der Unterrichtung 270
- Gesundheitskarte 259
- Inhaber 267
- Landesdatenschutzgesetze 261 ff.
- Lesegeräte 272
- Personalausweisbehörden 266
- Signaturkarten 260
- Unterrichtungspflichten 255, 265, 267 ff.

Musterberufsordnung für Ärzte
- Anforderungen an medizinische Behandlung 225
- Auskunftsanspruch 298 f.
- Datensicherheit 302
- Mindestaufbewahrungspflicht 366
- Rechtsnatur 59
- Schweigepflicht 219, 229, 252

Notfalldaten 42, 62
- Einwilligung 207
- Speicherungsort 216
- Zugriff 63, 215, 223, 328

Objektformel 168

Objektive Zumutbarkeit
- Anforderungen 156
- der Speicherung biometrischer Daten außerhalb des Ausweises 194 f.
- Erfordernis effektiver Rückfallsysteme 199 f., 283
- Gesundheitskarte 207
- zweier biometrischer Datensätze 203

OCSP-Abfrage 73, 284, 328, 368, 372

OECD-Richtlinien 133 f., 158, 163, 295

Organspendeausweis 226, 279

Ort der Datenspeicherung 176 f., 191 ff., 212, 213 ff., s.a. zentrale Datenbank

Patientenquittung 42, 62
- als besondere Art personenbezogener Daten 278
- Einwilligung 207
- fehlender normativer Schutz 237
- Speicherungsort 217
- Zugriff 224, 227

Patientenverfügung 226

Patriot Act 38

Personalausweis s. digitaler Personalausweis

Personalausweisbehörde
- § 6c BDSG 273
- Ausgabeverfahren 266, 301, 329
- Ausstattung 356, 360
- Datenschutzrecht 141
- Datenspeicherung 194

- in den einzelnen Bundesländern 50, 52
- Signatur der Ausweisdaten 193, 338
- Zusammenarbeit mit ZDA 286, 291, 309, 324, 426
Personalausweispflicht 29
- Entwicklung 47 f.
- im Ausland 98, 100, 102, 108, 111, 112, 115, 118, 119, 123, 165
- Inhalt 48
- Verfassungsmäßigkeit 165 f.
Personalausweisregister 51, 191, 193, 291, 292
Personenbezug 142 ff.
- anonyme und pseudonyme Daten 142 ff.
- biometrische Daten 146 ff.
- Daten auf Chipkarten 150 f.
- Relativität des 142
- Templates 149 f.
- templatefreie Verfahren 151 f.
Personenkennzeichen
- Akzeptanzfaktor 415
- Anforderungen 140, 159 ff.
- Biometrie 171, 194
- im Ausland 99, 101, 110, 114, 116, 117, 121
- im Zertifikat 320
- JobCard-Verfahren 376
- Personalausweis 55, 408
PKI, Begriff 71
Pointer 61, 213, 214, 217 f., 251, 328, 367
Postident-Verfahren 325, 361, 372
Praxisgebühr 274, 299, 421
Private Krankenkassen 60, 313
Profile
- Anforderungen 140, 159 ff.
- Biometrie 192, 310
- Problematik 32
- Protokolldaten 227
- zentrale Datenbanken 192
Projektgruppe verfassungsverträgliche Technikgestaltung (provet) 90
Protego 45
Protokolldaten 64 f. 227 f., 279, 280, 300
Protokollierung 172, 308, 328, 366, 369
Pseudonymisierung / pseudonyme Daten
- als Anforderung 157, 249
- Begriff 143
- Gesundheitskarte 251, 367
- Institutionskarte 329
- JobCard-Verfahren 376
- Offenbaren 231
- Übermittlung 289
- Zertifikat 246, 260, 318, 319, 323
PUK 376
Recht und Technik, Verhältnis 87 ff.
Rechtsbewusstsein 392, 397
Referenzdaten, biometrische
- adaptive Systeme 202
- Begriff 78, 80
- Personenbezug 148 ff.
- Speicherungsort 191 ff., 195 ff.
Regulierungsbehörde für Telekommunikation und Post 246, 316, 319, 330, 371
Reisepass
- EU-Verordnung 96, 175, 184
- Kosten 359
- Personalausweispflicht 48, 313
- Übertragbarkeit der Anforderungen zum Personalausweis 36, 39, 191, 347
- Vertraulichkeit der Daten 199
Replay Angriff 301, 335 f., 371
Rohdaten
- Begriff 78
- Erhebung im Ausland 206
- Extraktion durch Chipkarten 69, 196
- Überschussinformationen 188, 190, 277
- s.a. Templates, Volldaten
Rückfallsysteme
- als Akzeptanzfaktor 420
- Anforderungen 168 f., 283, 309, 339 f.
- Aufklärung über 268
- Biometrie 199 ff., 351
- Gesundheitskarte 364
Rückwärtskonstruktion von Templates 150, 152, 189, 251
Schutznormtheorie 255 f.
Schutzpflichten, staatliche 164 f., 206 f., 434
Schweigepflicht, ärztliche
- Herleitung 59 f., 219 f.
- gesetzliche 229 ff.
- Verhältnis zum BDSG 140 f., 288
- zwischen mehreren Leistungserbringern 209, 224

Schwellwert 80
Security Module Card 328, 343, 373
Selbstdatenschutz 88
Selbst zur Verfügung gestellte Daten der Gesundheitskarte 42, 62
- als besondere Arten personenbezogener Daten 278
- als Mittel zur Funktionserweiterung 212
- eigener technischer Zugriff 240, 371
- verfehlte Zugriffsregelung 226 f.
Sensible / sensitive Daten s. besondere Arten personenbezogener Daten
Sensor, biometrischer
- § 6c BDSG 258
- Angriffe 301
- auf Chipkarten 79, 148, 152, 195
- Lebenderkennung 335
- Matching-On-Card 150, 195, s.a. dort
Sichere Signaturerstellungseinheit, Begriff 315
Signatur s. elektronische Signatur
Signaturbündnis 40
Signaturrichtlinie 97, 314, 317
Skimming 198
Sozialer Druck 237 ff., 240 ff.
Sozialversicherungsnummer 122 f., 242 f., 245, 321, 328, 376 f.
Sperrdienst 319, 340, 368
Sphärentheorie 139
Stammdaten
- als besondere Arten personenbezogener Daten 279, 311
- Erhebung 59
- Erweiterung um Zuzahlungsstatus 61
- heutige Krankenversichertenkarte 42
- Speicherungsort 213, 216, 228
- unzureichender Schutz 221 ff.
- verpflichtende Speicherung 207
Standardisierung 131, 188, 190, 340 ff.
Straftatbestände im SGB V 237 ff.
Systemdatenschutz 88, 249, 258, 306
Technikgestaltung 90, 249, 337, 391, 433
Teledienstedatenschutzrecht 284 ff.
Telekommunikationsüberwachung 236
Telematik, Begriff 41
Template
- als besondere Arten personenbezogener Daten 276
- Mittel der Datensparsamkeit 251
- Begriff 78, 79
- Gesetzesvorbehalt 176
- Personenbezug 146 ff., 149
- Rückwärtskonstruktion 189
- Umsetzung des Auskunftsrechts 297
- Verhältnismäßigkeit 188 ff., 310
- s.a. Rohdaten, Volldaten
Templatefreie Verfahren 79, 151
Terrorismusbekämpfungsgesetz 37, 49, 192, 193, 406, 415
Therapeutisches Privileg 298
Transparenz (-prinzip)
- § 6c BDSG als Ausprägung 253
- als Akzeptanzfaktor 409, 422
- Anforderungen 134, 137, 140, 162
- Auskunftsrecht 297, 298
- eigenes Zugriffsrecht auf Gesundheitsdaten 240
- Erhebung von Zertifikatsdaten 246
- kontaktlose Schnittstellen 198, 354
- Mitwirkungsbindung biometrischer Verfahren 185, s.a. dort
Transsexuelle 172
Trusted Travellers 420
Übereinkommen des Europarats 134 f., 158, 163, 275, 295, 302
Überschussinformationen biometrischer Daten
- als Verhältnismäßigkeitskriterium 185
- bei einzelnen Merkmalen 185 ff., 276 f.
- Menschenwürde 170
- Problematik 86, 310
- umstrittener Zusammenhang mit Gesundheitsinformationen 276 f.
UN-Richtlinien zum Datenschutz 133, 157, 275, 295, 302
Verbraucherschutz 86, 420, 425
Verfassungsverträglichkeit 91 f., 435
Verfügbarkeitskontrolle 309
Verhältnismäßigkeit
- Anforderungen 134, 136, 140, 155 f., 249
- Einsatz von Templates 191
- Gesundheitskarte 207, 215
- Kosten 359, 374
- maschinenlesbarer Personalausweis 409

- Ort des Matchings 196 f.
- Volkszählung 400
- s.a. Erforderlichkeit
Verifikations- und Identifikationsmodus 80, 150, 179, 186, 192
VERSA-Konzept 336
Verschlüsselung
- Anforderungen 305, 337 f., 363 f.
- biometrische Daten 350 ff., 415
- Datenübermittlung 289, 329
- Ende-zu-Ende 72, 216, 217, 231, 233, 244 f., 290, 365, 377
- Funktionsweise 70 f.
- Hybrid- 72, 260, 364
- Personalausweisdaten 174, 177 ff., 297, 409
- symmetrische / asymmetrische 71 f.
- Unsicherheit der Algorithmen 351 f.
Videoüberwachung 171, 420
Visa-Waiver-Abkommen 38
Volkszählung
- Argumentationslinien 402 ff.
- Geschichte 399 ff.
- Melderegisterabgleich 401, 403
- -sgesetz 399
Volkszählungsurteil
- inhaltliche Anforderungen an Datenverarbeitung 138 ff., 275, 300
- Geschichte 400 f., 406, 409, 410
Volldaten
- Auskunft 297
- Begriff 79
- Empfehlung der ICAO 95, 116
- Datensparsamkeit 251
- Gesetzesvorbehalt 176
- Matching-On-Card 195
- Personenbezug 146 ff.
- Verhältnismäßigkeit 188 ff., 310
- s.a. Rohdaten, Templates
Vorratsdatenspeicherung
- biometrische Daten außerhalb des Personalausweises 195
- JobCard-Verfahren 244
- grundsätzliches Verbot 140, 157
- zu statistischen Zwecken 400
VPN 363
Weitergabekontrolle 307
Wesentlichkeitslehre 153 f., 174, 410
Zertifizierungsdiensteanbieter
- Begriff und Funktion 73 f.
- Datensicherungspflichten 246 f.
- Einwilligung zum Einsatz von Biometrie 282
- Gebühren 243
- Zusammenarbeit mit Personalausweisbehörden und Krankenkassen 283, 286, 291 f., 303, 323 ff., 358 f.
Zeitstempel 226, 308, 338
Zentrale Datenbank
- als Möglichkeit der Biometrie 79
- biometrische Daten im Ausland 104, 106, 108, 110
- biometrische Daten: Personenbezug 147 ff.
- biometrische Daten: Verbot de lege lata 52, 54, 179
- biometrische Daten: Verbot de lege ferenda 179, 191 ff.
- Gesundheitskarte 213 ff.
- JobCard-Verfahren 244
- Verzicht als Mittel der Datensparsamkeit 251
- s.a. Ort der Datenspeicherung
Zertifizierung 197, 344 f.
Zeugnisverweigerungsrecht 219, 233 ff.
Zugangskontrolle 305 f.
Zugriffskontrolle 305, 308
Zusatzinformationen, biometrische s. Überschussinformationen
Zutrittskontrolle 304
Zuzahlungsstatus
- als besondere Art personenbezogener Daten 279 f., 311
- Missbrauch 375
- Speicherung auf der Gesundheitskarte 61
- unzureichender Zugriffsschutz 221, 237
Zweckbindung
- Anforderungen 133 ff., 137, 140, 157 f., 400
- normativer Schutz bei der Gesundheitskarte 228 ff., 237 ff.
- Reichweite bei den biometrischen Ausweisdaten 177 ff.
- Zugriffsschutz 199, 218, 219
Zweitmeinung, ärztliche 209

Anhang: Fragebogen der internationalen Umfrage

1. Gibt es verfügbare Gutachten oder Machbarkeitsstudien für den Ausweis? Wenn der Ausweis bereits eingeführt wurde: gibt es Evaluationsberichte (gegebenenfalls von Versuchsprojekten)? Sind Zahlen verfügbar (zum Beispiel ausgegebene Karten)?
2. Was sind die (gegebenenfalls vorgesehenen) Rechtsgrundlagen für den Ausweis? Sind sie auf deutsch oder englisch verfügbar?
3. Wird die Karte freiwillig abgegeben? Können Zusatzfunktionen freiwillig gewählt werden?
4. Welcher Karten- und Chiptyp wird verwendet? Wer ist der Hersteller? Wer kann gegebenenfalls bei diesem Anfragen beantworten?
5. Was sind die vorgesehenen Einsatzfelder (Electronic Government, Electronic Commerce, Bankverkehr, Electronic Cash, Gesundheitswesen, Führerschein etc.)? Ist ein Einsatz für die elektronische Signatur vorgesehen?
6. Hinsichtlich der Kosten:
    a. Wie hoch sind die Kosten pro Karte, die Entwicklungskosten und die Kosten für die Infrastruktur?
    b. Gibt es Erfahrungen oder Berechnungen zur Kostendegression?
    c. Wer trägt die Kosten?
7. Gibt es eine Zusammenarbeit mit privaten Anbietern (Public Private Partnerships)?
    a. Bei der Ausgabe der Karten? Wer gibt diese aus: Behörden, private Anbieter, oder gibt es eine Zusammenarbeit?
    b. Bei Herstellung des Chips, Aufspielen der Schlüssel, Verzeichnis- und Sperrdienst, anderen Zertifizierungsdiensten, Software?
    c. Wer trägt die jeweiligen Kosten, und wie sieht das Geschäftsmodell aus?
8. Welche Persönlichkeitsdaten werden auf dem Chip gespeichert? Liegen alle Daten in sichtbarer und elektronischer Form vor, oder werden einige nur digital gespeichert?
9. Ist ein biometrisches Merkmal für die Karte vorgesehen? Wenn ja:
    a. Welches Merkmal wird verwendet, und warum wurde dieses ausgewählt?
    b. Wo sind die Referenzdaten gespeichert, und wo findet der Datenabgleich mit den ihnen statt?
    c. Gibt es eine zentrale Datei?
10. Welches sind die technischen Standards hinsichtlich der Fälschungssicherheit der Karte, ihrer Belastbarkeit und der Funktionsweise des Chips? Wer ist gegebenenfalls Ansprechpartner hinsichtlich der technischen Ausgestaltung?
11. Welche Methoden werden verwendet, um den Datenschutz sicherzustellen?
    a. Welche Gesetze / andere Regelungen gibt es konkret?
    b. Wie ist die Ausgestaltung der technischen Komponenten mit Blick auf den Datenschutz?
    c. Wer hat Zugriff auf welche Daten?
    d. Werden Datenschutzbeauftragte eingebunden?
12. Gab es bei der Einführung des Ausweises Akzeptanzschwierigkeiten (oder werden diese gegebenenfalls befürchtet)? Wenn ja, warum, wenn nein, warum nicht? Findet eine Einbindung der Öffentlichkeit statt oder ist diese geplant?
13. Was sind die (gegebenenfalls erwarteten) Auswirkungen auf den Markt für Chipkarten, Lesegeräte und andere verwendete Komponenten? Welche Folgen werden für Electronic Government und Electronic Commerce Anwendungen prognostiziert? Wer kann gegebenenfalls Fragen zu allgemeinen wirtschaftlichen Folgen beantworten?
14. Welche Initiativen sind in der Zukunft geplant und wie wird die weitere Entwicklung abgeschätzt?

Literaturverzeichnis*

Achterberg, N., Allgemeines Verwaltungsrecht. Ein Lehrbuch, 2. Auflage, Heidelberg 1986.

Adamovich, L., Akzeptabilität und Akzeptanz von Gerichtsentscheidungen am Beispiel der Verfassungsgerichtsbarkeit, in: Pichler, J. W. (Hrsg.), Rechtsakzeptanz und Handlungsorientierung, Wien 1998, 247.

Adams, A. / *Sasse, M. A.*, Users are not the enemy. Why users compromise computer security mechanisms and how to take remedial measures, C.ACM 12/1999, 41.

Adler, A., Sample images can be independently restored from face recognition templates, abrufbar unter http://www.site.uottawa.ca/~adler/publications/2003/adler-2003-fr-templates.pdf, 2003.

Agar, J., Modern Horrors: British Identity and Identity Cards, in: Caplan, J. / Torpey, J. (Ed.), Documenting Individual Identity. The Development of State Practices in the Modern World, Princeton 2001, 101.

Agre, P. E., Your Face Is Not a Bar Code. Arguments against Automatic Face Recognition in Public Places, abrufbar unter http://polaris.gseis.ucla.edu/pagre/bar-code.html, 2003.

Ahrend, V. / *Bijok, B.-C.* / *Diekmann, U.* / *Eitschberger, B.* / *Eul, H.* / *Guthmann, M.* / *Schmidt, M.* / *Schwarzhaupt, P.-D.*, Modernisierung des Datenschutzes?, DuD 2003, 433.

Akehurst, M., Akehurst's modern introduction to international law, 7. Edition by P. Malanczuk, London 1997.

Aktionsforum Telematik im Gesundheitswesen (ATG) / *Gesellschaft für Versicherungswissenschaft und -gestaltung (GVG)*, Management-Papier „Elektronisches Rezept“, Köln 2001a (abrufbar unter http://atg.gvg-koeln.de/xpage/objects/rezept/docs/1/files/atg-managementpapier_el-rezept_stand_09-05-2001_print_copy.pdf).

Aktionsforum Telematik im Gesundheitswesen (ATG) / *Gesellschaft für Versicherungswissenschaft und -gestaltung (GVG)*, Management-Papier „Elektronischer Arztbrief“, Köln 2001b (abrufbar unter http://atg.gvg-koeln.de/xpage/objects/arztbrief/docs/1/files/atg-managementpapier_el-arztbrief_stand_09-05-2001-print_copy.pdf).

Aktionsforum Telematik im Gesundheitswesen (ATG) / *Gesellschaft für Versicherungswissenschaft und -gestaltung (GVG)*, Management-Papier „Pseudonymisierung / Anonymisierung“, Köln 2004a (abrufbar unter http://atg.gvg-koeln.de/xpage/objects/pseudonymisierung/docs/5/files/MP040316.pdf).

Aktionsforum Telematik im Gesundheitswesen (ATG) / *Gesellschaft für Versicherungswissenschaft und -gestaltung (GVG)*, Management-Papier „Patienteninformationssysteme“, Köln 2004b (abrufbar unter http://atg.gvg-koeln.de/xpage/objects/pinformationssysteme/docs/5/files/MP_Infosys_041115.pdf).

Aktionsforum Telematik im Gesundheitswesen (ATG) / *Gesellschaft für Versicherungswissenschaft und -gestaltung (GVG)*, Managementpapier „Elektronischen Patientenakte“, Köln 2005 (abrufbar unter http://atg.gvg-koeln.de/xpage/objects/patientenakte/docs/4/files/MP_ePa_050118.pdf).

Alber, S. / *Widmaier, U.*, Die EU-Charta der Grundrechte und ihre Auswirkungen auf die Rechtsprechung. Zu den Beziehungen zwischen EuGH und EGMR, EuGRZ 2000, 497.

Albrecht, A., Biometrie zum Nutzen für Verbraucher? Kriterien der Verbraucherfreundlichkeit biometrischer Verfahren, DuD 2000, 332.

Albrecht, A., Stand der verbraucherpolitischen Diskussion zu biometrischen Erkennungsverfahren unter Berücksichtigung der Situation in den USA, Bonn 2001.

Albrecht, A., Relevanz biometrischer Verfahren im gesellschaftlichen Kontext, in: Nolde, V. / Leger, L. (Hrsg.): Biometrische Verfahren. Körpermerkmale als Passwort – Grundlagen, Sicherheit und Einsatzgebiete biometrischer Identifikation, Köln 2002a, 85.

---

* Die Internetseiten des Literaturverzeichnisses und der Belege im Text wurden letztmalig Anfang Mai 2005 geprüft. Die Fußnoten enthalten eine Reihe von Nachrichten aus Newslettern, die nicht in das Literaturverzeichnis aufgenommen wurden.

Albrecht, A., Biometrie und Recht, in: Nolde, V. / Leger, L. (Hrsg.): Biometrische Verfahren. Körpermerkmale als Passwort – Grundlagen, Sicherheit und Einsatzgebiete biometrischer Identifikation, Köln 2002b, 97.

Albrecht, A., Verbraucherpolitische Bedeutung der Biometrie, in: Nolde, V. / Leger, L. (Hrsg.): Biometrische Verfahren. Körpermerkmale als Passwort – Grundlagen, Sicherheit und Einsatzgebiete biometrischer Identifikation, Köln 2002c, 129.

Albrecht, A., Biometrische Verfahren im Spannungsfeld von Authentizität im elektronischen Rechtsverkehr und Persönlichkeitsschutz, Baden-Baden 2003a.

Albrecht, A., BIOVISION. Roadmap to Successful Deployments from the User and System Integrator Perspective. Privacy Best Practices in Deployment of Biometric Systems (WP 7), 28. August 2003, abrufbar unter http://www.eubiometricsforum.com/dmdocuments/D7.4%20Best%20Practices1.pdf, 2003b.

Albrecht, A., The European Biometrics Forum (EBF), DuD 2003, 571.

Albrecht, A. / *Probst, T.*, Biometrie für alle?, DuD 2000, 318.

Albrecht, A. / *Probst, T.*, Bedeutung der politischen und rechtlichen Rahmenbedingungen für biometrische Identifikationssysteme, in: Behrens, M. / Roth, R. (Hrsg.), Biometrische Identifikation. Grundlagen, Verfahren, Perspektiven, Braunschweig 2001, 27.

American Civil Liberties Union (ACLU), How the U.S. ignored international concerns and pushed for radio chips in passport without security. An ACLU white paper, abrufbar unter http://www.aclu.org/Privacy/Privacy.cfm?ID=17078&c=130, 2004.

Appel, R., Volkserfassung – zweiter Versuch. Das Volkszählungsprojekt 1987, in: Kutscha, M. / Paech, N. (Hrsg.), Totalerfassung. „Sicherheitsgesetze", Volkszählung, Neuer Personalausweis, Möglichkeiten der Gegenwehr, Köln 1986a, 45.

Appel, R., Volkserfassung – zweiter Versuch, in: Hummel, D. / Pollähne, H. / Ruhne, R. / Sögtrop, R. (Hrsg.), „Kein Staat mit diesem Staat?" Freiheitsrechte, Repression und staatliche Hilfe in der Demokratie, Bielefeld 1986b, 267.

Appel, R., Vorsicht Volkszählung!, in: ders. / Hummel, D. (Hrsg.), Vorsicht Volkszählung!, Köln 1987, 12.

Appel, R. / *Hummel, D.*, Die Republik nach der Volkszählung. Ein Beispiel für die Auseinandersetzung zwischen Herrschaftsapparat und außerparlamentarischer Bewegung, in: dies. / Hippe, W. (Hrsg.), Die neue Sicherheit. Vom Notstand zur Sozialen Kontrolle, Köln 1988, 9.

Arbeitskreis Technik der Datenschutzbeauftragten des Bundes und der Länder(AKT), Datenschutzfreundliche Technologien, DuD 1997, 709.

Arbeitskreis Technik der Datenschutzbeauftragten des Bundes und der Länder(AKT), JobCard: Modell der Ende-zu-Ende-Verschlüsselung. Rahmenbedingungen für die Beauftragung eines Gutachtens, DuD 2005, 29.

Article 29 – Data Protection Working Party (Art. 29 DPWP), WP 80: Working document on biometrics, 12168/02/EN, abrufbar unter http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2003/wp80_en.pdf, 2003.

Article 29 – Data Protection Working Party (Art. 29 DPWP), WP 96: Opinion No 7/2004 on the inclusion of biometric elements in residence permits and visas taking account of the establishment of the European information system on visas (VIS), 11224/04/EN, abrufbar unter http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2004/wp96_en.pdf, 2004.

Article 29 – Data Protection Working Party (Art. 29 DPWP), WP 105: Working document on data protection issues related to RFID technology, 10107/05/EN, abrufbar unter http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2005/wp105_en.pdf, 2005.

Ashbourn, J., Biometrics. Advanced Identity Verification. The Complete Guide, London 2000.

Auernhammer, H., Bundesdatenschutzgesetz. Kommentar, 3. Auflage, Köln 1993.

Aufreiter, R., Elektronische Signaturen und Passworte in Verbindung mit Biometrie, in: Nolde, V. / Leger, L. (Hrsg.): Biometrische Verfahren. Körpermerkmale als Passwort – Grundlagen, Sicherheit und Einsatzgebiete biometrischer Identifikation, Köln 2002, 250.

Aufsichtsbehörde Baden-Württemberg, Hinweise zum Bundesdatenschutzgesetz für die private Wirtschaft, Nr. 11, StAnz BW 1980, 5 (abgedruckt in *Schaffland/Wiltfang*, BDSG, Nr. 7010).

Aufsichtsbehörde Baden-Württemberg, Hinweise zum Bundesdatenschutzgesetz für die private Wirtschaft, Nr. 25, StAnz BW 1986, 4 (abgedruckt in *Schaffland/Wiltfang*, BDSG, Nr. 7010).
Aufsichtsbehörde Baden-Württemberg, Hinweise zum Bundesdatenschutzgesetz für die private Wirtschaft, Nr. 31, StAnz BW 1993, 5 (abgedruckt in *Schaffland/Wiltfang*, BDSG, Nr. 7010).
Bär, W., Der Zugriff auf Computerdaten im Strafverfahren, Köln 1992.
Bäumler, H., Das neue Pass- und Ausweisrecht, CR 1986, 284.
Bäumler, H., Wie geht es weiter mit dem Datenschutz?, DuD 1997, 446.
Bäumler, H., Medizinische Dokumentation und Datenschutzrecht, MedR 1998, 400.
Bäumler, H., „Der neue Datenschutz", RDV 1999, 5.
Bäumler, H., Das TDDSG aus Sicht eines Datenschutzbeauftragten, DuD 1999, 258.
Bäumler, H. / *Federrath, H.* / *Golembiewski, C.*, Bericht zum Vorgehen von Strafverfolgungsbehörden gegen das Projekt „AN.ON — Anonymität.Online", abrufbar unter http://www.datenschutzzentrum.de/projekte/anon/bericht.pdf, 2003.
Bäumler, H. / *Gundermann, L.* / *Probst, T.*, Stand der nationalen und internationalen Diskussion zum Thema Datenschutz bei biometrischen Systemen, Kiel 2001.
Bakker, E. de, Der (beinahe) weiße Fleck in der Legitimitätsforschung. Über Akzeptanz, verborgenes Unbehagen und Zynismus, ZfRSoz 2003, 219.
Balboni, P., Liability of Certification Service Providers towards Relying Parties and the Need for a Clear System to Enhance the Level of Trust in Electronic Communication, Information & Communications Technology Law 2004, 212.
Bales, S. / *Holland, J.*, Die elektronische Gesundheitskarte als Einstieg in ein vernetztes Gesundheitswesen, in: Jäckel, A. (Hrsg.), Telemedizinführer Deutschland, 5. Auflage, Darmstadt 2004, 14.
Banisar, D. / *Davies, S.*, Global Trends in Privacy Protection: An international Survey of Privacy, Data Protection, and Surveillance Laws and Developments, J. Marshall J. Computer & Info. L. 1999, 1.
Barkhaus, A., Theorie der Identität: Begriff und klassische theoretische Ansätze, in: Dohrenbusch, H. / Blickenstorfer, J. (Hrsg.), Allgemeine Heilpädagogik. Eine interdisziplinäre Einführung. Band II: Exemplarische Ausschnitte der Wirklichkeit, Luzern 1999, 55.
Bauer, F. L., Entzifferte Geheimnisse. Methoden und Maximen der Kryptologie, 2. Auflage, Berlin 1997.
Baum, M., Die elektronische Identität? Der Name als Zertifikatsbestandteil – ein Interpretationsvorschlag, DuD 1999, 511.
Baumbach, A. / *Lauterbach, W.* / *Albers, J.* / *Hartmann, P.*, Zivilprozessordnung mit Gerichtsverfassungsgesetz und anderen Nebengesetzen, 62. Auflage München 2004 (zitiert als: Baumbach-*Bearbeiter*)
Beck, U., Risikogesellschaft. Auf dem Weg in eine neue Moderne, Frankfurt am Main 1986.
Beck, U., Die Erfindung des Politischen. Zu einer Theorie reflexiver Modernisierung, Frankfurt am Main 1993.
Becker, J., Das Demokratieprinzip und die Mitwirkung Privater an der Erfüllung öffentlicher Aufgaben. Zum Beschluss des Bundesverfassungsgerichts „Lippeverband und Emschergenossenschaft" vom 5. Dezember 2002, DÖV 2004, 910.
Becker, U., Das Menschenbildnis des Grundgesetzes in der Rechtsprechung des Bundesverfassungsgerichts, Berlin 1996.
Behrens, M. / *Roth, R.*, Sind wir zu vermessen, die PIN zu vergessen? Erfahrungen aus einem Feldversuch, DuD 2000, 327.
Behrens, M. / *Roth, R.*, Biometrische Identifikationssysteme: Auf dem Weg vom Labor zum Markt. Eine Bestandsaufnahme – unter Berücksichtigung der USA, Gießen 2001a.
Behrens, M. / *Roth, R.*, Grundlagen und Perspektiven biometrischer Identifikation, in: dies. (Hrsg.), Biometrische Identifikation. Grundlagen, Verfahren, Perspektiven, Braunschweig 2001b, 8.
Behrens, M. / *Roth, R.*, BioTrust: Untersuchung der Akzeptanz und Nutzung biometrischer Identifikationssysteme, in: Nolde, V. / Leger, L. (Hrsg.): Biometrische Verfahren. Körpermerkmale

als Passwort – Grundlagen, Sicherheit und Einsatzgebiete biometrischer Identifikation, Köln 2002, 399.
Behrens, M. / *Roth, R.* / *Büchner, H.* / *Heumann, B.* / *Stäblein, B.* / *Weber, M.*, Endbericht der wissenschaftlichen Begleitforschung zum Forschungsprojekt BioTrusT, in: Bundesministerium für Wirtschaft und Technologie / S-Finanzgruppe / TeleTrusT Deutschland e.V., BioTrusT. Ein interdisziplinäres Projekt zur Förderung biometrischer Identifizierungsverfahren, Abschlussbericht, September 2002, Teilband II.
Beier, B., Datenschutz in der Medizin. Aspekte zu Überlegungen für eine bereichsspezifische Regelung im Gesundheitswesen, Frankfurt am Main 1979.
Below, G. v., Die schweizerische Gesundheitskarte. Aspekte aus der Sicht der Verbindung der schweizerischen Ärztinnen und Ärzte FMH. Abgleichtagung vom 30. August 2001, abrufbar unter http://www.isesuisse.ch/de/gesundheitskarte/rapport_below_d.pdf, 2001.
Benda, E., Privatsphäre und Persönlichkeitsprofil, in: Leibholz, G. / Faller, H. J. / Mikat, P. / Reis, H. (Hrsg.), Menschenwürde und freiheitsrechtliche Rechtsordnung. Festschrift für Willi Geiger zum 65. Geburtstag, Tübingen 1974, 23.
Benda, E., Zur gesellschaftlichen Akzeptanz verwaltungs- und verfassungsgerichtlicher Entscheidungen, DÖV 1983, 305.
Benfer, J., Rechtseingriffe von Polizei und Staatsanwaltschaft. Voraussetzungen und Grenzen, 2. Auflage, München 2001.
Berg, W., Vom Wettlauf zwischen Recht und Technik. Am Beispiel neuer Regelungsversuche im Bereich der Informationstechnik, JZ 1985, 401.
Berg, W., Telemedizin und Datenschutz, MedR 2004, 411.
Berger & Partner GmbH, Telematik im Gesundheitswesen. Perspektiven der Telemedizin in Deutschland. Gutachten für Bundesministerium für Bildung, Wissenschaft, Forschung und Technologie und Bundesministerium für Gesundheit, München 1997.
Bergfelder, M., Was ändert das 1. Signaturänderungsgesetz? Die qualifizierte elektronische Signatur zwischen Anspruch und Wirklichkeit, CR 2005, 148.
Bergmann, L. / *Möhrle, R.* / *Herb, A.*, Datenschutzrecht. Kommentar, Loseblatt, Stand: 29. Lieferung Februar 2004, Stuttgart.
Bernstein, G., Information Technologies and Identity, CRi 2005, 1.
Bertsch, A. / *Fleisch, S.-D.* / *Michels, M.*, Rechtliche Rahmenbedingungen des Einsatzes digitaler Signaturen, DuD 2002, 69.
Beske, F. / *Drabinski, T.* / *Zöllner, H.*, Das Gesundheitswesen im internationalen Vergleich. Eine Antwort auf die Kritik, Kiel 2004.
Betrand, U. / *Kuhlmann, J.* / *Stark, C.*, Der Gesundheitschip. Vom Arztgeheimnis zum gläsernen Patienten, Frankfurt am Main 1995.
Beulke, W., Der Verteidiger im Strafverfahren. Funktionen und Rechtsstellung, Frankfurt am Main 1980.
Beulke, W., Strafprozessrecht, 6. Auflage, Heidelberg 2002.
Beutelspacher, A. / *Schwenk, J.* / *Wolfenstetter, K.-P.*, Moderne Verfahren der Kryptographie. Von RSA zu Zero-Knowledge, 5. Auflage, Wiesbaden 2004.
Biometric Working Group, Best practices in testing and reporting performance of biometric devices, Version 1.0, abrufbar unter http://www.cesg.gov.uk/site/iacs/itsec/media/protection-profiles/BBP.pdf, 2000.
BITKOM, Freiräume schaffen für Wachstum, Innovation und Arbeitsplätze, Berlin 2002 (abrufbar unter http://www.bitkom.org/files/documents/ACF6BE1.pdf).
BITKOM, Sicherheit für Systeme und Netze in Unternehmen. Einführung in die IT-Sicherheit und Leitfaden für erste Maßnahmen, 2. Auflage, Berlin 2003 (abrufbar unter http://www. bitkom.org → Publikationen).
BITKOM / *VDAP* / *VHitG* / *ZVEI*, Einführung einer Telematik-Architektur im deutschen Gesundheitswesen. Expertise, abrufbar unter http://www.ztg-nrw.de/down/262/telematik_expertise.pdf, 2003.

Bizer, J., Forschungsfreiheit und Informationelle Selbstbestimmung. Gesetzliche Forschungsregelungen zwischen grundrechtlicher Förderungspflicht und grundrechtlichem Abwehrrecht, Baden-Baden 1992.
Bizer, J., Datenschutz durch Technikgestaltung, in: Bäumler, H. / Mutius, A. v. (Hrsg.), Datenschutzgesetze der dritten Generation. Texte und Materialien zur Modernisierung des Datenschutzrechts, Neuwied 1999, 28.
Bizer, J., Selbstregulierung des Datenschutzes, DuD 2001, 168.
Bizer, J., Selbstauthentifizierende Ausweiskarte, DuD 2002, 44.
Bizer, J., Datenspeicherung in zentralen und peripheren Netzen versus SmartCards – wozu digitale Signaturen in der öffentlichen Verwaltung?, in: v. Zezschwitz, F. / Möller, K. P. (Hrsg.), Verwaltung im Zeitalter des Internet. Vernetzte Verwaltung und Datenschutz, Baden-Baden 2002, 19.
Bizer, J., Personenkennzeichen, DuD 2004, 45.
Blanke, T., Antidemokratische Effekte der verfassungsgerichtlichen Demokratie, KJ 1998, 452.
Blankenagel, A., Das Recht, ein „Anderer" zu sein. Späte Überlegungen zum Transsexuellen-Beschluss (BVerfGE 49, 286) – überfällige Gedanken zum Namensänderungsrecht, DÖV 1985, 953.
Bleckmann, A., Der Grundsatz der Völkerrechtsfreundlichkeit der deutschen Rechtsordnung, DÖV 1996, 137.
Bludau, B. / *Buchauer, A.* / *Roßnagel, A.* / *Schneider, M. J.*, Die Simulationsstudie Gesundheitswesen, in: Roßnagel, A. / Haux, R. / Herzog, W. (Hrsg.): Mobile und sichere Kommunikation im Gesundheitswesen, Braunschweig 1999, 79.
Blum, F., Entwurf eines neuen Signaturgesetzes, DuD 2001, 71.
Bobrowski, M., Biometrie und Verbraucherschutz, DuD 1999, 159.
Bockelmann, P., Die Dokumentationspflicht des Arztes und ihre Konsequenzen, in: Vogler, T. (Hrsg.), Festschrift für Hans-Heinrich Jescheck zum 70. Geburtstag, Erster Halbband, Berlin 1985, 693.
Böhm, U. / *Röhrig, A.* / *Schadow, B.*, Telemonitoring und Smart Home Care. Hohe Akzeptanz bei den über 50-Jährigen, DÄ 2003, B 2743.
Bölsche, J., Der Weg in den Überwachungsstaat, Hamburg 1979.
Boente, W. / *Riehm, T.*, Das BGB im Zeitalter digitaler Kommunikation. Neue Formvorschriften, JURA 2001, 793.
Bogdandy, A. v., The European Union as a Human Rights Organization. Human Rights and the Core of the European Union, CMLRev 2000, 1307.
Bogdanowicz, M. / *Beslay, L.*, Cybersicherheit und die Zukunft der Identität, The IPTS Report Nr. 57 (September 2001), abrufbar unter http://www.jrc.es/home/report/german/articles/vol57/ICT4G576.htm, 2001.
Bolle, R. M. / *Connell, J. H.* / *Pankanti, S.* / *Ratha, N. K.* / *Senior, A. W.*, Guide to Biometrics, New York 2004.
Bongen, W. / *Kremer, R.*, Probleme der Abwicklung ärztlicher Privatliquidationen durch externe Verrechnungsstellen, NJW 1990, 2911.
Booz Allen Hamilton GmbH / *Bundesdruckerei GmbH* / *ZN Vision Technologies AG*, Leistungsfähigkeit biometrischer Identifikationssysteme zur Ausrüstung von Ausweispapieren (Gutachten für das Büro für Technikfolgenabschätzung beim Deutschen Bundestag), Bochum 2003.
Borges, G., Prozessuale Formvorschriften und der elektronische Rechtsverkehr, K&R 2001, 196.
Borges, G., Verträge im elektronischen Geschäftsverkehr. Vertragsabschluß, Beweis, Form, Lokalisierung, anwendbares Recht, München 2003.
Bourseau, F. / *Fox, D.* / *Thiel, C.*, Vorzüge und Grenzen des RSA-Verfahrens, DuD 2002, 84.
Brandner, R. / *Pordesch, U.*, Konzept zur signaturgesetzkonformen Erneuerung qualifizierter Signaturen, DuD 2003, 354.
Braun, W. / *Kollack, N.* / *Mund, S.*, Beitrag zur elektronischen Gesundheitskarte auf der OMNICARD 2004, in: Fluhr, M. (Hrsg.), Neue und bewährte Applikationsfelder der Chipkarte. Kongressdokumentation und Katalog, OMNICARD 2004, Berlin 2004, 231.

Breidenbach, J. / *Zukrigl, I.*, Vernetze Welten – Identitäten im Internet, in: Aus Politik und Zeitgeschichte. Beilage zur Zeitschrift „Das Parlament", B 49-50/2003, 29.
Breitenmoser, S., Der Schutz der Privatsphäre gemäß Art. 8 EMRK. Das Recht auf Achtung des Privat- und Familienlebens, der Wohnung und des Briefverkehrs, Basel 1986.
Breitenstein, M., Überblick über biometrische Verfahren, in: Nolde, V. / Leger, L. (Hrsg.): Biometrische Verfahren. Körpermerkmale als Passwort – Grundlagen, Sicherheit und Einsatzgebiete biometrischer Identifikation, Köln 2002, 35.
Brenner, G., Beitrag zur elektronischen Gesundheitskarte auf der OMNICARD 2004, in: Fluhr, M. (Hrsg.), Neue und bewährte Applikationsfelder der Chipkarte. Kongressdokumentation und Katalog, OMNICARD 2004, Berlin 2004, 219.
Britz, G., Bedeutung der EMRK für nationale Verwaltungsgerichte und Behörden. Erweiterte Bindungswirkung nach EuGH, Slg. 2002, I-6279 – Carpenter?, NVwZ 2004, 173.
Bröhl, G. / *Tettenborn, A.*, Das neue Recht der elektronischen Signaturen. Kommentierende Darstellung von Signaturgesetz und Signaturverordnung, Köln 2001.
Brohm, W., Öffentliches Baurecht. Bauplanungs-, Bauordnungs- und Raumordnungsrecht, 3. Auflage, München 2002.
Bromba, M., On the reconstruction of biometric raw data from template data, abrufbar unter http://www.bromba.com/knowhow/temppriv.htm, 2003.
Bromba, M., Biometric Myths, abrufbar unter http://www.bromba.com/knowhow/biomyths.htm, 2004.
Brown, C. / *Elliott, F.*, Labour to launch ID card – and it'll cost you GBP 25, The Daily Telegraph, 20.4.2003 (abrufbar unter http://www.dailytelegraph.co.uk/news/main.jhtml?xml=/news/2003/04/20/nid20.xml&sSheet=/news/2003/04/20/ixhome.html).
Brühann, U., Die Veröffentlichung personenbezogener Daten im Internet als Datenschutzproblem. Zur Rechtsprechung des Europäischen Gerichtshofs, DuD 2004, 201.
Brunnstein, K., Und wir finden ihn doch. Wie anonym sind die Volkszählungsdaten?, in: Taeger, J. (Hrsg.), Die Volkszählung, Hamburg 1983, 128.
Brunnstein, K., Über Möglichkeiten der Re-Identifikation von Personen aus Volkszählungsdaten, in: Appel, R. / Hummel, D. (Hrsg.), Vorsicht Volkszählung!, Köln 1987, 62.
Bryde, B.-O., Die bundesrepublikanische Volksdemokratie als Irrweg der Demokratietheorie, Staatswissenschaften und Staatspraxis 1994, 305.
Bryde, B.-O., Konstitutionalisierung des Völkerrechts und Internationalisierung des Verfassungsrechts, Der Staat 2003, 61.
Buchmann, J., Einführung in die Kryptographie, 2. Auflage, Berlin 2001.
Büger, M. / *Esslinger, B.* / *Koy, H.*, Das deutsche Signaturbündnis. Ein pragmatischer Weg zum Aufbau einer interoperablen Sicherheitsinfrastruktur und Applikationslandschaft, DuD 2004, 133.
Büllesbach, A., Den Anfängen wehren. Die Entwicklung des neuen Personalausweissystems aus datenschutzrechtlicher Sicht, in: Taeger, J. (Hrsg.), Der neue Personalausweis, Hamburg 1984, 113.
Büllesbach, A., Das TDDSG aus Sicht der Wirtschaft, DuD 1999, 263.
Büllesbach, A. / *Garstka, H.*, Systemdatenschutz und persönliche Verantwortung, in: Müller, G. / Pfitzmann, A. (Hrsg.), Mehrseitige Sicherheit in der Kommunikationstechnik. Verfahren, Komponenten, Integration, Band I, Bonn 1997, 383.
Büllingen, F. / *Hillebrand, A.*, Technikfolgenabschätzung und Akzeptanzforschung beim Einsatz biometrischer Verfahren, in: Nolde, V. / Leger, L. (Hrsg.): Biometrische Verfahren. Körpermerkmale als Passwort – Grundlagen, Sicherheit und Einsatzgebiete biometrischer Identifikation, Köln 2002, 420.
Bürge, U., Digitale Identität und eID-Karte – Das Projekt einer schweizerischen elektronischen Identitätskarte, in: Muralt-Müller, H. / Auer, A. / Koller, T. (Hrsg.), E-Voting. Tagung für Informatik und Recht 2002, Bern 2003 (abrufbar unter http://www.ofj.admin.ch/d/index.html → Rechtsinformatik und Informatikrecht → Amtliche Digitale Identität → Digitale Identität und eID-Karte).

Büro für Technikfolgenabschätzung beim Deutschen Bundestag (TAB), Biometrische Identifikationssysteme. Sachstandsbericht, BT-Drs. 14/10005, 2002.

Büro für Technikfolgenabschätzung beim Deutschen Bundestag (TAB), Biometrie und Ausweisdokumente. Leistungsfähigkeit, politische Rahmenbedingungen, rechtliche Ausgestaltung. Zweiter Sachstandsbericht, BT-Drs. 15/4000, 2004.

Bull, H. P., Datenschutz contra Amtshilfe. Von der „Einheit der Staatsgewalt" zur „informationellen Gewaltenteilung", DÖV 1979, 689.

Bull, H. P., Neue Konzepte, neue Instrumente? Zur Datenschutz-Diskussion des Bremer Juristentages, ZRP 1998, 310.

Bultmann, M. / *Wellbrock, R.* / *Biermann, H.* / *Engels, J.* / *Ernestus, W.* / *Höhn, U.* / *Wehrmann, R.* / *Schurig, A.*, Datenschutz und Telemedizin. Anforderungen an Medizinnetze. Stand 10/2002, abrufbar unter http://www.bfd.bund.de/technik/telemed.pdf.

Bundesärztekammer (BÄK), Empfehlungen zu ärztlicher Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis, DÄ 1996, A 2809 (abrufbar unter http://www.bundesaerzte kammer.de/30/Richtlinien/Empfidx/Schweigepfl/).

Bundesamt für Sicherheit in der Informationstechnik (BSI), Chipkarten im Gesundheitswesen. Technikfolgenabschätzung zur Sicherheit in der Informationstechnik, Abschlussbericht, Köln 1995.

Bundesamt für Sicherheit in der Informationstechnik (BSI), Technische Evaluierungskriterien zur Bewertung und Klassifizierung biometrischer Systeme, Entwurf, Version 0.6 vom 14. September 2000 (zitiert nach *Albrecht* 2003a, 60 f.).

Bundesamt für Sicherheit in der Informationstechnik (BSI), BioFace. Vergleichende Untersuchung von Gesichtserkennungssystemen. Öffentlicher Abschlussbericht BioFace I & II, Version 1.9a, abrufbar unter http://www.bsi.bund.de/literat/studien/BioFace/index.htm, 2003.

Bundesamt für Sicherheit in der Informationstechnik (BSI), IT-Grundschutzhandbuch, Loseblatt, Köln, Stand Oktober 2003 (abrufbar unter http://www.bsi.bund.de/gshb/deutsch/in dex.htm).

Bundesamt für Sicherheit in der Informationstechnik (BSI), Risiken und Chancen des Einsatzes von RFID-Systemen. Trends und Entwicklungen in Technologien, Anwendungen und Sicherheit, abrufbar unter http://www.bsi.de/fachthem/rfid/studie.htm, 2004.

Bundesamt für Sicherheit in der Informationstechnik (BSI) / *Bundeskriminalamt (BKA)* / *Fraunhofer Institut für Graphische Datenverarbeitung (IGD)*, Evaluierung biometrischer Systeme. Fingerabdrucktechnolgien – BioFinger. Öffentlicher Abschlussbereicht, Version 1.0, 20. Mai 2004, abrufbar unter http://www.bsi.de/literat/studien/BioFinger/BioFin ger_I.pdf, 2004.

Bundesamt für Sicherheit in der Informationstechnik (BSI) / *Bundeskriminalamt (BKA)* / *Secunet AG*, Untersuchung der Leistungsfähigkeit von Gesichtserkennungssystemen zum geplanten Einsatz in Lichtbilddokumenten – BioP I. Öffentlicher Abschlussbericht, Version 1.1, 7. April 2004, abrufbar unter http://www.bsi.de/literat/studien/biop/index.htm, 2004.

Bundesdruckerei, Abschlussbericht zum Pilotprojekt „Digitaler Dienstausweis", Version 1.3, Berlin 2002.

Bundesministerium für Wirtschaft und Arbeit / *Hans-Bredow-Institut* (Hrsg.), Rechtskonformes E-Government. Antworten auf Kernfragen beim Bau eines virtuellen Rathauses, Berlin 2003.

Bundesregierung, Informationsgesellschaft Deutschland 2006, abrufbar unter http://www.bmbf.de/pub/aktionsprogramm_informationsgesellschaft_2006.pdf, 2003.

Bundestags-Enquetekommission Zukunft der Medien in Wirtschaft und Gesellschaft – Deutschlands Weg in die Informationsgesellschaft, Vierter Zwischenbericht zum Thema Sicherheit und Schutz im Netz, BT-Drs. 13/11002, Bonn 1998.

Bundesvereinigung Deutscher Apothekerverbände e.V. (ABDA), VERSA – Verteilte Signatur Arbeitsplätze. Ein Überblick, abrufbar unter http://www.wuv-gmbh.de/media/versa_abstract.pdf, 2002.

Burchardt, U., Die EU lässt das Volk vermessen, FR v. 2.12.2004.

Burke, J. / *Warren, P.*, Smelling out wrongdoers will put the law ahead by a nose, The Observer, 28. Dezember 2003 (abrufbar unter http://politics.guardian.co.uk/homeaffairs/story/0,11026, 1113313,00.html).

Burkeman, O. / *Tuckman, J.*, How US paid for secret files on foreign citizens. Latin Americans furious in row over selling personal data, The Guardian, 5.5.2003, abrufbar unter http://www.guardian.co.uk/international/story/0,3604,949554,00.html, 2003.
Busch, C. / *Daum, H.* / *Finke, M.* / *Funk, W.*, Studie BioIS – Vergleichende Untersuchung biometrischer Identifikationssysteme, hrsg. vom Bundesamt für Sicherheit in der Informationstechnik, Bonn 2000.
Butzer, H., Verfassungsrechtliche Anmerkungen zum GKV-Gesundheitsmodernisierungsgesetz 2004 (GMG), MedR 2004, 177.
Callies, C., Die Charta der Grundrechte der Europäischen Union – Fragen der Konzeption, Kompetenz und Verbindlichkeit, EuZW 2001, 261.
Callies, C., Gewährleistung von Freiheit und Sicherheit im Lichte unterschiedlicher Staats- und Verfassungsverständnisse, DVBl. 2003, 1096.
Canadian Standing Committee on Citizenship and Immigration, A national Identity Card for Canada?, abrufbar unter http://www.parl.gc.ca/InfocomDoc/Documents/37/2/parlbus/commbus/house/reports/cimmrp06/cimmrp06-e.pdf, Oktober 2003.
Caplan, J. / *Torpey, J.* (Ed.), Documenting Individual Identity. The Development of State Practices in the Modern World, Princeton 2001.
Carl, D. / *Klos, J.*, Inhalt und Reichweite der Kontenwahrheitspflicht nach § 154 AO als Grundlage der steuerlichen Mitwirkungspflicht der Kreditinstitute, DStZ 1995, 296.
Cassese, A., International law, New York 2001.
Chaos Computer Club e.V., Stellungnahme zu den Vorstellungen des Bundesministeriums des Innern zur Terrorismusbekämpfung, 2001 (abrufbar unter http://www.cilip.de/terror/CCC2001 1022.pdf).
Citizenship and Immigration Canada, Tracking Public Perception of Biometrics, abrufbar unter http://www.cic.gc.ca/english/press/03/poll-biometrics-e.pdf, 2003.
Classen, D., Anmerkung zu EuGH, Rs C-117/01 – K.B. ./. National Health Service Pensions Agency, JZ 2004, 513.
Coppel, J. / *O'Neill, A.*, The European Court of Justice: Taking rights seriously?, CMLRev 1992, 669.
Correll, C., Im falschen Körper. Ein Beitrag zur rechtlichen und tatsächlichen Problematik der Transsexualität, NJW 1999, 3372.
Craig, P. / *De Búrca, G.*, EU law. Text, cases, and materials, 3rd Edition, Oxford 2002.
Cremona, J. J., The proportionality principle in the Jurisprudence of the European Court of Human Rights, in: Beyerlin, U. / Bothe, M. / Hofmann, R. / Petersmann, E.-U. (Hrsg.), Recht zwischen Umbruch und Bewahrung. Festschrift für Rudolf Bernhardt, Berlin 1995, 323.
Czybulka, D., Akzeptanz als staatsrechtliche Kategorie?, Die Verwaltung 1993, 27.
Dämmer, H. / *Männel, B.*, Großherzige Ziele, verzagte Schritte. Das GMG: Zwischen mehr Wettbewerb und Überregulierung, Die BKK 2003, 279.
Dästner, C., Neue Formvorschriften im Prozessrecht, NJW 2001, 3469.
Dammann, U. / *Rabenhorst, K.*, Outsourcing und Auftragsdatenverarbeitung, CR 1998, 643.
Dammann, U. / *Simitis, S.*, EG-Datenschutzrichtlinie. Kommentar, Baden-Baden 1997.
Daugman, J., Recognizing Persons by Their Iris Patterns, in: Jain, A. / Bolle, R. / Pankanti, S. (Eds.): Biometrics. Personal Identification in Networked Society, Boston 1999, 103.
Daugman, J., Iriserkennung, in: Behrens, M. / Roth, R., (Hrsg.), Biometrische Identifikation. Grundlagen, Verfahren, Perspektiven, Braunschweig 2001, 129.
Daum, H., Technische Untersuchung und Überwindbarkeit biometrischer Systeme, in: Nolde, V. / Leger, L. (Hrsg.): Biometrische Verfahren. Körpermerkmale als Passwort – Grundlagen, Sicherheit und Einsatzgebiete biometrischer Identifikation, Köln 2002, 183.
Debold & Lux Beratungsgesellschaft für Informationssysteme und Organisation im Gesundheitswesen mbH / *secunet Security Networks AG*, Kommunikationsplattformen im Gesundheitswesen – Kosten-Nutzen-Analyse. Neue Versichertenkarte und elektronisches Rezept, Endbericht, Mai 2001.

Denninger, E., Das Recht auf informationelle Selbstbestimmung und Innere Sicherheit. Folgerungen aus dem Volkszählungsurteil des Bundesverfassungsgerichts, KJ 1985, 215.
Denninger, E. / *Hoffmann-Riem, W.* / *Schneider, H.-P.* / *Stein, E.* (Hrsg.), Kommentar zum Grundgesetz für die Bundesrepublik Deutschland, 3. Auflage, Loseblatt, Stand: August 2002, Neuwied (zitiert als: AK GG-*Bearbeiter*).
Denz, M. D. / *Below, G. C. v.*, Die Gesundheitskarte als Schlüssel zu eHealthcare, Schweizerische Ärztezeitung 2002, 2026.
Der Berliner Beauftragte für Datenschutz und Informationsfreiheit, Jahresbericht 1990, Berlin 1991.
Der Berliner Beauftragter für Datenschutz und Informationsfreiheit, Jahresbericht 1997, Berlin 1998 (abrufbar unter http://www.datenschutz-berlin.de/jahresbe/98/index.htm).
Der Berliner Beauftragter für Datenschutz und Informationsfreiheit, Zum Umgang mit sensitiven Daten gemäß § 3 Abs. 9 BDSG, RDV 2003, 308 (zugl. Jahresbericht 2002, 25 ff., abrufbar unter http://www.datenschutz-berlin.de/jahresbe/02/index.htm).
Der Bundesbeauftragte für den Datenschutz, Auszug aus dem 7. Tätigkeitsbericht, DuD 1985, 87.
Der Bundesbeauftragte für den Datenschutz, 14. Tätigkeitsbericht vom 27. April 1993, BT-Drs. 12/4005, 1993.
Der Bundesbeauftragte für den Datenschutz, 19. Tätigkeitsbericht 2001-2002, abrufbar unter http://www.bfd.bund.de/information/19tb0102.pdf, 2002.
Der Bundesbeauftragte für den Datenschutz, 20. Tätigkeitsbericht 2003-2004, abrufbar unter http://www.bfd.bund.de/information/20tb_broschuere.pdf, 2005.
Der Hamburgische Datenschutzbeauftragte, 16. Tätigkeitsbericht, Hamburg 1998.
Der Hessische Datenschutzbeauftragte, 24. Tätigkeitsbericht, abrufbar unter http://www.datenschutz.hessen.de/tb24/inhalt.htm, 1995.
Der Landesbeauftragte für den Datenschutz Baden-Württemberg, 19. Tätigkeitsbericht, Stuttgart 1998.
Der Landesbeauftragte für den Datenschutz Freie Hansestadt Bremen, Ärztliche Behandlung und Abrechnung der Leistung demnächst nur noch mit Chipkarte?, DuD 1992, 276.
Der Landesbeauftragte für den Datenschutz Freie Hansestadt Bremen, 15. Jahresbericht (Berichtsjahr 1992), Bremen 1993.
Der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht Brandenburg, 11. Tätigkeitsbericht, Kleinmachnow 2002.
Dethloff, J., Die Chipkarte: Ein Instrument der Herrschenden? Ein Plädoyer für die Anonymität, a la Card Symposium 92. The International Card Congress from 22-23 October in Cooperation with Köln/Messe. Manuskript, Köln 1992 (zitiert nach: *Elkeles/Rosenbrock* 1995, 1).
Deutsch, E., Das therapeutische Privileg des Arztes: Nichtaufklärung zugunsten des Patienten, NJW 1980, 1305.
Deutsch, E. / *Spickhoff, A.*, Medizinrecht: Arztrecht, Arzneimittelrecht, Medizinprodukterecht und Transfusionsrecht, 5. Auflage, Berlin 2003.
Deutsche Gesellschaft für Versicherte und Patienten (DGVP), Stellungnahme zum Entwurf eines Gesetzes zur Modernisierung des Gesundheitswesens, Heppenheim 2003.
Deutsches Forum für Kriminalprävention (DFK), Workshop-Dokumentation vom 30. September 2002 in Bonn, 2002.
Deutsches Forum für Kriminalprävention (DFK), Airport-Security – Biometrische Applikationen zur Verbesserung der Sicherheit auf Flughäfen. Ein Diskussionsbeitrag, Bonn 2004 (abrufbar unter http://www.kriminalpraevention.de/download-data.htm).
Devigne, S., Patient à la carte, ZM 2003, 18.
De Witte, B., The Legal Status of the Charter: Vital Question or Non-Issue?, MJ 2001, 81.
Dickhoven, S., Modellgestützte Planung in der Regierungspraxis. Zur Einführung neuer Planungstechniken in der Politik, in: Taeger, J. (Hrsg.), Die Volkszählung, Hamburg 1983, 195.
Die Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen, 16. Tätigkeitsbericht, Düsseldorf 2003 (abrufbar unter http://www.lfd.nrw.de/pressestelle/presse_7_komplett.html).

Dierks, C., Schweigepflicht und Datenschutz in Gesundheitswesen und medizinischer Forschung, München 1993.
Dierks, C. / *Nitz, G.* / *Grau, U.*, Gesundheitstelematik und Recht. Rechtliche Rahmenbedingungen und legislativer Anpassungsbedarf, Frankfurt am Main 2003.
Dietzel, G. T. W., Von eEurope 2002 zur elektronischen Gesundheitskarte: Chancen für das Gesundheitswesen, DÄ 2002, A 1417.
Dietzel, G. T. W., Politische Verantwortung bei der Entwicklung von Gesundheitstelematik und -informationssystemen, Bundesgesundheitsbl. 2003, 267.
Dijk, P. v. / *Hoof, G. J. H. v.*, Theory and Practice of the European Convention on Human Rights, 3rd Edition, Deventer 1998.
Dippoldsmann, P., Bürokratische Herrschaftsinstrumente in der Bundesrepublik und im deutschen Faschismus – ein Vergleich, in: Kutscha, M. / Paech, N. (Hrsg.), Totalerfassung. „Sicherheitsgesetze", Volkszählung, Neuer Personalausweis, Möglichkeiten der Gegenwehr, Köln 1986, 163.
Dittmann, J. / *Mayerhöfer, A.* / *Vielhauer, C.*, Praktische Angriffsmöglichkeiten auf biometrische Systeme, in: Nolde, V. / Leger, L. (Hrsg.): Biometrische Verfahren. Körpermerkmale als Passwort – Grundlagen, Sicherheit und Einsatzgebiete biometrischer Identifikation, Köln 2002, 192.
Dobbertin, H., Digitale Fingerabdrücke. Sichere Hashfunktionen für digitale Signaturen, DuD 1997, 82.
Dolderer, G. / *Garrel, G. v.* / *Müthlein, T.* / *Schlumberger, P.*, Die Auftragsdatenverarbeitung im neuen BDSG, RDV 2001, 223.
Dolzer, R. / *Vogel, K.* / *Graßhof, K.* (Hrsg.), Bonner Kommentar zum Grundgesetz, Loseblattsammlung, Stand: 111. Lieferung Mai 2004, Heidelberg (zitiert als: BK-*Bearbeiter*).
Donnerhacke, L., Anonyme Biometrie, DuD 1999, 151.
Donos, P. K., Datenschutz – Prinzipien und Ziele. Unter besonderer Berücksichtigung der Entwicklung der Kommunikations- und Systemtheorie, Baden-Baden 1998.
Dorf, Y., Zur Interpretation der Grundrechtecharta, JZ 2005, 126.
Dreier, H. (Hrsg.), Grundgesetz. Kommentar, Band I, Art. 1-19, 2. Auflage, Tübingen 2004 (zitiert als: Dreier-*Bearbeiter*).
Dreier, H., Menschenwürde in der Rechtsprechung des Bundesverwaltungsgerichts, in: Schmidt-Aßmann, E. / Sellner, D. / Hirsch, G. / Kemper, G. H. / Lehmann-Grube, H. (Hrsg.), Festgabe 50 Jahre Bundesverwaltungsgericht, Köln 2003, 201.
Dürig, G., Der Grundrechtssatz von der Menschenwürde. Entwurf eines praktikablen Wertsystems der Grundrechte aus Art. 1 Abs. 1 in Verbindung mit Art. 19 Abs. 2 Grundgesetz, AöR 1956, 117.
Dürr, H., Baurecht, Reihe Besonderes Verwaltungsrecht in Baden-Württemberg, 9. Auflage, Baden-Baden 1998.
Duhr, E. / *Naujok, H.* / *Peter, M.* / *Seiffert, E.*, Neues Datenschutzrecht für die Wirtschaft. Erläuterungen und praktische Hinweise zu § 1 bis § 11 BDSG, DuD 2002, 5.
Duttge, G., Was bleibt noch von der Wissenschaftsfreiheit? – Zur Hypertrophie des Datenschutzes, NJW 1998, 1615.
Duve, F., Katalysator gegen den Orwell-Staat, in: Taeger, J. (Hrsg.), Die Volkszählung, Hamburg 1983, 25.
Eaton, J. W., The Privacy Card. A Low Cost Strategy to Combat Terrorism, Lanham 2003.
eEurope Smart Cards Trailblazer 11 Health (eESC/TB11 Health), Open Smart Card Infrastructure for Europe. v2, Volume 1: Application white papers and market oriented background documents, Part 4: Smart Cards as Enabling Technology for Future-Proof Healthcare: a requirement survey, abrufbar unter http://www.eeurope-smartcards.org/Download/01-4.pdf, 2003.
Ehmann, E., Strafbare Fernwartung in der Arztpraxis, CR 1991, 293.
Ehmann, E. / *Helfrich, M.*, EG-Datenschutzrichtlinie. Kurzkommentar, Köln 1999.
Eisenberg, U. / *Puschke, J.* / *Singelnstein, T.*, Überwachung mittels RFID-Technologie. Aspekte der Ausforschung und Kontrolle mit neuartigen Funk-Chips, ZRP 2005, 9.

Eissen, M.-A., The principle of proportionality in the Case-Law of the European Court of Human Rights, in: Macdonald, R. S. J. / Matscher, F. / Petzold, H. (Ed.), The European System for the protection of Human Rights, Dordrecht 1993, 125.

ElGamal, T., A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms, IEEE.IT 1985, 469.

Elkeles, T. / *Rosenbrock, R.*, Chipkarten im Gesundheitswesen. Nutzungsmöglichkeiten für Prävention und Gesundheitsförderung. Discussion Paper P95-203, Berlin 1995 (abrufbar unter http://bibliothek.wz-berlin.de/pdf/1995/p95-203.pdf).

Ellerbrock, B., Ausgeforscht und abgespeichert, in: Taeger, J. (Hrsg.), Die Volkszählung, Hamburg 1983, 10.

Ellger, R., Der Datenschutz im grenzüberschreitenden Datenverkehr, Baden-Baden 1990.

Ellis, R., Roles and Identities – Review an identification of the state of the art. EURESCOM project PROFIT (Potential pRofit Opportunities in the Future ambient InTelligence world), abrufbar unter http://www.eurescom.de/public/projects/P1300-series/p1302/P1302_portal.asp#P1302%20Deliverable%201, 2003.

Endruweit, G., Stichwort Akzeptanz und Sozialverträglichkeit, in: ders. / Trommsdorff, G. (Hrsg.), Wörterbuch der Soziologie, Stuttgart 1989, 9.

Engel-Flechsig, S., „Teledienstedatenschutz". Die Konzeption des Datenschutzes im Entwurf des Informations- und Kommunikationsdienstegesetzes des Bundes, DuD 1997, 8.

Engel-Flechsig, S., Die datenschutzrechtlichen Vorschriften im neuen Informations- und Kommunikationsdienste-Gesetz, RDV 1997, 59.

Eppler, E., Kavalleriepferde beim Hornsignal. Die Krise der Politik im Spiegel der Sprache, Frankfurt am Main 1992.

Erb, U., Volkszählung – zwischen den Interessen von Volk und Staat, in: Appel, R. / Hummel, D. (Hrsg.), Vorsicht Volkszählung!, Köln 1987, 82.

Erikson, E. H., Einsicht und Verantwortung. Die Rolle des Ethischen in der Psychoanalyse, Stuttgart 1964.

Erikson, E. H., Identität und Lebenszyklus. Drei Aufsätze, Frankfurt am Main 1973.

Ernestus, W., JobCard – Schlüssel zur elektronischen Signatur? Ein Fachverfahren könnte den Weg für den Durchbruch der elektronischen Signatur ebnen!, DuD 2004, 404.

Europäische Kommission, Mitteilung der Kommission an das Europäische Parlament und den Rat im Hinblick auf den Europäischen Rat in Thessaloniki. Entwicklung einer gemeinsamen Politik in den Bereichen illegale Einwanderung, Schleuserkriminalität und Menschenhandel, Außengrenzen und Rückführung illegal aufhältiger Personen, KOM(2003) 323 endgültig, abrufbar unter http://europa.eu.int/eur-lex/de/com/cnc/2003/com2003_ 0323de 01.pdf.

Europäische Kommission, Mitteilung der Kommission zur Einführung der europäischen Krankenversicherungskarte, KOM(2003) 73 endgültig, abrufbar unter http://europa.eu.int/eur-lex/de/com/cnc/2003/com2003_0073de01.pdf.

Europäische Kommission, Vorschlag für eine Verordnung des Rates über Normen für Sicherheitsmerkmale und Biometrie in Pässen der EU-Bürger, KOM(2004) 116 endgültig, abrufbar unter http://europa.eu.int/eur-lex/de/com/pdf/2004/com2004_0116de01.pdf.

Evers, J. / *Kiene, L. H.*, Datenschutzrechtliche Folgen der Ausgliederung von Dienstleistungen. Einwilligungserklärung und Auftragsdatenverarbeitung, DuD 2003, 341.

Faber, M., Verrechtlichung – ja, aber immer noch kein „Grundrecht"! – Zwanzig Jahre informationelles Selbstbestimmungsrecht, RDV 2003, 278.

Fenner, M., Ready for the big Leagues?, Card Technology 9/2003, abrufbar unter http://www.cardtechnology.com/cgi-bin/readstory.pl?story=20030902CTMC484.xml, 2003.

Ferreiro, F. G., The Spanish Social Security Smart Card (TASS), in: Fluhr, M. (Hrsg.), Neue und bewährte Applikationsfelder der Chipkarte. Kongressdokumentation und Katalog, OMNICARD 2004, Berlin 2004, 278.

Fiedler, A. / *Bickenbach, H.*, ISIS-MTT: Investitionen in die Zukunft. Verstärkte Ausrichtung auf den Anwendernutzen, DuD 2005, 149.

Fischer, G. / *Hitz, F.* / *Laskowski, R.* / *Walter, B.*, Bundesgrenzschutzgesetz und Zwangsanwendung nach Bundesrecht, 2. Auflage, Stuttgart 1996.
Fischer, R., Das Demokratiedefizit bei der Rechtsetzung durch die Europäische Gemeinschaft, Münster 2001.
Fischer-Dieskau, S., Der Entwurf zum Justizkommunikationsgesetz aus Sicht des Signaturrechts, MMR 2003, 704.
Fischer-Dieskau, S. / *Gitter, R.* / *Hornung, G.*, Die Beschränkung des qualifizierten Zertifikats. § 7 Abs. 1 Nr. 7 SigG als wichtiges Mittel der Risikokalkulation, MMR 2003, 384.
Fischer-Dieskau, S. / *Gitter, R.* / *Paul, S.* / *Steidle, R.*, Elektronisch signierte Dokumente als Beweismittel im Zivilprozess, MMR 2002, 709.
Fischer-Dieskau, S. / *Roßnagel, A.* / *Steidle, R.*, Beweisführung am seidenen Bit-String? Die Langzeitaufbewahrung elektronischer Signaturen auf dem Prüfstand, MMR 2004, 451.
Flynn, L., Case C-13/94, P. v. S. and Cornwall County Council, CMLRev 1996, 367.
Fox, D., Krankenversichertenkarte, DuD 1997, 600.
Fox, D., Entzaubert, DuD 2002, 450.
Frank, H.-H., 100 Jahre Daktyloskopie in Deutschland, Die Polizei 2004, 336.
Fromme, F. K., Ein neues Grundrecht ist erfunden, FAZ v. 17.12.1983, 12.
Frowein, J. A. / *Peukert, W.*, Europäische Menschenrechtskonvention. EMRK-Kommentar, 2. Auflage, Kehl 1996 (zitiert als: Frowein/Peukert-*Bearbeiter*).
Fuchs-Heinitz, W. / *Lautmann, R.* / *Rammstedt, O.* / *Wienold, H.* (Hrsg.), Lexikon zur Soziologie, 3. Auflage, Opladen 1995.
Fuest, B., Datenschutzrechtliche Probleme beim Einsatz von Patientenchipkarten, Mainz 1999.
Fuhrmann, H., Vertrauen im Electronic Commerce. Rechtliche Gestaltungsmöglichkeiten unter besonderer Berücksichtigung verbindlicher Rechtsgeschäfte und des Datenschutzes, Baden-Baden 2001.
Garstka, H., Datenschutz in Praxisnetzen aus Sicht des Datenschutzbeauftragten, ZaeFQ 1999, 781.
Garstka, H., Terrorismusbekämpfung und Datenschutz – Zwei Themen im Konflikt, NJ 2002, 524.
Gassen, D., Digitale Signaturen in der Praxis. Grundlagen, Sicherheitsfragen und normativer Rahmen, Köln 2003.
Geis, I., Individualrechte in der sich verändernden europäischen Datenschutzlandschaft, CR 1995, 171.
Geis, I., Rechtsfragen der Telearchivierung medizinischer Dokumente, DuD 1997, 582.
Geis, I., Schutz von Kundendaten im E-Commerce und elektronische Signatur, RDV 2000, 208.
Geis, I., Elektronische Kommunikation mit der öffentlichen Verwaltung, K&R 2003, 21.
Geis, M.-E., Der Kernbereich des Persönlichkeitsrechts. Ein Plädoyer für die „Sphärentheorie", JZ 1991, 112.
Gentili, M., Italian Electronic Identity Card. Principle and architecture, abrufbar unter http://www.electronic-identity.org/download/italian_eid.pdf, 2001.
Gesellschaft für Datenschutz und Datensicherung (GDD) e.V., Handbuch Datenschutz und Datensicherheit im Gesundheits- und Sozialwesen. Spezielle Probleme des Datenschutzes und der Datensicherheit im Bereich des Gesundheits- und Sozialwesens in Deutschland, Teil I: (Datenschutz) bearbeitet von C. Bake, J. Erdmann, H. Friedrich, H. Koch, P. Münch, B. Tietze und J. Wünscher, Teil II (Datensicherheit) bearbeitet von B. Blobel und K. Engel, Frechen-Königsdorf 2002.
Gesellschaft für Informatik e.V. (GI), Stellungnahme zum Gesetzentwurf „Formvorschriften des Privatrechts", DuD 2001, 38.
Gesellschaft für Informatik (GI) / *Informationstechnische Gesellschaft im VDE (ITG)*, Memorandum zur Förderung des elektronischen Rechts- und Geschäftsverkehrs vom 3.4.2003, DuD 2003, 763.
Geulen, R., Rechtliche Probleme der Volkszählung 1983, in: Taeger, J. (Hrsg.), Die Volkszählung, Hamburg 1983, 107.

Giesecke & Devrient, Smart Cards and Biometrics – A Crucial Element of Security Solutions. White paper on smart cards and biometrics, abrufbar unter http://www.gi-de.com/pls/portal/MAIA.display_custom_items.DOWNLOAD_SEEALSO_FILE?p_ID=5537, 2003.
Giesen, D., Arzthaftungsrecht im Umbruch (II): Die ärztliche Aufklärungspflicht in der Rechtsprechung seit 1974, JZ 1982, 391.
Gill, M. / *Spriggs, A.*, Assessing the impact of CCTV. Home Office Research Study 292, abrufbar unter http://www.homeoffice.gov.uk/rds/pdfs05/hors292.pdf, 2005.
Gitter, R. / *Strasser, M.*, Ausweise als Träger für Signaturverfahren, DuD 2005, 74.
Goerke, H., Ärztliche Schweigepflicht einst und jetzt, ZaeFQ 1999, 716.
Gössner, R., Die Legalisierung der Geheim-Polizei, in: Kutscha, M. / Paech, N. (Hrsg.), Totalerfassung. „Sicherheitsgesetze", Volkszählung, Neuer Personalausweis, Möglichkeiten der Gegenwehr, Köln 1986, 115.
Gössner, R. / *Herzog, U.*, Im Schatten des Rechts. Methoden einer neuen Geheim-Polizei, Köln 1984.
Goetz, C. F.-J., Online-Sicherheit von Patientendaten. Telematische Sicherheitskonzepte für niedergelassene Ärzte, Braunschweig 2001.
Goetz, C. F.-J., Telematik im Gesundheitswesen. Herausforderungen für eine Modernisierung, DÄ 2003, A 756.
Gola, P., Die Erhebung und Verarbeitung „besonderer Arten personenbezogener Daten" im Arbeitsverhältnis, RDV 2001, 125.
Gola, P. / *Klug, C.*, Grundzüge des Datenschutzrechts, München 2003.
Gola, P. / *Klug, C.*, Videoüberwachung gemäß § 6b BDSG – Anmerkungen zu einer verunglückten Gesetzeslage, RDV 2004, 65.
Gola, P. / *Schomerus, R.*, BDSG-Kommentar, 8. Auflage, München 2005.
Goldschmidt, A. J. W. / *Goetz, C. F.-J.* / *Hornung, G.*, Die elektronische Gesundheitskarte. Recht, Technologie, Infrastruktur und Ökonomie, in: Fischer, H. / Gerhardt, E.-P. / Greulich, A. (Hrsg.), Management Handbuch Krankenhaus, Loseblatt, Heidelberg, Stand: August 2004, 790 (zugl. gekürzter Vorabdruck: *Goldschmidt, A. J. W.* / *Goetz, C. F.-J.* / *Hornung, G.*, Die Gesundheitskarte. Teil 2: Ausgewählte rechtliche, technische und ökonomische Gesichtspunkte, mdi 2/2004, 61).
Golembiewski, C. / *Probst, T.*, Datenschutzrechtliche Anforderungen an den Einsatz biometrischer Verfahren in Ausweispapieren und bei ausländerrechtlichen Identitätsfeststellungen (Gutachten des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein für das Büro für Technikfolgenabschätzung beim Deutschen Bundestag), abrufbar unter http://www.datenschutzzentrum.de/download/Biometrie_Gutachten_Print.pdf, Kiel 2003.
Gounalakis, G. / *Mand, E.*, Die neue EG-Datenschutzrichtlinie – Grundlagen einer Umsetzung in nationales Recht (I), CR 1997, 431.
Gounalakis, G. / *Rhode, L.*, Persönlichkeitsschutz im Internet: Grundlagen und Online-Spezifika, München 2002.
Grabenwarter, C., Europäische Menschenrechtskonvention, München 2003.
Grabenwarter, C., Auf dem Weg in die Grundrechtsgemeinschaft?, EuGRZ 2004, 563.
Gräfin von Westerholt, M. / *Döring, W.*, Datenschutzrechtliche Aspekte der Radio Frequency Identification. Ein „Virtueller Rundgang" durch den Supermarkt der Zukunft, CR 2004, 710.
Grätzel v. Grätz, P., Elektronische Gesundheitskarte teurer als erwartet?, abrufbar unter http://www.heise.de/tp/deutsch/inhalt/lis/17421/1.html, 2004a.
Grätzel v. Grätz, P., An Medikamenten sterben noch immer zu viele Menschen, abrufbar unter http://www.heise.de/tp/deutsch/inhalt/lis/17870/1.html, 2004b.
Grätzel v. Grätz, P. (Hrsg.), Vernetzte Medizin. Patienten-Empowerment und Netzinfrastrukturen in der Medizin des 21. Jahrhunderts, Hannover 2004c.
Gridl, R., Datenschutz in globalen Telekommunikationssystemen. Eine völker- und europarechtliche Analyse der vom internationalen Datenschutzrecht vorgegebenen Rahmenbedingungen, Baden-Baden 1999.

Grimm, R., Datenverarbeitung im Internet, in: Roßnagel, A. / Banzhaf, J. / Grimm, R., Datenschutz im Electronic Commerce, Heidelberg 2003.
Groebner, V., Describing the Person, Reading the Signs in Late Medieval and Renaissance Europe: Identity Papers, Vested Figures, and the Limits of Identification 1400-1600, in: Caplan, J. / Torpey, J. (Ed.), Documenting Individual Identity. The Development of State Practices in the Modern World, Princeton 2001, 15.
Groebner, V., Der Schein der Person: Steckbrief, Ausweis und Kontrolle im Europa des Mittelalters, München 2004.
Grohmann, H., Geschichte und Zukunft der Volkszählung in Deutschland, Berliner Statistik – Monatsschrift 2000, 216.
Gropp, W., Anmerkung zu BayObLG, Urteil v. 8.11.1994 – 2 St RR 157/94 (JR 1996, 476), JR 1996, 478.
Grupp, K. / *Stelkens, U.*, Zur Berücksichtigung der Gewährleistungen der Europäischen Menschenrechtskonvention bei der Auslegung deutschen Rechts. Zugleich Anmerkung zu BVerfG, Beschluss v. 14.10.2004 - 2 BvR 1481/04, JZ 2005, 133.
Güllner, M., Von der Fiktion der Unfehlbarkeit. Kritische Anmerkungen zum Konzept der amtlichen Statistik, in: Taeger, J. (Hrsg.), Die Volkszählung, Hamburg 1983, 186.
Gundermann, L., E-Commerce trotz oder durch Datenschutz?, K&R 2000, 225.
Gundermann, L. / *Köhntopp, M.*, Biometrie zwischen Bond und Big Brother. Technische Möglichkeiten und rechtliche Grenzen, DuD 1999, 143.
Gusy, C., Grundrechtsschutz vor staatlichen Informationseingriffen, VerwA 1983, 91.
Gusy, C., Der Schutz der Privatsphäre in der Europäischen Menschenrechtskonvention Art. 8, DVR 1984, 289.
Gusy, C., Polizeirecht, 5. Auflage, Tübingen 2003.
Hadley, C., Your personal passport, EMBO reports 2004, 124.
Häberle, P., Das Menschenbild im Verfassungsstaat, Berlin 1988.
Häberle, P., Die europäische Verfassungsstaatlichkeit, KritV 1995, 298.
Hager, G., Mediation und Recht, ZKM 2003, 52.
Hall, J. A. Y. / *Kimura, D.*, Dermatoglyphic Asymmetric and Sexual Orientation in Men, Behavioral Neuroscience 1994, 1203.
Halley, J., Sexual Orientation and the Politics of Biology. A Critique of the Argument from Immutability, Stanford Law Review 1994, 503.
Hammer, V., „Elektronische Signaturen“, DuD 1993, 636.
Hammer, V., Digitale Signaturen mit integrierter Zertifikatkette – Gewinne für den Urheberschafts- und Autorisierungsnachweis, in: Brüggemann, H. H. / Gerhardt-Häckl, W. (Hrsg.), Verlässliche IT-Systeme. Proceedings der GI-Fachtagung VIS ’95, Braunschweig 1995, 265.
Hammer, V. / *Pordesch, U.* / *Roßnagel, A.*, Betriebliche Telefon- und ISDN-Anlagen rechtsgemäß gestalten, Berlin 1993.
Hammer, V. / *Pordesch, U.* / *Roßnagel, A.* / *Schneider, M. J.*, Vorlaufende Gestaltung von Telekooperationstechnik – am Beispiel von Verzeichnisdiensten, Personal Digital Assistants und Erreichbarkeitsmanagement in der Dienstleistungsgesellschaft, GMD-Studien Nr. 235, Sankt Augustin 1994.
Hammer, V. / *Roßnagel, A.*, Die Informatisierung des Gesundheitswesens, in: Roßnagel, A. (Hrsg.), Freiheit im Griff, Stuttgart 1989, 121.
Hammer, V. / *Schneider, M. J.*, Szenario künftiger Sicherungsinfrastrukturen für Telekooperation, in: Hammer, V. (Hrsg.), Sicherungsinfrastrukturen. Gestaltungsvorschläge für Technik, Organisation und Recht, Berlin 1995, 1.
Hanebeck, A., Bundesverfassungsgericht und Demokratieprinzip. Zwischen monistischem und pluralistischem Demokratieverständnis, DÖV 2004, 901.
Hansen, M. / *Krasemann, H.* / *Rost, M.* / *Genghini, R.*, Datenschutzaspekte von Identitätsmanagementsystemen. Recht und Praxis in Europa, DuD 2003, 551.
Hansen, M. / *Wiese, M.*, RFID – Radio Frequency Identification, DuD 2004, 109.

Harnier, A. v., Organisationsmöglichkeiten für Zertifizierungsstellen nach dem Signaturgesetz, Baden-Baden 2000.
Harnischfeger, M. / *Kolo, C.* / *Zoche, P.*, Literaturauswertung zum Thema Medienakzeptanz. Arbeitspapier ISI Mkomp97-02.0 im Rahmen des Verbundvorhabens "Entwicklung zukunftsträchtiger Mediendienste" (DeMeS), Modul M-3. Karlsruhe 1997.
Harris, D. J., Cases and materials on international law, 5th Edition, London 1998.
Harris, D. J. / *O'Boyle, M.* / *Warbrick, C.*, Law of the European Convention on Human Rights, London 1995.
Hart, H. L. A., The concept of Law, Oxford 1961. (Im Text zitiert nach der deutschen Übersetzung: Der Begriff des Rechts, Frankfurt am Main 1973).
Hassemer, W., Zeit zum Umdenken, DuD 1995, 448.
Hattenhauer, H., Rechtsakzeptanz – Gesetzesgehorsam – Homogenität, in: Pichler, J. W. (Hrsg.), Rechtsakzeptanz und Handlungsorientierung, Wien 1998, 91.
Hauck / *Noftz*, Sozialgesetzbuch. SGB III, Arbeitsförderung, Kommentar, Loseblatt, Stand: 41. Lieferung August 2004, Berlin (zitiert als: Hauck/Noftz-*Bearbeiter*).
Hauck-Scholz, P., Verfassungskonformität der Volkszählung 1987?, NJW 1987, 2769.
Hecker, F., Die Akzeptanz und Durchsetzung von Systemtechnologien. Marktbearbeitung und Diffusion am Beispiel der Verkehrstelematik, Saarbrücken 1997.
Heintschel-Heinegg, B. / *Stöckel, H.* (Hrsg.), KMR. Kommentar zur Strafprozessordnung, Loseblatt, Stand: 37. Lieferung Mai 2004, München (zitiert als: KMR-*Bearbeiter*).
Hemmi, A., „Es muss wirksam werben, wer nicht will verderben". Kontrastive Analyse von Phraseologismen in Anzeigen-, Radio- und Fernsehwerbung, Lang 1994.
Henke, F., Die Datenschutzkonvention des Europarats, Frankfurt am Main 1986.
Herchenbach, J., Datenschutz und digitale Signatur, K&R 2000, 235.
Hermeler, A. E., Rechtliche Rahmenbedingungen der Telemedizin. Dargestellt am Beispiel der Elektronischen Patientenakte sowie des Outsourcing von Patientendaten, München 2000.
Herold, H., Interview mit der Zeitschrift „Bürgerrechte und Polizei" (CILIP), in: Appel, R. / Hummel, D. / Hippe, W. (Hrsg.), Die neue Sicherheit. Vom Notstand zur Sozialen Kontrolle, Köln 1988, 65.
Herzog, R., Von der Akzeptanz des Rechts, in: Rüthers, B. / Stern, K. (Hrsg.), Freiheit und Verantwortung im Verfassungsstaat. Festgabe zum 10jährigen Jubiläum der Gesellschaft für Rechtspolitik, München 1984, 127.
Hesse, K., Die verfassungsgerichtliche Kontrolle der Wahrnehmung grundrechtlicher Schutzpflichten des Gesetzgebers, in: Däubler-Gmelin, H. / Kinkel, K. / Meyer, H. / Simon, H. (Hrsg.), Gegenrede: Aufklärung – Kritik – Öffentlichkeit. Festschrift für Ernst Gottfried Mahrenholz, Baden-Baden 1994, 541.
Hesse, K., Grundzüge des Verfassungsrechts der Bundesrepublik Deutschland, 20. Auflage, Heidelberg 1995.
Heußner, H., Das informationelle Selbstbestimmungsrecht des Grundgesetzes als Schutz des Menschen vor totaler Erfassung, BB 1990, 1281.
Heydwolff, A. v. / *Anderson, R.*, Eine klare Sicherheitspolitik für klinische Informationssysteme, DuD 1997, 569.
Hiddemann, T.-C. / *Muckel, S.*, Das Gesetz zur Modernisierung der gesetzlichen Krankenversicherung, NJW 2004, 7.
Hill, H., Akzeptanz des Rechts – Notwendigkeit eines besseren Politikmanagements, JZ 1988, 377.
Hill, H., Das Verhältnis des Bürgers zum Gesetz, DÖV 1988, 666.
Hillebrand, A., Sicherheit im Internet aus Sicht der Nutzer. Eine Analyse auf der Basis von Ergebnissen einer Online-Umfrage, DuD 1998, 218.
Hoenike, M. / *Hülsdunk, L.*, Outsourcing im Versicherungs- und Gesundheitswesen ohne Einwilligung?, MMR 2004, 788.
Hoeren, T. / *Sieber, U.*, Handbuch Multimedia-Recht. Rechtsfragen des elektronischen Geschäftsverkehrs, Loseblatt, Stand: Mai 2003, München (zitiert als: Hoeren/Sieber-*Bearbeiter*).

Hoffmann, G., Im Jahrzehnt der Großen Brüder. Orwells „1984“ aktueller denn je. Vom Alptraum zur Realität, Frankfurt am Main 1983.
Hoffmann-Riem, W., Reform des allgemeinen Verwaltungsrechts als Aufgabe – Ansätze am Beispiel des Umweltschutzes, AöR 1990, 400.
Hoffmann-Riem, W., Informationelle Selbstbestimmung in der Informationsgesellschaft. Auf dem Weg zu einem neuen Konzept des Datenschutzes, AöR 1998, 513.
Hoffmann-Riem, W., Informationelle Selbstbestimmung als Grundrecht kommunikativer Entfaltung, in: Bäumler, H. (Hrsg.), Der neue Datenschutz. Datenschutz in der Informationsgesellschaft von morgen, Neuwied 1998, 11.
Hollmann, A., Aktuelle Datenschutzprobleme im medizinischen Bereich aus der Sicht der Ärztekammer, in: Kilian, W. / Porth, A. J. (Hrsg.), Juristische Probleme der Datenverarbeitung in der Medizin. GMDS/GRVI Datenschutz-Workshop 1979, Berlin 1979, 34.
Holtfort, W., Denunziationspflicht und Bewegungskontrolle, in: Kutscha, M. / Paech, N. (Hrsg.), Totalerfassung. „Sicherheitsgesetze“, Volkszählung, Neuer Personalausweis, Möglichkeiten der Gegenwehr, Köln 1986, 109.
Home Affairs Committee of the House of Commons, Identity Cards. Fourth Report of Session 2003-04, Volume I: Report, together with formal minutes, abrufbar unter http://www.publications.parliament.uk/pa/cm200304/cmselect/cmhaff/130/130.pdf, 2004.
Hopp, C. / *Grünvogel, A.*, Pseudonyme nach dem deutschen und österreichischen Signaturgesetz. Datenschutzrechtliche Aspekte rechtsvergleichend betrachtet, DuD 2002, 79.
Hornung, G., Datenschutz für Chipkarten. Die Anwendung des § 6c BDSG auf Signatur- und Biometriekarten, DuD 2004, 15.
Hornung, G., Zwei runde Geburtstage: Das Recht auf informationelle Selbstbestimmung und das World Wide Web, MMR 2004, 3.
Hornung, G., Der Personenbezug biometrischer Daten. Zugleich eine Erwiderung auf Saeltzer (DuD 2004, 218 ff.), DuD 2004, 429.
Hornung, G., Fortentwicklung des datenschutzrechtlichen Regelungssystems des Europarats. Das Zusatzprotokoll über Kontrollstellen und grenzüberschreitenden Datenverkehr ist in Kraft getreten, DuD 2004, 719.
Hornung, G., Biometrische Systeme – Rechtsfragen eines Identifikationsmittels der Zukunft, KJ 2004, 344.
Hornung, G., Der zukünftige Einsatz von Chipkarten im deutschen Gesundheitswesen, in: Horster, P. (Hrsg.), D-A-CH Security 2004, Klagenfurt 2004a, 226.
Hornung, G., Biometric Identity Cards: Technical, Legal, and Policy Issues, in: Paulus, S. / Pohlmann, N. / Reimer, H. (Ed.), ISSE 2004: Securing Electronic Business Processes, Wiesbaden 2004b, 47.
Hornung, G., „Digitale“ Ausweise im Ausland. Zum Stand der internationalen Entwicklung bei Chipkartenausweisen, DuD 2005, 62.
Hornung, G. / *Goetz, C. F.-J.* / *Goldschmidt, A. J. W.*, Die künftige Telematik-Rahmenarchitektur im Gesundheitswesen. Recht, Technologie, Infrastruktur und Ökonomie, WI 2005, 171.
Hornung, G. / *Roßnagel, A.*, Die JobCard – „Killer-Applikation“ für die elektronische Signatur?, K&R 2004, 263.
Hornung, G. / *Steidle, R.*, Biometrie am Arbeitsplatz – sichere Kontrollverfahren versus ausuferndes Kontrollpotential, AuR 2005, 201.
Huber, B., Die Änderung des Ausländer- und Asylrechts durch das Terrorismusbekämpfungsgesetz, NVwZ 2002, 787.
Huber, E., Politiker fragen – Bürger antworten nicht! Die Boykottbewegung gegen die Volkszählung, in: Taeger, J. (Hrsg.), Die Volkszählung, Hamburg 1983, 254.
Human Rights Committee, General Comment 16/32 on Art. 17, UN-Doc. HRI/GEN/1/Rev. 1, S. 21, abrufbar unter http://heiwww.unige.ch/humanrts/gencomm/hrcom16.htm, 1994.
Informationstechnische Servicestelle der Gesetzlichen Krankenversicherung GmbH (ITSG), Das JobCard-Verfahren, abrufbar unter http://www.itsg.de/download/BroschuereJobcard.pdf, 2003.

Inhester, M., Rechtliche Konsequenzen des Einsatzes von Bildarchivierungs- und Kommunikationssystemen (PACS), NJW 1995, 685.

Initiative D21, Informationsgesellschaft: Regierung muss Schrittmacher werden. Presseerklärung 52/2002 vom 30.9.2002, abrufbar unter http://www.initiatived21.de/news/pages/show.prl?params=keyword%3DPersonalausweis%26all%3D1%26type%3D10%26laufzeit%3D0&id=11410&currPage=1.

Institute for Prospective Technological Studies (IPTS), Security and Privacy for the Citizen in the Post-September 11 Digital Age: A prospective Overview. Report to the European Parliament Committee on Citizens Freedoms and Rights, Justice and Home Affairs (LIBE), abrufbar unter http://www.jrc.es/home/publications/publication.cfm?pub=1118, 2003.

International Biometric Group, White House OSTP Biometric Report Brief: A Visa Issuance/Border Crossing Case Study, 2003.

International Civil Aviation Organisation (ICAO), Doc 9303: Machine Readable Travel Documents. Part 1: Machine Readable Passports. 5fth Edition, 2003a ; Part 2: Visa, 1994; Part 3: Size 1 and Size 2 Machine Readable Official Travel Documents. 2nd Edition, 2002.

International Civil Aviation Organisation (ICAO), PKI Digital Signatures for Machine Readable Travel Documents. Technical Report, Version 4.0, 19. April 2003b, abrufbar unter http://www.icao.int/mrtd/Home/Index.cfm.

International Civil Aviation Organisation (ICAO), Biometrics Deployment of Machine Readable Travel Documents. Technical Report, Version 2.0, 2004a, abrufbar unter http://www.icao.int/mrtd/Home/Index.cfm.

International Civil Aviation Organisation (ICAO), Annex I: Use of Contactless Integrated Circuits in Machine Readable Travel Documents, Version 4.0, 2004b, abrufbar unter http://www.icao.int/mrtd/Home/Index.cfm.

International Civil Aviation Organisation (ICAO), Development of a Logical Data Structure – LDS for optional Capacity Expansion Technologies. Technical Report, Version 1.7, 2004c, abrufbar unter http://www.icao.int/mrtd/Home/Index.cfm.

International Civil Aviation Organisation (ICAO), PKI for Machine Readable Travel Documents offering ICC Read-Only Access, Version 1.1, 2004d, abrufbar unter http://www.icao.int/mrtd/Home/Index.cfm.

Isensee, J. / *Kirchhof, P.* (Hrsg.), Handbuch des Staatsrechts der Bundesrepublik Deutschland, Heidelberg. Band 1: Grundlagen von Staat und Verfassung, 1987; Band 2, Verfassungsstaat, 3. Auflage 2004; Band 3: Das Handeln des Staates, 2. Auflage 1996; Band 5: Allgemeine Grundrechtslehren, 2. Auflage 2000; Band 6: Freiheitsrechte, 2. Auflage 2001; Band 7: Normativität und Schutz der Verfassung, Internationale Beziehungen, 1992 (zitiert als: *Bearbeiter*, HdbStR).

Iwansky, P., Datenschutzrechtliche Probleme von Chipkarten am Beispiel der geplanten Patientenkarte unter besonderer Berücksichtigung der europäischen Entwicklung, Berlin 1999.

Jacob, J., „Ist die Novellierung des BDSG gescheitert?“ – Perspektiven im Hinblick auf den globalen Datenverkehr, RDV 1999, 1.

Jacob, J., Perspektiven des neuen Datenschutzrechts. Zur Zukunft des Bundesdatenschutzgesetzes, DuD 2000, 5.

Jacob, J. / *Heil, H.*, Datenschutz im Spannungsfeld von staatlicher Kontrolle und Selbstregulierung, in: Bizer, J. / Lutterbeck, B. / Rieß, J. (Hrsg.), Umbruch von Regelungssystemen in der Informationsgesellschaft. Freundesgabe für Alfred Büllesbach, Stuttgart 2002, 213.

Jacobs, F. G., Human rights in the European Union: the role of the Court of Justice, E.L.Rev. 2001, 331.

Jähnke, B. / *Laufhütte, H. W.* / *Odersky, W*. (Hrsg.), Strafgesetzbuch. Leipziger Kommentar, Großkommentar, Erster Band: Einleitung; §§ 1 bis 31, 11. Auflage, Berlin 2003 (zitiert als: LK-*Bearbeiter*).

Jain, A. K. / *Bolle, R.* / *Pankanti, S.*, Introduction to Biometrics, in: dies. (Eds.), Biometrics. Personal Identifikation in Networked Society, Boston 1999, 1.

Janke, M., Die „Parkinson-Card", eine biometrische SmartCard mit integriertem Fingerprint Sensor, in: Nolde, V. / Leger, L. (Hrsg.): Biometrische Verfahren. Körpermerkmale als Passwort – Grundlagen, Sicherheit und Einsatzgebiete biometrischer Identifikation, Köln 2002, 203.
Jarass, H. D., Das allgemeine Persönlichkeitsrecht im Grundgesetz, NJW 1989, 857.
Jarass, H. D. / *Pieroth, B.*, Grundgesetz für die Bundesrepublik Deutschland. Kommentar, 7. Auflage, München 2004 (zitiert als: Jarass/Pieroth-*Bearbeiter*).
Jaufmann, D. / *Kistler, E.* (Hrsg.), Einstellungen zum technischen Fortschritt. Technikakzeptanz im nationalen und internationalen Vergleich, Frankfurt am Main 1991.
Jay, R. / *Hamilton, A.*, Data protection law and practice, 2nd Edition, London 2002.
Jentsch, H.-J., Der Rechtsstaat – von vielen ersehnt, von wenigen angenommen. Ein Plädoyer für seine Akzeptanz, ZRP 1995, 9.
Jescheck, H.-H. / *Ruß, W.* / *Willms, G.* (Hrsg.), Strafgesetzbuch. Leipziger Kommentar, Großkommentar, Fünfter Band: §§ 185 bis 262, 10. Auflage, Berlin 1989 (zitiert als: LK-*Bearbeiter*).
Jodda, B., Bostons Gesichtserkennung versagt – im Geheimen, abrufbar unter http://www.heise.de/tp/deutsch/inhalt/te/15551/1.html, 2003.
Joint Research Center of the European Commission (JRC) / *Institute for Prospective Technological Studies (IPTS)*, Biometrics at the Frontiers: Assessing the Impact on Society, abrufbar unter ftp://ftp.jrc.es/pub/EURdoc/eur21585en.pdf, 2005.
Jürgens, U., Datenschutzrechtliche und sicherheitstechnische Anforderungen an IT-Systeme im medizinischen Bereich (Stand: Mai 2003), abrufbar unter http://www.datenschutzzentrum.de/material/themen/gesund/dsichmed.htm, 2003.
Junginger, M. / *Beek, M. v.*, Biometrie in einem automatischen Grenzkontrollprojekt. Ein Erfahrungsbereicht über den Entscheidungsprozess am Flughafen Schipol in Amsterdam, in: Nolde, V. / Leger, L. (Hrsg.): Biometrische Verfahren. Körpermerkmale als Passwort – Grundlagen, Sicherheit und Einsatzgebiete biometrischer Identifikation, Köln 2002, 218.
Justi, J. H. G. v., Natur und Wesen der Staaten als der Quelle aller Regierungswissenschaften und Gesetze, Mitau 1771 (Neudruck Aalen 1969).
Kaiser, E., Der Mensch muss einen Ausweis haben. Gedichte, Rosdorf 1983.
Kaltenbrunner, G.-K., Vorwort, in: ders. (Hrsg.), Über die Gewalt. Kommt das Faustrecht wieder?, Freiburg 1986, 7.
Kant, I., Grundlegung zur Metaphysik der Sitten, 1795 (zitiert nach: Kant's gesammelte Schriften, hrsg. von der Königlich Preußischen Akademie der Wissenschaften, Band IV, Berlin 1911).
Kant, I., Die Metaphysik der Sitten. Zweiter Theil: Metaphysische Anfangsgründe der Tugendlehre, 1797 (zitiert nach: Kant's gesammelte Schriften, hrsg. von der Königlich Preußischen Akademie der Wissenschaften, Band VI, Berlin 1907)
Kartte, J., Beitrag zur elektronischen Gesundheitskarte auf der OMNICARD 2004, in: Fluhr, M. (Hrsg.), Neue und bewährte Applikationsfelder der Chipkarte. Kongressdokumentation und Katalog, OMNICARD 2004, Berlin 2004, 212.
Kauß, U., Das neue Ausweissystem – Eine Lücke wird geschlossen, in: Taeger, J. (Hrsg.), Der neue Personalausweis, Hamburg 1984, 41.
Kelter, H. / *Wittmann, S.*, Radio Frequency Identification – RFID. Chancen und Risiken des RFID-Einsatzes, DuD 2004, 331.
Kempfler, K. F., Die Allgemeine Erklärung der Menschenrechte: Grundlage des modernen Menschenrechtsschutzes – Eine Einführung, JA 2004, 577.
Kent, S. T. / *Millet, L. I.* (Ed.), IDs – not that easy. Questions about nationwide identity systems, Washington D.C. 2002.
Kent, S. T. / *Millet, L. I.*, Who Goes There? Authentication trough the Lens of Privacy, Washington D.C. 2003.
Kersten, S., Datenschutz in der Medizin. Aktuelle Problemfelder, CR 1989, 1020.
Keupp, H., Diskursarena Identität: Lernprozesse in der Identitätsforschung, in: *ders.* / *Höfer, R.* (Hrsg.), Identitätsarbeit heute. Klassische und aktuelle Perspektiven der Identitätsforschung, Frankfurt am Main 1997, 11.

Keupp, H., Fragmente oder Einheit? Wie heute Identität geschaffen wird, in: Landeshauptstadt München, Stelle für interkulturelle Zusammenarbeit (Hrsg.), Baustelle Identität. Zu Sanierungsarbeiten an einem beschädigten Konstrukt. Dokumentation einer Fachtagung am 8. März 2001, München 2001

Keupp, H. / *Ahbe, T.* / *Gmür, W.* / *Höfer, R.* / *Mitzscherlich, B.* / *Kraus, W.* / *Straus, F.*, Identitätskonstruktionen. Das Patchwork der Identitäten in der Spätmoderne, Hamburg 1999.

Keupp, H. / *Höfer, R.*, Vorwort, in: dies. (Hrsg.), Identitätsarbeit heute. Klassische und aktuelle Perspektiven der Identitätsforschung, Frankfurt am Main 1997, 7.

Kilian, W., Verfügungsberechtigung über medizinische Daten, in: ders. / Porth, A. J. (Hrsg.), Juristische Probleme der Datenverarbeitung in der Medizin. GMDS/GRVI Datenschutz-Workshop 1979, Berlin 1979, 119.

Kilian, W., Rechtliche Aspekte der digitalen medizinischen Archivierung von Röntgenunterlagen, NJW 1987, 695.

Kilian, W., Rechtliche Aspekte bei Verwendung von Patientenchipkarten, NJW 1992, 2313.

Kilian, W. / *Heussen, B*. (Hrsg.), Computerrechtshandbuch. Informationstechnik in der Rechts- und Wirtschaftspraxis, Stand: Januar 2003, München (zitiert als: Kilian/Heussen-*Bearbeiter*).

Kindermann, H., Gesetzessprache und Akzeptanz der Norm, in: Öhlinger, T. (Hrsg.), Recht und Sprache. Fritz Schönherr-Gedächtnissymposium 1985, Wien 1986, 53.

Kingreen, T., Theorie und Dogmatik der Grundrechte im europäischen Verfassungsrecht, EuGRZ 2004, 570 ff.

Kirchberg, A.-T., Personenkennzeichen – Ende der Privatsphäre?, ZRP 1977, 137.

Kirchmann, J. v., Die Wertlosigkeit der Jurisprudenz als Wissenschaft. Vortrag, gehalten in der Juristischen Gesellschaft zu Berlin, Berlin 1848.

Kistler, E. / *Jaufmann, D*. (Hrsg.), Mensch – Gesellschaft – Technik. Orientierungspunkte in der Technikakzeptanzdebatte, Opladen 1990.

Klein, E., Anmerkung zu BVerfG, Beschluss v. 14.10.2004 – 2 BvR 1481/04, JZ 2004, 1176.

Klinkhammer, G., Kommunikation im Gesundheitswesen. Telematik: Patientenschutz steht an erster Stelle, DÄ 1998, A 1437.

Klöcker, I. / *Meister, J.*, Datenschutz im Krankenhaus (begründet von T. Barta), 2. Auflage, Düsseldorf 2001.

Kloepfer, M., Geben moderne Technologien und die europäische Integration Anlass, Notwendigkeit und Grenzen des Schutzes personenbezogener Informationen neu zu bestimmen? Gutachten für den 62. Deutschen Juristentag, in: Ständige Deputation des Deutschen Juristentages (Hrsg.), Verhandlungen des 62. Deutschen Juristentages Bremen 1998, Band I Teil D, München 1998.

Kniesel, M. / *Vahle, J.*, VE ME PolG. Musterentwurf eines einheitlichen Polizeigesetzes in der Fassung des Vorentwurfs zur Änderung des ME PolG. Text und amtliche Begründung, Heidelberg 1990.

Koch, C., Scoring-Systeme in der Kreditwirtschaft. Einsatz unter datenschutzrechtlichen Aspekten, MMR 1998, 458.

Koch, C., Freiheitsbeschränkung in Raten? Biometrische Merkmale und das Terrorismusbekämpfungsgesetz. HSFK-Report 5/2002, Frankfurt am Main 2002.

Koch, H., Gerichtliche Mediation. Gerichts- und verfahrensrechtliche Rahmenbedingungen, NJ 2005, 97.

Köhntopp, M., Technische Randbedingungen für einen datenschutzgerechten Einsatz biometrischer Verfahren, in: Horster, P. (Hrsg.), Sicherheitsinfrastrukturen. Grundlagen, Realisierung, Rechtliche Aspekte, Anwendungen, Braunschweig 1999, 177.

Köhntopp, M. / *Pfitzmann, A.*, Datenschutz Next Generation, in: Bäumler, H. (Hrsg.): E-Privacy, Wiesbaden 2000, 316.

Körner-Dammann, M., Weitergabe von Patientendaten an ärztliche Verrechnungsstellen, NJW 1992, 729.

Kollmann, T., Akzeptanz innovativer Nutzungsgüter und -systeme. Konsequenzen für die Einführung von Telekommunikations- und Multimediasystemen, Wiesbaden 1998.

Kommission zum Abbau der Arbeitslosigkeit und zur Umstrukturierung der Bundesanstalt für Arbeit, Moderne Dienstleistungen am Arbeitsmarkt, abrufbar unter http://www.bmwa.bund.de/Navigation/Service/bestellservice,did=12168.html, Berlin 2002.

Konferenz der Datenschutzbeauftragten des Bundes und der Länder, Auswirkungen des Volkszählungsurteils, DÖV 1984, 504.

Konferenz der Datenschutzbeauftragten des Bundes und der Länder, Entschließung der 47. Konferenz zur Einführung von Chipkarten im Gesundheitswesen, DuD 1994, 308 (abrufbar unter http://www.datenschutz-berlin.de/jahresbe/94/anlage/an2_2.htm).

Konferenz der Datenschutzbeauftragten des Bundes und der Länder, Entschließung der 49. Konferenz zum Datenschutz bei elektronischen Mitteilungssystemen, abrufbar unter http://www.datenschutz-berlin.de/jahresbe/95/anlage/an2_3.htm, 1995a.

Konferenz der Datenschutzbeauftragten des Bundes und der Länder, Entschließung der 50. Konferenz zu Datenschutzrechtlichen Anforderungen an den Einsatz von Chipkarten im Gesundheitswesen, abrufbar unter http://www.datenschutz-berlin.de/jahresbe/95/anlage/an2_10.htm, 1995b.

Konferenz der Datenschutzbeauftragten des Bundes und der Länder, Entschließung der 54. Konferenz zur Erforderlichkeit datenschutzfreundlicher Technologien, DuD 1997, 735 (abrufbar unter http://www.datenschutz-berlin.de/doc/de/konf/54/dstech.htm).

Konferenz der Datenschutzbeauftragten des Bundes und der Länder, Entschließung der 62. Konferenz zu Datenschutzrechtlichen Anforderungen an den „Arzneimittelpass" (Medikamentenchipkarte), abrufbar unter http://www.datenschutz-berlin.de/doc/de/konf/62/medikamentenchipkarten.htm, 2001.

Konferenz der Datenschutzbeauftragten des Bundes und der Länder, Positionspapier zu technischen Aspekten biometrischer Merkmale in Personalausweisen und Pässen, DuD 2002, 247 (abrufbar unter http://www.datenschutz-berlin.de/doc/de/konf/63/bio.htm).

Konferenz der Datenschutzbeauftragten des Bundes und der Länder, Entschließung der 69. Konferenz zur Einführung der elektronischen Gesundheitskarte, abrufbar unter http://www.lfd.m-v.de/beschlue/entsch69.html, 2005.

Koppelman, A., Sex, Law and Equality. Three Arguments for Gay Rights, Michigan Law Review 1997, 1636.

Kraft, D., Telematik im Gesundheitswesen. Vertragsarzt- und datenschutzrechtliche Aspekte, Wiesbaden 2003.

Kramer, P. / *Herrmann, M.*, Auftragsdatenverarbeitung. Zur Reichweite der Privilegierung durch den Tatbestand des § 11 Bundesdatenschutzgesetz, CR 2003, 938.

Kraus, D., Kostenübernahme für medizinische Dienstleistungen in der Europäischen Union, GesR 2004, 37.

Kraus, M. / *Wagemann, D.*, Chipkartenbasierter Self-Service für die Studierenden- und Prüfungsverwaltung, V&M 2002, 297.

Krebs, W., Zum aktuellen Stand der Lehre vom Vorbehalt des Gesetzes, Jura 1979, 304.

Krüger-Brand, H. E., Hoher Stellenwert der Gesundheitstelematik, DÄ 2002, A 3304.

Krüger-Brand, H. E., Elektronischer Heilberufsausweis: Zentraler Schlüssel, DÄ 2005, A 14.

Kruse, D. / *Peuckert, H.* Chipkarte und Sicherheit, DuD 1995, 142.

Kruse, J. / *Hänlein, A.* (Hrsg.), Gesetzliche Krankenversicherung: Lehr- und Praxiskommentar, 2. Auflage, Baden-Baden 2003 (zitiert als: LPK-SGB V-*Bearbeiter*).

Kubicek, H., Von der Technikakzeptanz zur digitalen Integration. Fortschritt in Worten und Taten?, in: Klumpp, D. / Kubicek, H. / Roßnagel, A. (Hrsg.), next generation information society? Notwendigkeit einer Neuorientierung, Mössingen-Talheim 2003, 96.

Kügler, D., Kryptographische Sicherheitsfunktionen bei Machine Readable Travel Documents, abrufbar unter http://www.sit.fraunhofer.de/smartcard-ws/WS_04/beitraege/download.php?file index=11, 2004.

Kügler, D., Risiko Reisepass? Schutz der biometrischen Daten im RF-Chip, c't 5/2005, 84.

Kühling, J., Kontrolle durch den EuGH: Kommunikationsfreiheit und Pluralismussicherung im Gemeinschaftsrecht. Zugleich eine Besprechung des Familiapress-Urteils des EuGH, EuGRZ 1997, 296.

Kuip, A., Vergleich biometrischer Erkennungssysteme sowie deren Weiterentwicklung in der Praxis, in: Nolde, V. / Leger, L. (Hrsg.): Biometrische Verfahren. Körpermerkmale als Passwort – Grundlagen, Sicherheit und Einsatzgebiete biometrischer Identifikation, Köln 2002, 367.
Kunig, P., Der Grundsatz informationeller Selbstbestimmung, Jura 1993, 595.
Kutscha, M., Kurze Stellungnahme zum Entwurf des Terrorismusbekämpfungsgesetzes (Bundestagsdrucksache 14/7386), abrufbar unter http://www.cilip.de/terror/kutscha.htm, 2001.
Kutscha, M., Rechtsschutzdefizite bei Grundrechtseingriffen von Sicherheitsbehörden, NVwZ 2003, 1296.
Ladeur, K. H., Datenschutz – vom Abwehrrecht zur planerischen Optimierung von Wissensnetzwerken. Zur „objektiv-rechtlichen Dimension" des Datenschutzes, DuD 2000, 12.
Lampe, E.-J., Erziehung zum Recht als Voraussetzung von Rechtsakzeptanz, in: Pichler, J. W. (Hrsg.), Rechtsakzeptanz und Handlungsorientierung, Wien 1998, 99.
Langkeit, J., Umfang und Grenzen der ärztlichen Schweigepflicht gemäß § 203 I Nr. 1 StGB, NStZ 1994, 6.
Larenz, K., Richtiges Recht. Grundzüge einer Rechtsethik, München 1979.
Larenz, K., Methodenlehre der Rechtswissenschaft, 6. Auflage, Berlin 1991.
Larenz, K. / *Canaris, C.-W.*, Methodenlehre der Rechtswissenschaft. Studienausgabe, 3. Auflage, Berlin 1995.
Laskaridis, E., Elektronische Patientenakte. Ärztliche Dokumentationspflicht und elektronische Datenverarbeitung, Frankfurt am Main 2003.
Laßmann, G., Bewertungskriterien zum Vergleich biometrischer Verfahren. Kriterienkatalog der Arbeitsgruppe 6 „Biometrische Identifikationsverfahren" von TeleTrusT Deutschland e.V., DuD 1999, 135.
Laufs, A., Krankenpapiere und Persönlichkeitsschutz, NJW 1975, 1433.
Laufs, A. / *Uhlenbruck, W.* (Hrsg.), Handbuch des Arztrechts, 3. Auflage München 2002 (zitiert als: Laufs/Uhlenbruck-*Bearbeiter*).
Laws, Sir J., Is the High Court the Guardian of Fundamental Constitutional Rights?, Public Law 1993, 59.
Leistenschneider, M., JobCard, DuD 2004, 175.
Lemmens, P., The Relation between the Charter of Fundamental Rights of the European Union and the European Convention on Human Rights – Substantive Aspects, MJ 2001, 49.
Lenaerts, K. / *De Smijter, E.*, The Charter and the Role of the European Courts, MJ 2001, 90.
Lenckner, T. / *Winkelbauer, W.*, Computerkriminalität. Möglichkeiten und Grenzen des 2. WiKG (I), CR 1986, 483.
Lennartz, H.-A., Probleme der Techniksteuerung durch Recht – am Beispiel des bundesdeutschen Datenschutzrechts, RDV 1990, 25.
Lepsius, O., Freiheit, Sicherheit und Terror: Die Rechtslage in Deutschland, Leviathan 2004, 64.
LeVay, S., Queer Science. The Use and Abuse of Research into Homosexuality, Cambridge 1996.
Liberty Alliance, Privacy and Security Best Practices, Version 2.0, abrufbar unter http://www.projectliberty.org/specs/final_privacy_security_best_practices.pdf, 2003.
Lilie, B., Medizinische Datenverarbeitung, Schweigepflicht und Persönlichkeitsrecht im deutschen und amerikanischen Recht, Göttingen 1980.
Limbach, J., Die Akzeptanz verfassungsgerichtlicher Entscheidungen – Die Rolle der Demoskopie, in: Pichler, J. W. (Hrsg.), Rechtsakzeptanz und Handlungsorientierung, Wien 1998, 258.
Lin, A.-P., Persönlichkeitsrechtsverletzung des Patienten und Arzthaftung, Regensburg 1996.
Lincke, K. H. / *Vázques, J. L. C.*, Die neue ISO/IEC 17799: Zertifizierung von Informationssicherheit, K&R 2003, 337.
Lisken, H., Polizei und Verfassungsschutz. Aspekte der gesetzlichen Zusammenarbeit, NJW 1982, 1481.
Lisken, H., „Verdachts- und ereignisunabhängige Personenkontrollen zur Bekämpfung der grenzüberschreitenden Kriminalität"?, NVwZ 1998, 22.
Lisken, H. / *Denninger, E.* (Hrsg.), Handbuch des Polizeirechts, 3. Auflage, München 2001 (zitiert als: Lisken/Denninger-*Bearbeiter*).

Löwe / *Rosenberg*, Die Strafprozessordnung und das Gerichtsverfassungsgesetz. Großkommentar, hrsg. von Peter Rieß, 1. Band: Einleitung; §§ 1 bis 111n, 24. Auflage, Berlin 1988 (zitiert als: Löwe/Rosenberg-*Bearbeiter*).

London School of Economics & Political Science (LSE), The Identity Project. An assessment of the UK Identity Cards Bill & its implications. Interim Report, London, abrufbar unter http://www.lse.ac.uk/collections/pressAndInformationOffice/PDF/IDreport.pdf, 2005.

Lord Irvine of Lairg, Judges and Decision-Makers: The Theory and Practice of Wednesbury Review, Public Law 1996, 59.

Lord Irvine of Lairg, The Development of Human Rights in Britain under an Incorporated Convention on Human Rights, Public Law 1998, 221.

Lorenz, D., Die Novellierung des Bundesdatenschutzgesetzes in ihren Auswirkungen auf die Kirchen, DVBl. 2001, 428.

Lucke, D., Akzeptanz. Legitimität in der „Abstimmungsgesellschaft", Opladen 1995.

Lucke, D., Riskante Annahmen – Angenommene Risiken. Eine Einführung in die Akzeptanzforschung, in: dies. / Hasse, M. (Hrsg.), Annahme verweigert. Beiträge zur soziologischen Akzeptanzforschung, Opladen 1998, 15.

Lücke, J., Die speziellen Schranken des Allgemeinen Persönlichkeitsrechts und ihre Geltung für die vorbehaltlosen Grundrechte. Zu den Schranken der vorbehaltlosen Freiheitsrechte aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG, DÖV 2002, 93.

Lüdemann, J., Die verfassungskonforme Auslegung von Gesetzen, JuS 2004, 27.

Luhmann, N., Grundrechte als Institution. Ein Beitrag zur politischen Soziologie, Berlin 1965.

Lyon, D., Under My Skin: From Identification Papers to Body Surveillance, in: Caplan, J. / Torpey, J., (Ed.), Documenting Individual Identity. The Development of State Practices in the Modern World, Princeton 2001, 291.

Mähring, M., Das Recht auf informationelle Selbstbestimmung im europäischen Gemeinschaftsrecht, EuR 1991, 369.

Magiera, S., Parlament und Staatsleitung in der Verfassungsordnung des Grundgesetzes: eine Untersuchung zu den Grundlagen der Stellung und Aufgaben des Deutschen Bundestages, Berlin 1979.

Maihofer, W., Rechtsstaat und menschliche Würde, Frankfurt am Main 1968.

Maihofer, W., Prinzipien freiheitlicher Demokratie, in: Benda, E. / Maihofer, W. / Vogel, H.-J. (Hrsg.), Handbuch des Verfassungsrechts der Bundesrepublik Deutschland, 2. Auflage, Berlin 1994, 427.

Mallmann, C. Datenschutz in Verwaltungs-Informationssystemen. Zur Verhältnismäßigkeit des Austausches von Individualinformationen in der normvollziehenden Verwaltung, München 1976.

Mallmann, O., Volkszählung und Grundgesetz, JZ 1983, 651.

Mallmann, O., Das Volkszählungsgesetz 1987, NJW 1986, 1850.

Mallmann, O., Zweigeteilter Datenschutz? Auswirkungen des Volkszählungsurteils auf die Privatwirtschaft, CR 1988, 93.

Malzer, H., Gesetzentwurf des BMJ: Die Anpassung der Formvorschriften an den modernen Rechtsverkehr, in: Geis, I. (Hrsg.), Die digitale Signatur – eine Sicherheitstechnik für die Informationsgesellschaft. Ein Leitfaden für Anwender und Entscheider, Eschborn 2000, 171.

Mangoldt, H. v. / *Klein, F.* / *Starck, C.*, Das Bonner Grundgesetz, Band 1: Präambel, Artikel 1 bis 19, 4. Auflage, München 1999; Band 2: Artikel 20 bis 78, 4. Auflage, München 2000 (zitiert als: v. Mangoldt/Klein/Starck-*Bearbeiter*).

Mansfield, T. / *Kelly, G.* / *Chandler, D.* / *Kane, J.*, Biometric Product Testing Final Report. Issue 1.0, 19 March 2001 (Bericht des Centre for Mathematics and Scientific Computing, Middlesex), abrufbar unter http://www.cesg.gov.uk/site/ast/biometrics/media/BiometricTestReportpt1.pdf, 2001.

Mansfield, T. / *Rejman-Greene, M.*, Feasibility Study on the Use of Biometrics in an Entitlement Scheme, February 2003 (abrufbar unter http://www.homeoffice.gov.uk/docs2/feasibility_study 031111_v2.pdf).

Manssen, G. (Hrsg.), Telekommunikations- und Medienrecht. Kommentar, Loseblatt, Stand: Juli 2003, Berlin (zitiert als: Manssen-*Bearbeiter*).
Martius, K., Sicherheitsmanagement in TCP/IP-Netzen. Aktuelle Protokolle, Praktischer Einsatz, Neue Entwicklungen, Braunschweig 2000.
Marzetta, A. / *Stöckle, R.* / *Vaterlaus, O.*, Braucht die Schweiz einen amtlichen digitalen Ausweis?, abrufbar unter http://www.ofj.admin.ch/themen/ri-ir/dig-id/intro-d.htm, 2001.
Matz, R. D., Europol: Datenschutz und Individualrechtsschutz im Hinblick auf die Anforderungen der EMRK, Aachen 2003.
Maunz, T. / *Dürig, G.* / *Herzog, R.* / *Scholz, R.* / *Lerche, P.* / *Papier, H.-J.* / *Randelzhofer, A.* / *Badura, P.* / *Herdegen, M.* / *di Fabio, U.* / *Klein, H. M.* / *Schmidt-Aßmann, E.*, Grundgesetz. Kommentar, Loseblatt, Stand: 42. Lieferung Februar 2003, München (zitiert als: M/D-*Bearbeiter*).
Maurer, H., Allgemeines Verwaltungsrecht, 14. Auflage, München 2002.
Maus, I., Sinn und Bedeutung von Volkssouveränität in der modernen Gesellschaft, KJ 1991, 137.
McCahill, M. / *Norris, C.*, CCTV in London, Urbaneye Working Paper No. 6 (RTD-Project "On the Threshold to Urban Panopticon? Analysing the Employment of CCTV in European Cities and Assessing its Social and Political Impacts"), Hull 2002 (abrufbar unter http://www.urban eye.net/results/ue_wp6.pdf).
McCormack, D., Can corporate America secure our nation? An analysis of the identix framework for the regulation and use of facial recognition technology, B. U. J. Sci. & Tech. L. 2003, 128.
McGoldrick, D., The Human Rights Committee. Its role in the development of the International Covenant on Civil and Political Rights, Oxford 1991.
Medert K. M. / *Süßmuth, W.*, Pass- und Personalausweisrecht. Band 1: Personalausweisrecht des Bundes und der Länder. Kommentar, 3. Auflage, Stuttgart 1998.
Meier, A., Der rechtliche Schutz patientenbezogener Gesundheitsdaten, Karlsruhe 2003.
Meinel, C. / *Gollan, L.*, Der elektronische Personalausweis? – Elektronische Signaturen und staatliche Verantwortung. Was fehlt den heutigen digitalen Signaturen?, JurPC Web-Dok. 223/2002, abrufbar unter http://www.jurpc.de/aufsatz/20020223.htm, 2002.
Meister, H., Europäische Harmonisierung des Datenschutzes, DuD 1980, 9.
Menezes, A. J., Elliptic Curve Public Key Cryptosystems, Boston 1993.
Menzel, H.-J. / *Schläger, U.*, Der Patient im Gesundheitsnetz, DuD 1999, 70.
Merrills, J. G. / *Robertson, A. H.*, Human rights in Europe: a study of the European Convention on Human Rights, 4th Edition, Manchester 2001.
Merten, M., Europäische Krankenversicherungskarte – Das Fundament ist gelegt. DÄ 2004, C 17.
Merz, M., Electronic Commerce. Marktmodelle, Anwendungen und Technologien, Heidelberg 1999.
Mey, G., Adoleszenz, Identität, Erzählung. Theoretische, methodologische und empirische Erkundungen, Berlin 1999.
Meyer, J. (Hrsg.), Kommentar zur Charta der Grundrechte der Europäischen Union, Baden-Baden 2003 (zitiert als: Meyer-*Bearbeiter*).
Meyer-Abich, K. M., Akzeptabilität von Techniken, in: Bröchler, S. / Simonis, G. / Sundermann, K. (Hrsg.), Handbuch Technikfolgenabschätzung, Berlin 1999, 309.
Meyer-Goßner, L., Strafprozessordnung. Gerichtsverfassungsgesetz, Nebengesetze und ergänzende Bestimmungen, 47. Auflage, München 2004.
Meyer-Ladewig, J., Konvention zum Schutz der Menschenrechte und Grundfreiheiten. Handkommentar, Baden-Baden 2003.
Meyer-Ladewig, J., Menschenwürde und Europäische Menschenrechtskonvention, NJW 2004, 981.
Michalowski, S., Schutz der Vertraulichkeit strafrechtlich relevanter Patienteninformationen, ZStW 1997, 519.
Möhrenschlager, M., Computerstraftaten und ihre Bekämpfung in der Bundesrepublik Deutschland, wistra 1991, 321.
Mowbray, A. R., Cases and materials on the European Convention on Human Rights, London 2001.

Mückenberger, U., Datenschutz als Verfassungsgebot. Das Volkszählungsurteil des Bundesverfassungsgerichts, KJ 1984, 1.
Müglich, A., Neue Formvorschriften für den E-Commerce. Zur Umsetzung der EU-Signaturrichtlinie in deutsches Recht, MMR 2000, 7.
Müller, G. / *Pfitzmann, A.* (Hrsg.), Mehrseitige Sicherheit in der Kommunikationstechnik: Verfahren, Komponenten, Integration, Bonn 1997.
Müller, J., Ist das Auslesen von RFID-Tags zulässig? Schutz von RFID-Transponderinformationen durch § 86 TKG, DuD 2004, 215.
Müller, J. / *Handy, M.*, RFID und Datenschutzrecht. Risiken, Schutzbedarf und Gestaltungsvorschläge, DuD 2004, 655.
Müller, J., Beitrag zur elektronischen Gesundheitskarte auf der OMNICARD 2004, in: Fluhr, M. (Hrsg.), Neue und bewährte Applikationsfelder der Chipkarte. Kongressdokumentation und Katalog, OMNICARD 2004, Berlin 2004, 215.
Müller, S., Akzeptanz, in: Dichtl, E. / Issing, O. (Hrsg.): Vahlens Großes Wirtschaftslexikon, Band 1, A-E, 2. Auflage, München 1994, 55.
Müller-Böling, D. / *Müller, M.*, Akzeptanzfaktoren der Bürokommunikation, München 1986.
Müller-Heidelberg, T., Das Terrorismusbekämpfungsgesetz – Ein Erfolg der Terroristen, Zeitschrift für Bürgerrechte und Gesellschaftspolitik Nr. 159, September 2002 (abrufbar unter http://www.bpb.de/files/Q7E6IU.pdf).
Münch, I. v. / *Kunig, P.*, Grundgesetz-Kommentar, Band 1 (Präambel bis Art. 19), 5. Auflage, München 2000; Band 2, Art. 20-69, 5. Auflage, München 2001 (zitiert als: v. Münch/Kunig-*Bearbeiter*).
Münch, S., Chipkarten, GMD-Spiegel 1/92, 4.
Müthlein, T., Abgrenzungsprobleme bei der Auftragsdatenverarbeitung, RDV 1993, 165.
Müthlein, T. / *Heck, J.*, Outsourcing und Datenschutz: Vertragsgestaltungen aus datenschutzrechtlicher Sicht, 2. Auflage, Frechen 1997.
Munde, A., Die Evaluation biometrischer Systeme – Im internationalen Kontext, in: Nolde, V. / Leger, L. (Hrsg.): Biometrische Verfahren. Körpermerkmale als Passwort – Grundlagen, Sicherheit und Einsatzgebiete biometrischer Identifikation, Köln 2002, 145.
Musielak, J. (Hrsg.), Kommentar zur Zivilprozessordnung, mit Gerichtsverfassungsgesetz, 3. Auflage, München 2002 (zitiert als: *Musielak*-Bearbeiter).
Musil, A., Das Bundesverfassungsgericht und die demokratische Legitimation der funktionalen Selbstverwaltung, DÖV 2004, 116.
Mußmann, E., Allgemeines Polizeirecht in Baden-Württemberg, 4. Auflage, Stuttgart 1994.
Myrell, G., Kontrollieren und kontrolliert werden. Formen sozialer Kontrolle, in: ders. (Hrsg.), Daten-Schatten. Wie die Computer dein Leben kontrollieren, Hamburg 1984, 11.
Nanavati, S. / *Thieme, M.* / *Nanavati, R.*, Biometrics – Identity Verification in a Networked World. A Wiley Tech Brief, New York 2002.
Nedden, B., Risiken und Chancen für das Datenschutzrecht, in: Roßnagel, A. (Hrsg.), Allianz von Medienrecht und Informationstechnik? Ordnung in digitalen Medien durch Gestaltung der Technik am Beispiel von Urheberschutz, Datenschutz, Jugendschutz und Vielfaltschutz, Baden-Baden 2001, 67.
Nettesheim, M., Die Garantie der Menschenwürde zwischen metaphysischer Überhöhung und bloßen Abwägungstopos, AöR 2005, 71.
Neumann, F., Demokratietheorien – Modelle zur Herrschaft des Volkes, in: ders. (Hrsg.), Handbuch Politische Theorien und Ideologien, Band 1, 2. Auflage, Opladen 1998, 1.
Nguyen, A. T., Here's Looking at you, Kid: Has Face-Recognition Technology Completely Outflanked The Fourth Amendment?, Va. J. L. & Tech. 2002, 2.
Nicolaysen, G., Die gemeinschaftsrechtliche Begründung von Grundrechten, EuR 2003, 719.
Nobis, F., Beweisverwertungsverbot bei Weitergabe eines Lichtbildes durch die Meldebehörde, DAR 2002, 299.

Nolde, V., Grundlegende Aspekte biometrischer Verfahren, in: dies. / Leger, L. (Hrsg.), Biometrische Verfahren. Körpermerkmale als Passwort – Grundlagen, Sicherheit und Einsatzgebiete biometrischer Identifikation, Köln 2002, 20.
Nolte, M., Die Anti-Terror-Pakete im Lichte des Verfassungsrechts, DVBl 2002, 573.
Norris, C. / *Armstrong, G.*, The Maximum Surveillance Society: The Rise of CCTV, Oxford 1999.
Nowak, C., Zur grundfreiheitlichen Inanspruchnahme von Gesundheitsleistungen im europäischen Binnenmarkt. Zugleich Anmerkung zu: EuGH, Urteil vom 13.05.2003 - Rs. C-385/99 -, EuR 2003, 644.
Oertel, K., Elektronische Form und notarielle Aufgaben im elektronischen Rechtsverkehr, MMR 2001, 419.
OMNICARD, Newsletter, Ausgaben: 2003: Juli, August, September, Oktober; 2004: Januar, Januar/2, März, März/2, September/2 2004, März 2005, alle abrufbar unter http://www.omnicard.de/index.php?m=17.
Oppermann, T., Europarecht. Ein Studienbuch, 2. Auflage, München 1999.
Ordemann, H.-J., Sicherheit und Datenschutz. Anmerkungen zu den Gesetzesentwürfen der Koalition, RDV 1986, 60.
Organisation for Economic Co-operation and Development (OECD), Working Party on Information Security and Privacy: Biometric-Based Technologies, OECD-Doc DSTI/ICCP/REG(2003) 2/FINAL, 28 April 2004, abrufbar unter http://appli1.oecd.org/olis/2003doc.nsf/linkto/dsti-iccp-reg(2003)2-final, 2004.
Orlowski, U., Ziele des GKV-Modernisierungsgesetzes (GMG), MedR 2004, 202.
Ortner, F.-J. / *Geis, I.*, Die elektronische Patientenakte. Rechtsfragen medizinischer Dokumentation in digitalen Dokumentationssystemen und digitalen Netzen, MedR 1997, 337.
Otter, H., Die österreichische Bürgerkarte mit Sozialversicherungs- und elektronischer Signaturfunktion. Beitrag zum 11. GMD Smartcard Workshop am 6. / 7. Februar 2001, abrufbar unter http://www.sit.fraunhofer.de/smartcard-ws/WS_01/Beitrag_Otter.pdf, 2001.
Otto, H., Strafrechtliche Konsequenzen aus der Ermöglichung der Kenntnisnahme von Bankgeheimnissen in einem öffentlich-rechtlichen Kreditinstitut durch Wartungs- und Servicepersonal eines Computer-Netzwerks, wistra 1999, 201.
Pache, E., Die Europäische Menschenrechtskonvention und die deutsche Rechtsordnung, EuR 2004, 393.
Paech, N., Vom langen Elend der Inneren Sicherheit, in: Kutscha, M. / Paech, N. (Hrsg.), Totalerfassung. „Sicherheitsgesetze", Volkszählung, Neuer Personalausweis, Möglichkeiten der Gegenwehr, Köln 1986, 72.
Pätzel, C., Lichtbildabgleich im Verkehrsordnungswidrigkeitenverfahren, DuD 1998, 188.
Palandt, Bürgerliches Gesetzbuch, 64. Auflage, München 2005 (zitiert als: Palandt-*Bearbeiter*)
Papier, H.-J. / *Möller, J.*, Das Bestimmtheitsgebot und seine Durchsetzung, AöR 1997, 177.
Pawlowski, H.-M., Methodenlehre für Juristen. Theorie der Norm und des Gesetzes, 3. Auflage, Heidelberg 1999.
Peeters, M., Security Policy vs. Data Protection. Transfer of Passengers Data to U.S. Authorities, MMR 2005, 11.
Pelzer, K. (Hrsg.), Enzyklopädisches Handbuch der Werbung und Publikation, Ott 1961.
Perelman, C., Recht und Rhetorik, in: Ballweg, O. / Seibert, T.-M. (Hrsg.), Rhetorische Rechtstheorie, Freiburg 1982.
Petermann, T., Biometrische Identifikationssysteme vor dem Durchbruch?, TAB-Brief Nr. 24/Juni 2003, 19.
Peters, A., Einführung in die Europäische Menschenrechtskonvention. Mit rechtsvergleichenden Bezügen zum deutschen Grundgesetz, München 2003.
Pfeiffer, G. (Hrsg.), Karlsruher Kommentar zur Strafprozessordnung und zum Gerichtsverfassungsgesetz mit Einführungsgesetz, 5. Auflage, München 2003 (zitiert als: KK-*Bearbeiter*).
Pfitzmann, A., Datenschutz durch Technik. Vorschlag für eine Systematik, DuD 1999, 405.
Pflüger, F., Haftungsfragen der Telemedizin, VersR 1999, 1070.

Phillips, P. J. / *Grother, P.* / *Micheals, R. J.* / *Blackburn, D. M.* / *Tabassi, E.* / *Bone, M.*, Face Recognition Vendor Test 2002. Overview and Summary, abrufbar unter http://www.frvt.org/DLs/FRVT_2002_Overview_and_Summary.pdf, 2003.

Pichler, J. W., Rechtsakzeptanz. Genügt der Befund, oder gibt es auch eine Aufgabe?, Graz 1996.

Pichler, J. W. / *Giese, K. J.*, Rechtsakzeptanz, Wien 1993.

Pieroth, B. / *Schlink, B.*, Grundrechte. Staatsrecht II, 12. Auflage, Heidelberg 1996; 19. Auflage, Heidelberg 2003.

Pieroth, B. / *Schlink, B.* / *Kniesel, M.*, Polizei- und Ordnungsrecht, München 2002.

Pietzker, J., Vorrang und Vorbehalt des Gesetzes, JuS 1979, 710.

Pitschas, R., Informationelle Selbstbestimmung zwischen digitaler Ökonomie und Internet. Zum Paradigmawandel des Datenschutzrechts in der globalen Informationsgesellschaft, DuD 1998, 139.

Pitschas, R., Wo bleibt der Patient in der Gesundheitsreform?, in: ders. (Hrsg.), Reformoptionen der gesetzlichen Krankenversicherung: „Quo vadis Gesundheitswesen?". Referate und Berichte der 4. Speyerer Gesundheitstage am 15./16. April 2002, Speyer 2002.

Podlech, A., Verfassungsrechtliche Probleme öffentlicher Informationssysteme, DVR 1972/73, 149.

Podlech, A., Aufgaben und Problematik des Datenschutzes, DVR 1976, 23.

Podlech, A., Gesellschaftstheoretische Grundlage des Datenschutzes, in: Dierstein, R. / Fiedler, H. / Schulz, A. (Hrsg.), Datenschutz und Datensicherung, Köln 1976, 311.

Podlech, A., Individualdatenschutz – Systemdatenschutz, in: Brückner, K. / Dalichau, G. (Hrsg.), Beiträge zum Sozialrecht. Festgabe für Hans Grüner, Percha 1982, 451.

Podlech, A., Die Begrenzung staatlicher Informationsverarbeitung durch die Verfassung angesichts der Möglichkeiten unbegrenzter Informationsverarbeitung mittels der Technik. Zur Entscheidung des Bundesverfassungsgerichts über das Volkszählungsgesetz 1983, Leviathan 1984, 85.

Pötzl, N., Das elektronische Schleppnetz. Technische Bausteine zur Total-Kontrolle des Volkes, in: Meyer-Larsen, W. (Hrsg.), Der Orwell-Staat 1984. Vision und Wirklichkeit, Hamburg 1983, 67.

Pötzl, N., Total unter Kontrolle. Computerausweis, Volkszählung, Verkabelung, Hamburg 1985.

Pordesch, U., Die elektronische Form und das Präsentationsproblem, Baden-Baden 2003.

Pordesch, U. / *Roßnagel, A.*, Elektronische Signaturverfahren rechtsgemäß gestalten, DuD 1994, 82.

Pordesch, U. / *Roßnagel, A.* / *Schneider, M. J.*, Erprobung sicherheits- und datenschutzrelevanter Informationstechniken mit Simulationsstudien, DuD 1993, 491.

Posch, R., Weißbuch Bürgerkarte, 2002 (abrufbar unter http://www.buergerkarte.at/weissbuch/20020515/WeissbuchBuergerkarte.20020515.pdf).

Pressmar, D. B., Zur Akzeptanz von computergestützten Planungssystemen, in: Krallmann, H. (Hrsg.), Unternehmensplanung und -steuerung in den 80er Jahren. Eine Herausforderung an die Informatik, Berlin 1982, 324.

Prins, C., Biometric Technology Law. Making our Body identify for us: Legal Implications of Biometric Technologies, The Computer Law & Security Report 1998, 159.

Privacy International, Transferring Privacy: The Transfer of Passenger Records and the Abdication of Privacy Protection. The first report on 'Towards an International Infrastructure for Surveillance of Movement', abrufbar unter http://www.privacyinternational.org/issues/terrorism/rpt/transferringprivacy.pdf, 2004.

Privacy International et. al., An Open Letter to the ICAO. A second report on 'Towards an International Infrastructure for Surveillance of Movement', abrufbar unter http://www.privacyinternational.org/issues/terrorism/rpt/icaoletter.pdf, 2004.

Probst, T., Biometrie und SmartCards. Wie kann Datenschutz technisch sichergestellt werden?, DuD 2000, 322.

Probst, T., Biometrie aus datenschutzrechtlicher Sicht, in: Nolde, V. / Leger, L. (Hrsg.), Biometrische Verfahren. Körpermerkmale als Passwort – Grundlagen, Sicherheit und Einsatzgebiete biometrischer Identifikation, Köln 2002, 115.

Projektgruppe verfassungsverträgliche Technikgestaltung e.V. (provet) / *Gesellschaft für Mathematik und Datenverarbeitung mbH (GMD)*, Die Simulationsstudie Rechtspflege. Eine neue Methode zur Technikgestaltung für Telekooperation, Berlin 1994.
Ptascheck, S., Studierendenausweise auf Chipkartenbasis, in: Horster, P. (Hrsg.), Chipkarten. Grundlagen, Realisierungen, Sicherheitsaspekte, Anwendungen, Braunschweig 1998, 192.
Pütter, P. S., Datensicherheit – Voraussetzung der Akzeptanz der Datenverarbeitung, DuD 1991, 67.
Pütter, P. S., Gewährleisten der Datensicherheit, DuD 1991, 227.
Quaas, M. / *Zuck, R.*, Medizinrecht, München 2004.
Rabbata, S., Elektronische Gesundheitskarte: Kein Start auf Knopfdruck, DÄ 2005, A 96.
Räther, P. C., Die EU-US-Flugdaten-Affäre. Aus der Sicht der Betreiber von Datenbanken mit Fluggastdaten, DuD 2004, 468.
Raiser, T., Rechtsgefühl, Rechtsbewusstsein, Rechtskenntnis, Rechtsakzeptanz. Einige begriffliche und methodische Bemerkungen zu den Grundlagen der Akzeptanzforschung, in: Pichler, J. W. (Hrsg.), Rechtsakzeptanz und Handlungsorientierung, Wien 1998, 109.
Rankl, W. / *Effing, W.*, Handbuch der Chipkarten. Aufbau – Funktionsweise – Einsatz von Smart Cards, 4. Auflage, München 2002.
Rapp, C., Rechtliche Rahmenbedingungen und Formqualität elektronischer Signaturen, München 2002.
Raßmann, S., Elektronische Unterschrift im Zahlungsverkehr, CR 1998, 36.
Reed, R. / *Murdoch, J.*, A guide to human rights law in Scotland, Edinburgh 2001.
Rehbinder, M., Rechtssoziologie, 5. Auflage, München 2003.
Reichl, H. / *Roßnagel, A.* / *Müller, G.*, Der Digitale Personalausweis, Wiesbaden 2005.
Reichow, H. / *Hartlep, U.* / *Schmidt, W.*, Möglichkeiten medizinischer Datenverarbeitung und Datenschutz, MedR 1998, 162.
Reichwald, R., Zur Notwendigkeit der Akzeptanzforschung bei der Entwicklung neuer Systeme der Bürotechnik. Band 1 der Arbeitsberichte "Die Akzeptanz neuer Bürotechnologie". Hochschule der Bundeswehr, München 1978.
Reid, P., Biometrics for Networked Security, Upper Saddle River 2004.
Rejman-Greene, M., BIOVISION. Roadmap to Successful Deployments from the User and System Integrator Perspective. Final Report (WP 1), 17. Oktober 2003, abrufbar unter http://www.eubiometricsforum.com/dmdocuments/D1.4%20BIOVISION%20Final%20Report%20(11.11).pdf, 2003a.
Rejman-Greene, M. (Ed.), BIOVISION. Roadmap to Successful Deployments from the User and System Integrator Perspective. Roadmap for Biometrics in Europe to 2010 (WP 2), 15. Oktober 2003, abrufbar unter http://www.eubiometricsforum.com/dmdocuments/BIOVISION_Roadmap.pdf, 2003b.
Richter, E., Recht in interaktiven Umgebungen, in: Bieber, C. / Leggewie, C. (Hrsg.), Interaktivität. Ein interdisziplinärer Schlüsselbegriff, Gießen 2004, 240.
Richter-Kuhlmann, E. A., Ranking von Gesundheitssystemen: Äpfel mit Birnen verglichen. Aktuelle Studie widerlegt WHO-Ranking und OECD-Statistiken, DÄ 2004, A 1215.
Rienhoff, O., Zeitgemäßer Schutz des Patientengeheimnisses, DuD 1997, 579.
Rienhoff, O., Chipkarten im Gesundheitswesen, ZaeFQ 2001, 642.
Rinken, A., Demokratie und Hierarchie. Zum Demokratieverständnis des Zweiten Senats des Bundesverfassungsgerichts, KritV 1996, 282.
Rivest, R. / *Shamir, A.* / *Adleman, L.*, A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, C.ACM 1978, 120.
Röhl, K. F., Allgemeine Rechtslehre, Köln 1994.
Röken, H., Gesetzesgehorsam statt Gesetzesakzeptanz, DÖV 1989, 54.
Roellecke, G., Normakzeptanz und Rechtsbewusstsein. Konsequenzen aus der Autonomie des Rechts, JZ 1997, 577.
Rössler, B., Der Wert des Privaten, Frankfurt am Main 2001.

Rojahn, O., Die Auslegung völkerrechtlicher Verträge in der Entscheidungspraxis des Bundesverwaltungsgerichts, in: Geiger, R. (Hrsg.), Völkerrechtlicher Vertrag und staatliches Recht vor dem Hintergrund zunehmender Verdichtung der internationalen Beziehungen, Baden-Baden 2000, 123.
Roland Berger & Partner, Telematik im Gesundheitswesen – Perspektiven der Telemedizin in Deutschland, München 1997.
Rosenbaum, U. / *Sauerbrey, J.*, Bedrohungs- und Risikoanalysen bei der Entwicklung sicherer IT-Systeme, DuD 1995, 28.
Roßnagel, A., Verfassungsänderung und Verfassungswandel in der Verfassungspraxis, Der Staat 1983, 551.
Roßnagel, A., Radioaktiver Zerfall der Grundrechte? Zur Verfassungsverträglichkeit der Kernenergie, München 1984.
Roßnagel, A., Demokratische Kontrolle großtechnischer Anlagen durch Verwaltungsreferendum, KritV 1986, 343.
Roßnagel, A., Datenschutz bei Praxisübergabe, NJW 1989, 2303.
Roßnagel, A., Die (tele-)kommunikative Selbstbestimmung, KJ 1990, 267.
Roßnagel, A., Die parlamentarische Verantwortung für den technischen Fortschritt, ZRP 1992, 55.
Roßnagel, A., Rechtswissenschaftliche Technikfolgenforschung. Umrisse einer Forschungsdisziplin, Baden-Baden 1993.
Roßnagel, A., Freiheit durch Systemgestaltung. Strategien des Grundrechtsschutzes in der Informationsgesellschaft, in: Egbert, N. / Roßnagel, A. / Schlink, B. (Hrsg.), die Freiheit und die Macht – Wissenschaft im Ernstfall. Festschrift für Adalbert Podlech, Baden-Baden 1994a, 227.
Roßnagel, A., Grundrechtliche Risiken und Chancen durch Chipkartennutzung, in: Wolfinger, B. (Hrsg.), Innovationen bei Rechen- und Kommunikationssystemen. Eine Herausforderung für die Informatik, Berlin 1994b, 267.
Roßnagel, A., Datenschutz in Sicherungsinfrastrukturen offener Telekooperation, DuD 1995, 582.
Roßnagel, A., Die Infrastruktur sicherer und verbindlicher Telekooperation. Gutachten für die Friedrich Ebert Stiftung, Bonn 1996 (abrufbar unter http://www.fes.de/fulltext/stabsabteilung/00217toc.htm).
Roßnagel, A., Globale Datennetze: Ohnmacht des Staates – Selbstschutz der Bürger. Thesen zur Änderung der Staatsaufgaben in einer „civil information society", ZRP 1997, 26.
Roßnagel, A., Rechtliche Regelungen als Voraussetzung für Technikgestaltung, in: Müller, G. / Pfitzmann, A. (Hrsg.), Mehrseitige Sicherheit in der Kommunikationstechnik: Verfahren, Komponenten, Integration, Bonn 1997a, Band I, 361.
Roßnagel, A., Rechtswissenschaftliche Technikfolgenforschung – am Beispiel der Informations- und Kommunikationstechniken, in: Schulte, M. (Hrsg.), Technische Innovation und Recht – Antrieb oder Hemmnis?, Heidelberg 1997b, 139.
Roßnagel, A., Neues Recht für Multimediadienste Informations- und Kommunikationsdienste-Gesetz und Mediendienste-Staatsvertrag, NVwZ 1998, 1.
Roßnagel, A., Die Sicherheitsvermutung des Signaturgesetzes, NJW 1998, 3312.
Roßnagel, A., Datenschutz in globalen Netzen. Das TDDSG – ein wichtiger erster Schritt, DuD 1999, 253.
Roßnagel, A., Simulationsstudien – Ziel und Methode, in: ders. / Haux, R. / Herzog, W. (Hrsg.), Mobile und sichere Kommunikation im Gesundheitswesen, Braunschweig 1999, 65.
Roßnagel, A., Digitale Signatur im europäischen elektronischen Rechtsverkehr, K&R 2000, 313.
Roßnagel, A., Datenschutzaudit. Konzeption, Durchführung, gesetzliche Regelung. Braunschweig/Wiesbaden 2000a.
Roßnagel, A., Regulierung und Selbstregulierung im Datenschutz, in: Kubicek, H. / Bracyk, H.-J. / Klumpp, D. / Roßnagel, A. (Hrsg.), Global@Home. Informations- und Dienstleistungsstrukturen der Zukunft. Jahrbuch Telekommunikation und Gesellschaft, Heidelberg 2000b, 385.
Roßnagel, A., Allianz von Medienrecht und Informationstechnik: Hoffnungen und Herausforderungen, in: ders. (Hrsg.), Allianz von Medienrecht und Informationstechnik? Ordnung in digitalen

Medien durch Gestaltung der Technik am Beispiel von Urheberschutz, Datenschutz, Jugendschutz und Vielfaltschutz, Baden-Baden 2001a, 17.
Roßnagel, A., Rechtswissenschaft, in: Ropohl, G. (Hrsg.), Erträge der Interdisziplinären Technikforschung. Eine Bilanz nach 20 Jahren, Berlin 2001b, 195.
Roßnagel, A., Das neue Recht elektronischer Signaturen. Neufassung des Signaturgesetzes und Änderungen des BGB und der ZPO, NJW 2001, 1817.
Roßnagel, A., Rechtliche Unterschiede von Signaturverfahren, MMR 2002, 215.
Roßnagel, A., Der elektronische Ausweis. Notwendige und mögliche Identifizierung im E-Government, DuD 2002, 281.
Roßnagel, A., Rechtliche Unterschiede von Signaturverfahren, MMR 2002, 215.
Roßnagel, A., Die neue Signaturverordnung, BB 2002, 261.
Roßnagel, A., Die elektronische Signatur in der öffentlichen Verwaltung: Hoffnungen und Herausforderungen, in: *ders.* (Hrsg.), Die elektronische Signatur in der öffentlichen Verwaltung. Die künftigen Regelungen und ihre praktische Umsetzung, Baden-Baden 2002, 13.
Roßnagel, A. (Hrsg.), Recht der Multimedia-Dienste. Kommentar zum IuKDG und zum MDStV, Loseblatt, Stand: Juni 2004, München (zitiert als: RMD-*Bearbeiter*).
Roßnagel, A., Eine konzertierte Aktion für die elektronische Signatur, MMR 2003, 1.
Roßnagel, A., Recht und Technik in der globalen Informationsgesellschaft, in: Klumpp, D. / Kubicek, H. / Roßnagel, A. (Hrsg.), next generation information society? Notwendigkeit einer Neuorientierung, Mössingen-Talheim 2003, 423.
Roßnagel, A., Das elektronische Verwaltungsverfahren. Das Dritte Verwaltungsverfahrensänderungsgesetz, NJW 2003, 469.
Roßnagel, A., Die fortgeschrittene elektronische Signatur, MMR 2003, 164.
Roßnagel, A., Qualifizierte elektronische Signatur mit Einschränkungen für das Besteuerungsverfahren, K&R 2003, 379.
Roßnagel, A. (Hrsg.), Sicherheit für Freiheit? Riskante Sicherheit oder riskante Freiheit in der Informationsgesellschaft, Baden-Baden 2003.
Roßnagel, A. (Hrsg.), Handbuch zum Datenschutzrecht. Die neuen Grundlagen für Wirtschaft und Verwaltung, München 2003 (zitiert als: Roßnagel-*Bearbeiter*).
Roßnagel, A., Anmerkung zu EuGH, Urteil v. 6.11.2003 – Rs. C-101/01 (Lindqvist/Schwe-den), MMR 2004, 99.
Roßnagel, A., Digitale Ausweise. Hoffnungen und Risiken, DuD 2005, 59.
Roßnagel, A., Elektronische Signaturen mit der Bankkarte? Das Erste Gesetz zur Änderung des Signaturgesetzes, NJW 2005, 385.
Roßnagel, A. / *Bizer, J.* / *Hammer, V.* / *Kumbruck, C.* / *Pordesch, U.* / *Sarbinowski, H.* / *Schneider, M. J.*, Die Simulationsstudie Rechtspflege. Eine neue Methode zur Technikgestaltung für Telekooperation, Berlin 1994.
Roßnagel, A. / *Fischer-Dieskau, S.*, Automatisiert erzeugte elektronische Signaturen, MMR 2004, 133.
Roßnagel, A. / *Fischer-Dieskau, S.* / *Pordesch, U.* / *Brandner, R.*, Erneuerung elektronischer Signaturen – Grundfragen der Archivierung elektronischer Dokumente, CR 2003, 301.
Roßnagel, A. / *Hornung, G.*, Biometrische Daten in Ausweisen, DuD 2005, 69.
Roßnagel, A. / *Hornung, G.*, Reisepässe mit elektronischem Gesichtsbild und Fingerabdruck, DÖV 2005, i.E.
Roßnagel, A. / *Pfitzmann, A.* / *Garstka, H.*, Modernisierung des Datenschutzrechts. Gutachten im Auftrag des Bundesministeriums des Innern, Berlin 2001.
Roßnagel, A. / *Sarbinowski, H.*, Simulationsstudien zur Gestaltung von Telekooperationstechnik – Wir brauch(t)en eine neue Methode, GMD-Spiegel 2/1993, 30.
Roßnagel, A. / *Scholz, P.*, Datenschutz durch Anonymität und Pseudonymität. Rechtsfolgen der Verwendung anonymer und pseudonymer Daten, MMR 2000, 721.
Roßnagel, A. / *Wedde, P.* / *Hammer, V.* / *Pordesch, U.*, Digitalisierung der Grundrechte? Zur Verfassungsverträglichkeit der Informations- und Kommunikationstechnik, Opladen 1990.

Rother, S., Prüfung von Chipkartensicherheit, in: Horster, P. (Hrsg.), Chipkarten. Grundlagen, Realisierungen, Sicherheitsaspekte, Anwendungen, Braunschweig 1998, 251.
Rublack, S., INPOL-neu aus datenschutzrechtlicher Sicht, DuD 1999, 437.
Rudolphi, H.-J. / *Frisch, W.* / *Paeffgen, H.-U.* / *Rogall, K.* / *Schlüchter, E.* / *Wolter, J.*, Systematischer Kommentar zur Strafprozessordnung und zum Gerichtsverfassungsgesetz. Loseblatt, Stand: Juli 2003, Neuwied (zitiert als: SK StPO-*Bearbeiter*)
Rühling, U., Die „Sicherheitsgesetze" im Überblick, in: Kutscha, M. / Paech, N. (Hrsg.), Totalerfassung. „Sicherheitsgesetze", Volkszählung, Neuer Personalausweis, Möglichkeiten der Gegenwehr, Köln 1986, 11.
Rüthers, B., Rechtstheorie. Begriff, Geltung und Anwendung des Rechts, 2. Auflage, München 2005.
Sachs, M. (Hrsg.), Grundgesetz. Kommentar, 3. Auflage, München 2003 (zitiert als: Sachs-*Bearbeiter*).
Sachverständigenrate für die konzertierte Aktion im Gesundheitswesen, Gutachten zur Finanzierung, Nutzerorientierung und Qualität, BT-Drs. 15/530, 2003.
Sagel-Grande, I., Der Zusammenhang zwischen Normakzeptanz, Normhandhabung und Normbefolgung, ZRP 1990, 26.
Sauer, H., Die neue Schlagkraft der gemeineuropäischen Grundrechtsjudikatur. Zur Bindung deutscher Gerichte an die Entscheidungen des Europäischen Gerichtshofs für Menschenrechte. Zugleich Anmerkung zu BVerfG, B. v. 14.10.2004 (JZ 2004, 1176), ZaörV 2005, 35.
Schaar, P., Mit heißer Nadel gegen den Terrorismus?, MMR 2001, 713.
Schaar, P., Datenschutz bei Web-Services, RDV 2003, 59.
Schaar, P., Selbstregulierung und Selbstkontrolle – Auswege aus dem Kontrolldilemma?, DuD 2003, 421.
Schäfer, H., Der Computer im Strafverfahren, wistra 1989, 8.
Schaefer, O. P., Gefährdung von Patientendaten bei konventioneller und automatischer Verarbeitung im System der kassenärztlichen Versorgung, in: Kilian, W. / Porth, A. J. (Hrsg.), Juristische Probleme der Datenverarbeitung in der Medizin. GMDS/GRVI Datenschutz-Workshop 1979, Berlin 1979, 13.
Schaefer, O. P., Die Versichertenkarte – Auftakt zu neuen Kommunikationsstrukturen im Gesundheitswesen, DuD 1993, 685.
Schäpe, M., Grenzen der Fahrerermittlung durch die Behörde, DAR 1999, 186.
Schäpe, M., Anmerkung zu OLG Stuttgart, Beschluss vom 26.8.2002 (DAR 2002, 566), DAR 2002, 568.
Schaffland, H. J. / *Wiltfang, N.*, Bundesdatenschutzgesetz: ergänzbarer Kommentar nebst einschlägigen Rechtsvorschriften, Loseblatt, (Stand: Februar 2004) Berlin.
Scheffler, H. / *Dressel, C.*, Vorschläge zur Änderung zivilrechtlicher Formvorschriften und ihre Bedeutung für den Wirtschaftszweig E-Commerce, CR 2000, 378.
Scheiwe, K., Informationsrechte von Patienten hinsichtlich der medizinischen und psychiatrischen Dokumentation. Eine Diskussion der Grenzen des vertraglichen Einsichtsrechts nach der BGH-Rechtsprechung im Verhältnis zu datenschutzrechtlichen Auskunftsansprüchen, KritV 1998, 313.
Schenke, W.-R., Verfassungskonformität der Volkszählung, NJW 1987, 2777.
Schenke, W.-R., Verwaltungsprozessrecht, 9. Auflage, Heidelberg 2004.
Scheuermann, D., Digitale Ausweise – Möglichkeiten und Empfehlungen aus technischer Sicht, DuD 2005, 66.
Scheuermann, D. / *Schwiderski-Grosche, S.* / *Struif, B.*, Usability of Biometrics in Relation to Electronic Signatures. EU Study 502533/8, abrufbar unter http://www.sit.fraunhofer.de/english/SICA/sica_projects/project_pdfs/eubiosig.pdf, 2000.
Schieder, A., Die automatisierte KFZ-Kennzeichenerfassung als polizeiliche Maßnahme, NJW 2004, 778.
Schiff, J., Die virtuelle Verwaltung braucht die digitale Signatur. Gesetze müssen schnell angepasst werden, der städtetag 6/2002, 20.

Schild, H.-H., Datenschutz in Europa, EuZW 1991, 745.
Schild, H.-H., Die EG-Datenschutz-Richtlinie, EuZW 1996, 549.
Schlatmann, A., Verwaltungsverfahrensrecht und elektronischer Rechtsverkehr, LKV 2002, 489.
Schlink, B., Das Recht der informationellen Selbstbestimmung, Der Staat 1986, 233.
Schmidt, C. / *Lenz, J.-M.*, Authentifizierung der Nutzer elektronischer Signaturen durch Biometrie, in Nolde, V. / Leger, L. (Hrsg.): Biometrische Verfahren. Körpermerkmale als Passwort – Grundlagen, Sicherheit und Einsatzgebiete biometrischer Identifikation, Köln 2002, 263.
Schmidt, E., Ärztliche Schweigepflicht und Zeugnisverweigerungsrecht im Bereich der Sozialgerichtsbarkeit, NJW 1962, 1745.
Schmidt, W., Die bedrohte Entscheidungsfreiheit, JZ 1974, 241.
Schmidt, W., Bürgerinitiativen – politische Willensbildung – Staatsgewalt, JZ 1979, 293.
Schmidt-Aßmann, E., Verwaltungslegitimation als Rechtsbegriff, AöR 1991, 329.
Schmidt-Beck, J. R., Rechtliche Aspekte der EDV-gestützten ärztlichen Dokumentation, NJW 1991, 2335.
Schmidt-Beck, J. R., Die Dokumentationspflichtverletzung und ihre Auswirkungen im Arzthaftungsprozess, Bayreuth 1994.
Schmitz, H. / *Schlatmann, A.*, Digitale Verwaltung? – Das Dritte Gesetz zur Änderung verwaltungsverfahrensrechtlicher Vorschriften, NVwZ 2002, 1281.
Schmitz, P., TDDSG und das Recht auf informationelle Selbstbestimmung, München 2000.
Schmitz, T., Die Grundrechtecharta als Teil der Verfassung der Europäischen Union, EuR 2004, 691.
Schnabel, U., Der vermessene Mensch, Spektrum der Wissenschaft 6/2003, 76.
Schneider, U. K., Datenschutz in der vernetzten Medizin, in: Grätzel v. Grätz, P. (Hrsg.), Vernetzte Medizin. Patienten-Empowerment und Netzinfrastrukturen in der Medizin des 21. Jahrhunderts, Hannover 2004, 136.
Schneier, B., Angewandte Kryptographie. Protokolle, Algorithmen und Sourcecode in C, Bonn 1996.
Schneier, B., The uses and abuses of biometrics, C.ACM 8/1999, 136.
Schneier, B., Secrets & Lies. Digital Security in a Networked World, New York 2000.
Schnepel, J., Maschinenverlesbare Menschen, in: Taeger, J. (Hrsg.), Der neue Personalausweis, Hamburg 1984, 143.
Schoch, F., Polizei- und Ordnungsrecht, in: Schmidt-Aßmann, E. (Hrsg.), Besonderes Verwaltungsrecht, 12. Auflage 2003, 111.
Schönke, A. / *Schröder, H.*, Strafgesetzbuch. Kommentar, 26. Auflage, München 2001 (zitiert als: Schönke/Schröder-*Bearbeiter*).
Scholz, P., Datenschutz beim Internet-Einkauf. Gefährdungen – Anforderungen – Gestaltungen, Baden-Baden 2003.
Scholz, R. / *Pitschas, R.*, Informationelle Selbstbestimmung und staatliche Informationsverantwortung, Berlin 1984.
Schorkopf, F., Persönlichkeits- und Kommunikationsgrundrechte, in: Ehlers, D. (Hrsg.), Europäische Grundrechte und Grundfreiheiten, Berlin 2002, 339.
Schröder, C., Der Zugriff der USA auf Daten europäischer Flugpassagiere – Neue Gefahren durch Passagier-Profilbildung? (CAPPS II), RDV 2003, 285.
Schröder, T., Die Gesundheitskarte wird den Medizinbetrieb stärker verändern als alle bisherigen Reformen, Gesundheits- und Sozialpolitik: Nachrichten, Analysen, Hintergrund, Ausgabe 15-16/2004, 13. August 2004.
Schröter, K. G., Standardisierung biometrischer APIs, DuD 1999, 160.
Schürer, T., EMV: Business Case und praktische Erfahrungen, in: Fluhr, M. (Hrsg.), Neue und bewährte Applikationsfelder der Chipkarte. Kongressdokumentation und Katalog, OMNICARD 2004, Berlin 2004, 107.
Schug, S. H. / *Schramm-Wölk, I.*, Telematik-Standards für das Gesundheitswesen, in: Jähn, K. / Nagel, E. (Hrsg.), e-Health, Berlin 2004, 11.

Schulte, M., Techniksteuerung durch Technikrecht – rechtsrealistisch betrachtet, in: Vieweg, K. (Hrsg.), Techniksteuerung und Recht. Referate und Diskussionen eines Symposiums an der Universität Erlangen-Nürnberg, Köln 2000, 23.

Schulz, B., Bericht aus Bonn, ZRP 1981, 143.

Schulzki-Haddouti, C., Digitale Signatur noch im Selbstfindungsprozess, VDI-Nachrichten vom 23.5.2003, abrufbar unter http://www.vdi-nachrichten.com/vdi_nachrichten/aktuelle_ausgabe/akt_ausg_detail.asp?source=rubrik&cat=3&id=12176, 2003.

Schulzki-Haddouti, C., Alles auf eine Karte. Die JobCard in schwerem Fahrwasser, c't 13/2004, 46.

Schulzki-Haddouti, C., Biometrie ohne Nebenwirkungen? Kritik an den geplanten Reisepässen, c't 10/2005, 94.

Schwetlick, W., Intranets und virtuelle private Netzwerke (VPNs), in: Jähn, K. / Nagel, E. (Hrsg.), e-Health, Berlin 2004, 30.

Secartis AG / *Secunet AG*, Ausgabe der Health Professional Card durch die Landesärztekammern, Teil I: Anforderungsanalyse; Teil II: Grobkonzept, Version 1.02, 29. Juni 2004, abrufbar unter http://www.aekwl.de/public/aktuelles/download/pdf/gutachten-secartis.pdf, 2004.

Seidel, G., Handbuch der Grund- und Menschenrechte auf staatlicher, europäischer und universeller Ebene. Eine vergleichende Darstellung der Grund- und Menschenrechte des deutschen Grundgesetzes, der Europäischen Menschenrechtskonvention von 1950 und des Internationalen Pakts über bürgerliche und politische Rechte von 1966 sowie der Entscheidungspraxis des Bundesverfassungsgerichts und der zuständigen Vertragsorgane, Baden-Baden 1996.

Seidel, M., Der neue Arztausweis. Schlüssel zur Kartei, DÄ 1994, A 1858.

Seifert, J., Der Bürger unter Aufsicht, in: Taeger, J. (Hrsg.), Der neue Personalausweis, Hamburg 1984, 172.

Sendatzki, V., Elektronisches Rezept: kompatibel mit Gesundheitskarte, Die BKK 2002, 206.

Shaw, M. N., International law, 4. Edition, Cambridge 1997.

Sieber, S. / *Nöding, T.*, Die Reform der elektronischen Unterschrift, ZUM 2001, 199.

Siemen, B., Grundrechtsschutz durch Richtlinien / Die Fälle Österreichischer Rundfunk u.a. und Lindqvist. Anmerkungen zu den Urteilen des Europäischen Gerichtshofes in den verbundenen Rechtssachen C-465/00, C-138/01 und C-139/01 und C-101/01, EuR 2004, 306.

Sietmann, R., Volkszählung ohne Fragebögen. Kopfzerbrechen um den nächsten Zensus, c't 19/1999, 268.

Sietmann, R., Chipkarte mit Fingerabdruck. Kompetenzgerangel um neue biometrische Systemstandards, c't 23/2002, 54.

Sietmann, R., Im Fadenkreuz. Auf dem Weg in eine andere Gesellschaft, c't 5/2002, 146.

Simitis, S., Datenschutz – Notwendigkeit und Voraussetzungen einer gesetzlichen Regelung, DVR 1973, 138.

Simitis, S., Datenschutz: Voraussetzung oder Ende der Kommunikation?, in: Horn, N. (Hrsg.), Europäisches Rechtsdenken in Geschichte und Gegenwart. Festschrift für H. Coing zum 70. Geburtstag, Band 2, München 1982, 495.

Simitis, S., Die informationelle Selbstbestimmung – Grundbedingung einer verfassungskonformen Informationsordnung, NJW 1984, 398.

Simitis, S., Urteilsanmerkung zu BGH, JZ 1986, JZ 1986, 188.

Simitis, S., Von der Amtshilfe zur Informationshilfe – Informationsaustausch und Datenschutzanforderungen in der öffentlichen Verwaltung, NJW 1986, 2795.

Simitis, S., „Sensitive Daten" – Zur Geschichte und Wirkung einer Fiktion, in: Brem, E. / Druey, J. N. / Kramer, E. A. / Schwander, I. (Hrsg.), Festschrift zum 65. Geburtstag von Mario M. Pedrazzini, Bern 1990, 469.

Simitis, S., Virtuelle Präsenz und Spurenlosigkeit. Ein neues Datenschutzkonzept, in: Hassemer, W. / Möller, K. P. (Hrsg.), 25 Jahre Datenschutz, Baden-Baden 1996, 28.

Simitis, S., Internet oder der entzauberte Mythos vom „freien Markt der Meinungen", in: Assmann, H.-D. / Brinkmann, T. / Gounalakis, G. / Kohl, H. / Walz, R. (Hrsg.), Wirtschafts- und Medienrecht in der offenen Demokratie: Freundesgabe für Friedrich Kübler zum 65. Geburtstag, Heidelberg 1997, 285.

Simitis, S., Die EU-Datenschutzrichtlinie – Stillstand oder Anreiz?, NJW 1997, 281.
Simitis, S., Datenschutz – Rückschritt oder Neubeginn?, NJW 1998, 2473.
Simitis, S., Auf dem Weg zu einem neuen Datenschutzkonzept. Die zweite Novellierungsstufe des BDSG, DuD 2000, 714.
Simitis, S. (Hrsg.), Kommentar zum Bundesdatenschutzgesetz, 5. Auflage, Baden-Baden 2003 (zitiert als: Simitis-*Bearbeiter*).
Simon, B., Wissensmedien im Bildungssektor: eine Akzeptanzuntersuchung an Hochschulen, Wien 2001.
Simon, J., Die erfasste Persönlichkeit, in: Taeger, J. (Hrsg.), Die Volkszählung, Hamburg 1983, 136.
Singh, S., Geheime Botschaften. Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internets, München 1999.
Skrobotz, J., „Lex Deutsche Bank": Das 1. SigÄndG. Anmerkungen zum Entwurf eines Ersten Gesetzes zur Änderung des Signaturgesetzes (Stand 1. April 2004), DuD 2004, 410.
Smith, R., Registering fears – proposals for the National Identity Register have sparked concerns about invasions of privacy, Law Society Gazette 2004, No. 24, 17.
Sobel, R., The Degradation of political Identity under a National Identification System, B.U. J. Sci. & Tech. L. 2002, 37.
Sobel, R., The Demeaning of Identity and Personhood in National Identification Systems, Harv. J. Law & Tec 2002, 319.
Sommermann K.-P., Völkerrechtlich garantierte Menschenrechte als Maßstab der Verfassungskonkretisierung. Die Menschenrechtsfreundlichkeit des Grundgesetzes, AöR 1989, 391.
Sosna, G., Out of Control: Der Milliardenbetrug mit den Versichertenkarten, Nordlicht Aktuell 3/2003, 10.
Soutar, C., Biometric System Security, Secure Nr. 5, 2002, 46 (abrufbar unter http://www.silicon trust.com/pdf/secure_5/46_techno_4.pdf).
Stange, H.-J., Datenschutz: Recht und Praxis. Ein Leitfaden für den öffentlichen Dienst in Bund und Ländern, Bonn 1992.
Stark, C., Patientenkarten. Betroffenenorientierte Technikbewertung und Gestaltung, in: Horster, P. (Hrsg.), Chipkarten. Grundlagen, Realisierungen, Sicherheitsaspekte, Anwendungen, Braunschweig 1998, 35.
Stark, C. / *Wohlmacher, P.*, Chipkartenprojekte im Gesundheitswesen, DuD 1997, 595.
Staudinger, J. v., Kommentar zum bürgerlichen Gesetzbuch mit Einführungsgesetz und Nebengesetzen. Zweites Buch: Recht der Schuldverhältnisse, §§ 611-615, 13. Bearbeitung, Berlin 1999 (zitiert als: Staudinger-*Bearbeiter*).
Steffen, E., Einige Überlegungen zur Haftung für Arztfehler in der Telemedizin, in: Hohloch, G. / Frank, R. / Schlechtriem, P. (Hrsg.), Festschrift für Hans Stoll zum 75. Geburtstag, Tübingen 2001, 71.
Steidle, R., Die datenschutzkonforme Gestaltung von Multimedia-Assistenzsystemen im Betrieb. Datenschutzrechtliche Anforderungen, rechtliche Regelungs- und technische Gestaltungsvorschläge für mobile Agentensysteme, Wiesbaden 2005, i.E.
Steiger, P., Die Akzeptanzprüfung bei Multimediaanwendungen, in: Silberer, G. (Hrsg.), Marketing mit Multimedia: Grundlagen, Anwendungen und Management einer neuen Technologie im Marketing, Stuttgart 1995, 269.
Stein, E., The Mismeasure of Desire. The Science, Theory, and Ethics of Sexual Orientation, Oxford 1999.
Steiner, H. J. / *Alston, P.*, International human rights in context: law, politics, morals. Text and materials, 2nd Edition, Oxford 2000.
Steinmüller, W., Informationstechnologie und staatliche Kontrolle, in: Arbeitskreis Rationalisierung Bonn (Hrsg.), Verdatet, Verdrahtet, Verkauft, Stuttgart 1982, 16.
Steinmüller, W., Personenkennzeichen, Versichertennummer und Personalausweis. Eine systemanalytische und verfassungsrechtliche Studie zu Datenverbund und Datenschutz im Sozial- und Sicherheitsbereich, DVR 1983, 205.

Steinmüller, W., Der maschinenlesbare Personalausweis, in: Kutscha, M. / Paech, N. (Hrsg.), Totalerfassung. „Sicherheitsgesetze", Volkszählung, Neuer Personalausweis, Möglichkeiten der Gegenwehr, Köln 1986, 60.

Steinmüller, W., Informationstechnologie und Gesellschaft. Einführung in die Angewandte Informatik, Darmstadt 1993.

Steinmüller, W. / *Ermer, L.* / *Schimmel, W.*, Datenschutz bei riskanten Systemen. Eine Konzeption entwickelt am Beispiel eines medizinischen Informationssystems, Berlin 1978.

Steinmüller, W. / *Lutterbeck, B.* / *Mallmann, C.* / *Harbort, U.* / *Kolb, G.* / *Schneider, J.*, Grundfragen des Datenschutzes. Gutachten im Auftrag des Bundesministeriums des Innern, BT-Drs. 6/3826, 1971.

Stern, K., Das Staatsrecht der Bundesrepublik Deutschland, Band I: Grundbegriffe und Grundlagen des Staatsrechts, Strukturprinzipien der Verfassung, 2. Auflage, München 1984; Band III: Allgemeine Lehren der Grundrechte. Unter Mitwirkung von M. Sachs, Halbband 1, München 1988; Halbband 2, München 1994.

Stock, J., Biometrie und innere Sicherheit, in: Deutsches Forum für Kriminalprävention (Hrsg.), Arbeitskreis Kriminalprävention und Biometrie. Workshop-Dokumentation vom 30. September 2002 in Bonn, 5.

Stocker, T., Java™ für Chipkarten, in: Horster, P. (Hrsg.), Chipkarten. Grundlagen, Realisierungen, Sicherheitsaspekte, Anwendungen, Braunschweig 1998, 227.

Stollreither, K., Die maschinenlesbare Gesellschaft, DuD 1986, 6.

Storch, M., Vertiefung: Identität in der Postmoderne – mögliche Fragen und mögliche Antworten, in: Dohrenbusch, H. / Blickenstorfer, J. (Hrsg.), Allgemeine Heilpädagogik. Eine interdisziplinäre Einführung. Band II: Exemplarische Ausschnitte der Wirklichkeit, Luzern 1999, 70.

Straub, J., Personale und kollektive Identität. Zur Analyse eines theoretischen Begriffs, in: Assmann, A. / Friese, H. (Hrsg.), Identitäten. Erinnerungen, Geschichte, Identität 3, 2. Auflage, Frankfurt am Main 1999, 73.

Strauß, G. (Leitung), Deutsches Fremdwörterbuch, Band 1, 2. Auflage, Berlin 1995.

Strebling, A. / *Burgheim, J.*, Subjektive Wahrnehmung der Gefahren des internationalen Terrorismus. Empirische Teilergebnisse einer Bürgerbefragung, Die Polizei 2003, 181.

Streinz, R., Europarecht, 6. Auflage, Heidelberg 2003.

Ströbele, H.-C., Nur ein leerer Volkszählungsfragebogen ist ein harmloser Volkszählungsfragebogen, in: Appel, R. / Hummel, D. (Hrsg.), Vorsicht Volkszählung!, Köln 1987, 8.

Struif, B., TeleTrusT – vertrauenswürdige elektronische Kommunikation, GMD-Spiegel 1/1998, 38.

Struif, B. (Ed.), German Health Professional Card and Security Module Card. Specification – Pharmacist & Physician –, Commissioned by: Central Research Institute of Ambulatory Health Care in Germany, German Medical Association, National Association of Office Based Physicians, Werbe- u. Vertriebsgesellschaft Deutscher Apotheker mbH, Version 2.0, 31.07.2003 (abrufbar unter http://www.aekwl.de/public/aktuelles/download/pdf/hpc20.pdf).

Struif, B. (Ed.), Die Spezifikation der elektronischen Gesundheitskarte, Teil 1: Kommandos, Algorithmen und Funktionen der COS-Plattform, Version 1.2, 28.1.2005, (abrufbar unter http://www.dimdi.de/dynamic/de/ehealth/karte/download/egk_spezifikation_teil1_v1-2.pdf); Teil 2: Basis-Anwendungen und Funktionen, Version 1.0, 10.3.2005 (abrufbar unter http://www.dimdi.de/dynamic/de/ehealth/karte/download/egk_spezifikation_teil2_v1-0.pdf); Teil 3: Elektronisches Rezept, Version 0.9, 11.3.2005 (abrufbar unter http://www.dimdi.de/dynamic/de/ehealth/karte/download/egk_spezifikation_teil3_v0-9.pdf).

Sutschet, H., Auftragsdatenverarbeitung und Funktionsübertragung, RDV 2004, 97.

Szczekalla, P., Die sogenannten grundrechtlichen Schutzpflichten im deutschen und europäischen Recht. Inhalt und Reichweite einer „gemeineuropäischen Grundrechtsfunktion", Berlin 2002.

Taeger, J., Das Volkszählungsgesetz 1983. Eine Bestandsaufnahme, in: ders. (Hrsg.), Die Volkszählung, Hamburg 1983, 68.

Taeger, J., Der neue maschinenlesbare Personalausweis, in: ders. (Hrsg.), Der neue Personalausweis, Hamburg 1984a, 9.

Taeger, J., Die Auswirkungen des Volkszählungsurteils auf das Personalausweisgesetz, in: ders. (Hrsg.), Der neue Personalausweis, Hamburg 1984b, 210.
Tanenbaum, A. S., Computernetzwerke, 4. Auflage, München 2003.
Taraschka, K., „Auslandsübermittlungen" personenbezogener Daten im Internet. Auswirkungen des Urteils des EuGH v. 6.11.2003 – Rs. C-101/01 – Bodil Lindqvist auf die Auslegung deutschen Rechts, CR 2004, 280.
Taupitz, J., Die ärztliche Schweigepflicht in der aktuellen Rechtsprechung des BGH, MDR 1992, 421.
TeleTrusT Deutschland e.V., Kriterienkatalog – Bewertungskriterien zur Vergleichbarkeit biometrischer Verfahren. Arbeitsgruppe 6: Biometrische Identifikationsverfahren, Version 2.0, Stand 10.7.2002, Erfurt 2002 (abrufbar unter http://www.teletrust.de/publikat.asp?id=40600).
*TeleTrusT Deutschland e.*V., Kartenreport: Intelligente Chipkarten im Gesundheitswesen, Version 1.0, München 2004.
Thalheim, L. / *Krissler, J.* / *Ziegler, P.-M.*, Körperkontrolle. Biometrische Zugangssicherungen auf die Probe gestellt, c't 11/2002, 114.
Thomale, H.-C., Haftung und Prävention nach dem Signaturgesetz, Baden-Baden 2003.
Thomale, H.-C., Die Haftungsregelung nach § 11 SigG, MMR 2004, 80.
Thomas, P. A., Mistaken Identity, NLJ 1995, 1254.
Thomas, P. A., Identity Cards, MLR 1995, 702.
Tiedemann, P., Von den Schranken des Allgemeinen Persönlichkeitsrechts, DÖV 2003, 74.
Tiemann, F., Missbrauch ist auszuschließen. Kritische Anmerkungen zur Volkszählung, in: Taeger, J. (Hrsg.), Die Volkszählung, Hamburg 1983, 219
Tinnefeld, M.-T., die Novellierung des BDSG im Zeichen des Gemeinschaftsrechts, NJW 2001, 3078.
Tinnefeld, M.-T. / *Ehmann, E.*, Einführung in das Datenschutzrecht, 3. Auflage, München 1998.
Tönnessen, C., Statische und dynamische biometrische Verfahren, DuD 1999, 161.
Torpey, J., The Invention of the Passport. Surveillance, Citizenship and the State, Cambridge 2000.
Towler, A., Mistaken Identity?, Law Society Gazette 2004, No. 17, 20.
Tröndle, H. / *Fischer, T.*, Strafgesetzbuch und Nebengesetze. Kommentar, 52. Auflage, München 2004.
Tschoepe, S., Recht á la carte. Juristischer Hürdenlauf zur JobCard, c't 13/2004, 49.
Uerpmann, R., Die Europäische Menschenrechtskonvention und die deutsche Rechtsprechung. Ein Beitrag zum Thema Völkerrecht und Landesrecht, Berlin 1993.
Ulsenheimer, K. / *Heinemann, N.*, Rechtliche Aspekte der Telemedizin – Grenzen der Telemedizin? MedR 1999, 197.
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD), Hinweise zur Anwendung des Schleswig-Holsteinischen Gesetzes zum Schutz personenbezogener Daten (Landesdatenschutzgesetz) v. 9.2.2000, 05-17 GS Schleswig-Holstein II G. Nr. 204-4, abrufbar unter http://www.datenschutzzentrum.de/download/hinwldsg.pdf, 2000.
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD), Positionspapier zum Antiterrorgesetz der Bundesregierung, abrufbar unter http://www.datenschutzzentrum.de/material/themen/divers/antiterr.pdf, Kiel 2001.
Unhabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD), Patientendatenverarbeitung im Auftrag, abrufbar unter http://www.datenschutzzentrum.de/material/themen/gesund/patdvia.htm, 2002.
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD), Tätigkeitsbericht 2003, LT-Drs. 15/2535, 2003a (abrufbar unter http://www.datenschutzzentrum.de/download/tb25.pdf).
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD), Kundenbindungssysteme und Datenschutz. Gutachten im Auftrag des Verbraucherzentrale Bundesverbandes e.V., Berlin 2003b (abrufbar unter http://www.datenschutzzentrum.de/wirtschaft/Kundenbindungssysteme.pdf).

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD), Biometrie in offiziellen Ausweisen: Rechtliche Rahmenbedingungen, abrufbar unter http://www.datenschutzzentrum.de/material/themen/divers/biometrie_ausweis.htm, 2004.

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD), Tätigkeitsbericht 2005, LT-Drs. 16/50, 2005 (abrufbar unter http://www.datenschutzzentrum.de/download/tb27.pdf).

Unruh, P., Anmerkung zu BVerwG, Beschluss v. 5.12.2002 – 2 BvL 5/98 u. 6/98, JZ 2003, 1061.

Usher, J. A., General principles of EC law, Harlow 1998.

Vahle, J., Medizinische Daten und Datenschutz, DuD 1991, 614.

Vedder, K. / *Weikmann, F.*, Smart Cards. Requirements, Properties and Applications, in: Horster, P. (Hrsg.), Chipkarten. Grundlagen, Realisierungen, Sicherheitsaspekte, Anwendungen, Braunschweig 1998, 1.

Vehslage, T., Das geplante Gesetz zur Anpassung der Formvorschriften des Privatrechts und anderer Vorschriften an den modernen Rechtsverkehr, DB 2000, 1801.

Verbraucherzentrale Bundesverband e.V. (VZBV), Abschlussbericht Projekt BioTrusT, in: Bundesministerium für Wirtschaft und Technologie / S-Finanzgruppe / TeleTrusT Deutschland e.V., BioTrusT. Ein interdisziplinäres Projekt zur Förderung biometrischer Identifizierungsverfahren, Abschlussbericht, September 2002, 38.

Verbraucherzentrale Bundesverband e.V. (VZBV), Stellungnahme zum Entwurf eines Gesetzes zur Modernisierung des Gesundheitswesens, abrufbar unter http://www.patientenunterstuetzung.de/Grundsaetzliches/StellungnahmeGMG20.6.2003.pdf, Berlin 2003.

Verein zur Förderung des öffentlichen bewegten und unbewegten Datenverkehrs (FoeBuD) e.V. et. al., Positionspapier über den Gebrauch von RFID auf und in Konsumgütern, abrufbar unter http://www.foebud.org/texte/aktion/rfid/positionspapier.pdf, 2003.

Viefhues, W., Das Gesetz über die Verwendung elektronischer Kommunikationsformen in der Justiz, NJW 2005, 1009.

Viefhues, W. / *Scherf, U.*, Sicherheitsaspekte bei der elektronischen Kommunikation zwischen Anwalt und Gericht. Ein Beitrag zum elektronischen Rechtsverkehr, K&R 2002, 170.

Vieten, G., Holland – ein Land lässt sich nicht zählen, in: Taeger, J. (Hrsg.), Die Volkszählung, Hamburg 1983, 270.

Viethen, A., Datenschutz als Aufgabe der EG – Bestandsaufnahme des datenschutzspezifischen Sekundärrechts und Analyse anhand der Kompetenzordnung des EG-Vertrages, Münster 2003.

Vieweg, K., Reaktionen des Rechts auf Entwicklungen der Technik, in: Schulte, M. (Hrsg.), Technische Innovation und Recht: Antrieb oder Hemmnis?, Heidelberg 1996, 35.

Vogelgesang, K., Grundrecht auf informationelle Selbstbestimmung?, Baden-Baden 1987.

Volle, P., § 9 BDSG als irrealer Maßstab für PCs, CR 1992, 500.

Volpe, F. P. / *Volpe, S.*, Chipkarten. Grundlagen, Technik, Anwendungen, Hannover 1996.

Vultejus, U., Informationelle Selbstbestimmung auch bei Genen, ZRP 2002, 70.

Wächter, M., Rechtliche Grundstrukturen der Datenverarbeitung im Auftrag, CR 1991, 333.

Wagner, P., Fest-Stellungen. Beobachtungen zur sozialwissenschaftlichen Diskussion über Identität, in: Assmann, A. / Friese, H. (Hrsg.), Identitäten. Erinnerungen, Geschichte, Identität 3, 2. Auflage, Frankfurt am Main 1999, 44.

Warda, F. / *Noelle, G.*, Telemedizin und eHealth in Deutschland: Materialien und Empfehlungen für eine nationale Telematikplattform. Deutsches Institut für medizinische Dokumentation und Information 2002 (abrufbar unter http://www.dimdi.de/de/ehealth/public/telematikbuch19_02_03_web.pdf).

Wassermann, R. (Hrsg.), Kommentar zum Grundgesetz für die Bundesrepublik Deutschland, Reihe Alternativkommentare, 2. Auflage, Neuwied 1989 (zitiert als: AK GG-*Bearbeiter*).

Wassermann, R. (Hrsg.), Kommentar zur Strafprozessordnung, Reihe Alternativkommentare, Band 2, Teilband 1: §§ 94-212b, Neuwied 1992 (zitiert als: AK StPO-*Bearbeiter*).

Weatherill, S. / *Beaumont, P.*, EU law, 3rd Edition, London 1999.

Weber, A., Charta der Grundrechte der Europäischen Union, München 2002.

Weber, M., Wirtschaft und Gesellschaft: Grundriss der verstehenden Soziologie, 5. Auflage (besorgt von J. Winckelmann), Tübingen 1976.

Weghaus, B., Die sicherheitstechnische Beurteilung biometrischer Produkte – Wird eine Science-Fiction-Vision zur Alltagsanwendung?, in: Nolde, V. / Leger, L. (Hrsg.): Biometrische Verfahren. Körpermerkmale als Passwort – Grundlagen, Sicherheit und Einsatzgebiete biometrischer Identifikation, Köln 2002, 167.
Wehrmann, R. / *Wellbrock, R.*, Datenschutzrechtliche Anforderungen an die Datenverarbeitung und Kommunikation im medizinischen Bereich, CR 1997, 754.
Weichert, T., Datenschutz und medizinische Forschung. Was nützt ein „medizinisches Forschungsgeheimnis?“, MedR 1996, 258.
Weichert, T., Datenschutzrechtliche Anforderungen an Chipkarten, DuD 1997, 266.
Weichert, T., Biometrie – Freund oder Feind des Datenschutzes?, CR 1997, 369.
Weichert, T., Automatisches Fingerabdruck-Identifizierungssystem – AFIS, DuD 1999, 167.
Weichert, T., Die Ökonomisierung des Rechts auf informationelle Selbstbestimmung, NJW 2001, 1463.
Weichert, T., Die Wiederbelebung des Personenkennzeichens – insbesondere am Beispiel der Einführung einer einheitlichen Wirtschaftsnummer, RDV 2002, 170.
Weichert, T., Datenschutz für Ausländer…nach dem 11. September 2001, DuD 2002, 423.
Weichert, T., Die elektronische Gesundheitskarte, DuD 2004, 391.
Weiler, J. H. H. / *Lockhart, N. J. S.*, „Taking rights seriously“ seriously: The European Court of Justice and its fundamental rights jurisprudence, CMLRev 1995, 51 und 579.
Weinberger, O., Akzeptanz, Akzeptabilität und Diskurs. Eine demokratietheoretische Überlegung, in: Pichler, J. W. (Hrsg.), Rechtsakzeptanz und Handlungsorientierung, Wien 1998, 73.
Wellbrock, R., Chancen und Risiken des Einsatzes maschinenlesbarer Patientenkarten, DuD 1994, 70.
Wende, I., Normen und Spezifikationen, in: Rechenberg, P. / Pomberger, G., Informatik-Handbuch, 3. Auflage, München 2002, 1101.
Wendt, G., Die ärztliche Dokumentation. Eine beweisrechtliche Untersuchung zu ihrer Bedeutung für die Entscheidung der Sorgfaltsfrage bei der deliktischen Arzthaftung, Baden-Baden 2001.
Werle, G., Schutz von Vertrauensverhältnissen bei der strafprozessualen Fernmeldeüberwachung?, JZ 1991, 482.
Wessels, J. / *Hettinger, M.*, Strafrecht, Besonderer Teil 1. Straftaten gegen Persönlichkeits- und Gemeinschaftswerte, 27. Auflage, Heidelberg 2003.
Westphalen, R. Graf v. / *Neubert, K.*: Zur Rolle von Recht und Rechtswissenschaft im Technikfolgenabschätzung- und Bewertungsprozess. Ein Problemaufriss, in: Westphalen, R. Graf v. (Hrsg.), Technikfolgenabschätzung, München, 1988, 257.
Wienke, A. / *Sauerborn, J.*, EDV-gestützte Patientendokumentation und Datenschutz in der Arztpraxis, MedR 1000, 517.
Wintemute, R., Sexual Orientation and Human Rights. The United States Constitution, the European Convention, and The Canadian Charter, Oxford 1995.
Wirtz, B., Biometrische Verfahren. Überblick, Evaluierung und aktuelle Themen, DuD 1999, 129.
Wittig, P., Die datenschutzrechtliche Problematik der Anfertigung von Persönlichkeitsprofilen zu Marketingzwecken, RDV 2000, 59.
Wohlfarth, J., Elektronische Verwaltung - Vorgaben und Werkzeuge für datenschutzgerechte Anwendungen RDV 2002, 231.
Wolf, C. / *Weber, M.* / *Knauer, C.*, Gefährdung der Privatautonomie durch Mediation?, NJW 2003, 1488.
Wollweber, H., Verbindungsdaten der Telekommunikation im Visier der Strafverfolgungsbehörden, NJW 2002, 1554.
Woodward, J. D., Jr., Biometrics: Identifying Law and Policy Concerns, in: Jain, A. / Bolle, R. / Pankanti, S. (Eds.): Biometrics. Personal Identification in Networked Society, Boston 1999, 385.
Woodward, J. D., Jr., Super Bowl Surveillance. Facing Up to Biometrics, abrufbar unter http://www.rand.org/publications/IP/IP209/, 2001.

Woodward, J. D., Jr. / *Orlans, N. M.* / *Higgins, P. T.*, Biometrics. Identity Assurance in the Information Age, New York 2003.
Wronka, G., Zur Interessenlage bei der Auftragsdatenverarbeitung, RDV 2003, 132.
Wuermeling, U., Neues Multimediarecht ab 1. August 1997, Datenschutzberater 7+8/1997, 6.
Wuermeling, U., Handelshemmnis Datenschutz. Die Drittländerregelung der Europäischen Datenschutzrichtlinie, Köln 2000.
Würtenberger, T., Akzeptanz von Recht und Rechtsfortbildung, in: Eisenmann, P. / Rill, B. (Hrsg.), Jurist und Staatsbewusstsein, Heidelberg 1987, 79.
Würtenberger, T., Akzeptanz durch Verwaltungsverfahren, NJW 1991, 257.
Würtenberger, T., Die Akzeptanz von Verwaltungsentscheidungen, Baden-Baden 1996.
Würtenberger, T., Die Akzeptanz von Gesetzen, Sonderheft 39/1999 der KZfSS, 380.
Würtenberger, T. / *Heckmann, D.* / *Riggert, R.*, Polizeirecht in Baden-Württemberg, 5. Auflage, Heidelberg 2002.
Würzberger, P. / *Stürmer, B.*, Der Staat braucht unsere Daten. Das Programm der Volkszählung 1983, in: Taeger, J. (Hrsg.), Die Volkszählung, Hamburg 1983, 164.
Wulff, M., „Lebenslagen": Verwaltungsorganisation aus Bürger- und Kundensicht. KGSt-Bericht Nr. 5/2002, Köln 2002.
Wurst, M., Europa 1992: Auf dem Weg zu einem einheitlichen Datenschutzrecht in der Europäischen Gemeinschaft, JuS 1991, 448.
Yildirim, N., Datenschutz im Electronic Government. Risiken, Anforderungen und Gestaltungsmöglichkeiten für ein datenschutzgerechtes und rechtsverbindliches eGovernment, Wiesbaden 2004.
Ziegler, P.-M., Bezahlfinger, c't 12/2003, 38.
Ziegler, T., Was tun, wenn man Zähler wird?, in: Appel, R. / Hummel, D. (Hrsg.), Vorsicht Volkszählung!, Köln 1987a, 37.
Ziegler, T., Was tun, wenn die Zähler kommen?, in: Appel, R. / Hummel, D. (Hrsg.), Vorsicht Volkszählung!, Köln 1987b, 46.
Zippelius, R., Juristische Methodenlehre, 9. Auflage, München 2005.
Zitzelsberger, R. / *Hogen, G.*, die Chipkarte der Deutschen Kreditwirtschaft. Übersicht und aktuelle Entwicklungen, DuD 2002, 271.
Zöllner, W., Die gesetzgeberische Trennung des Datenschutzes für öffentliche und private Datenverarbeitung, RDV 1985, 3.
Zuck, R., Grundrechtsschutz und Grundrechtsentfaltung im Gesundheitswesen. Ein verfassungsrechtlicher Diskurs, Bad Liebenzell 1983.