Der „elektronische Personalausweis“ in Deutschland: Gesetzgebungsverfahren, Einflussfaktoren und Pfade

Bericht im Rahmen des Projekts „Systemic Change of the Identification of Citizens by Government – Electronic Identity Management as a Complex Technical Innovation and its Organisational, Legal and Cultural Matching in Selected European Countries“ für das Institut für Informationsmanagement Bremen (ifib)

Dr. Gerrit Hornung, LL.M. / Prof. Dr. Alexander Roßnagel

Projektgruppe verfassungsverträgliche Technikgestaltung (provet)
im Forschungszentrum für Informationstechnikgestaltung (ITeG)
der Universität Kassel

Kassel, August 2010

Gliederung

Vorwort

Der vorliegende Bericht wurde im Rahmen des Projekts „Systemic Change of the Identification of Citizens by Government – Electronic Identity Management as a Complex Technical Innovation and its Organisational, Legal and Cultural Matching in Selected European Countries“ für das Institut für Informationsmanagement Bremen (ifib) erstellt. Das Projekt wurde durch die VolkswagenStiftung gefördert. Der Bericht wurde im Juni 2009 fertiggestellt und diente als Grundlage für die vergleichende Analyse der Einführung elektronischer Identitätspapiere in acht europäischen Staaten. Erste Ergebnisse sind in einem Sonderheft der Zeitschrift „Identity in the Information Society“ (Heft 3/2010) veröffentlicht. Der Endbericht wird Ende 2010 im LIT Verlag erscheinen (Herbert Kubicek, Torsten Noak: Mehr Sicherheit im Internet durch elektronischen Identitätsnachweis? Der neue Personalausweis im europäischen Vergleich).

Gegenüber der im Juni 2009 abgegebenen Fassung des Berichts wurden einige wenige Aktualisierungen vorgenommen, insbesondere hinsichtlich weiterer technischer Weichenstellungen, der inzwischen erlassenen Personalausweisverordnung und neuerer Literatur. Da Thema des Berichts die Entwicklung bis zum Abschluss des Gesetzgebungsprozesses ist, wurden Struktur und Inhalt im Übrigen beibehalten.

Die im Text und im Literaturverzeichnis zitierten Internetadressen wurden letztmalig Ende August 2010 geprüft.

1 Einführung

Mit der Verabschiedung des neuen Gesetzes über Personalausweise und den elektronischen Identitätsnachweis (PAuswG) sowie zur Änderung weiterer Vorschriften im Bundestag am 18. Dezember 2008, der Zustimmung des Bundesrats am 13. Februar 2009 und der Veröffentlichung im Bundesgesetzblatt am 24. Juni 2009[1] ist das Gesetzgebungsverfahren zum neuen elektronischen Personalausweis in formaler Hinsicht abgeschlossen. Wie bei anderen Gesetzgebungsverfahren sind diesem formalen Verfahren wissenschaftliche und politische, in diesem Fall auch technische, Diskussionen vorangegangen, die darüber hinaus während des Gesetzgebungsverfahrens fortgesetzt wurden. Überdies startete das Gesamtvorhaben nicht im luftleeren Raum: In Deutschland bestand schon bisher eine allgemeine Personalausweispflicht hinsichtlich des bisherigen, eingeschweißten Ausweises; mit den Veränderungen des Passrechts auf europäischer und deutscher Ebene wurden wichtige Rahmenbedingungen gesetzt; für die qualifizierte elektronische Signatur bestanden rechtliche Rahmenbedingungen, die allerdings nicht zu praktischem Erfolg geführt hatten.

Zu diesen Rahmenbedingungen mussten sich die am Projekt des elektronischen Personalausweises beteiligten Akteure verhalten. Das betrifft mehrere Ebenen, nämlich die politischen Grundentscheidungen, die Formulierung des neuen Gesetzes, die technische Ausgestaltung des neuen Dokuments, aber auch Verhalten und Argumentationsmodi von Befürwortern und Gegnern der Pläne in der öffentlichen Diskussion. Wenn die handelnden Personen sich zu den genannten Rahmenbedingungen verhalten, kann dies in Form einer starken Orientierung, einer neutralen Haltung und dem Ignorieren (beziehungsweise Gegenarbeiten) erfolgen.

Im Folgenden werden in einem ersten Schritt die Eckdaten der Diskussion und des Gesetzgebungsverfahrens beschrieben. Im Anschluss erfolgt eine Darlegung einzelner Einflussfaktoren und „Pfade“ der rechtlichen, technischen und politischen Entwicklung. Daran schließt sich eine Betrachtung der einzelnen Akteure an, bevor der Gesamtprozess – vorläufig – bewertet wird.

2 Politische Diskussion und Gesetzgebungsverfahren

Die Einführung des neuen Personalausweises hat sich im Laufe der Zeit mehrfach verzögert. Die erste Erwähnung biometrischer Daten im Personalausweisgesetz erfolgte zeitgleich mit der im Passgesetz. In beide Gesetze wurde durch das Terrorismusbekämpfungsgesetz vom 9. Januar 2002[2] entsprechende Passagen eingefügt.[3] Während der Pass jedoch bereits seit dem 1. November 2005 mit biometrischen Daten des Gesichts, und seit dem 1. November 2007 zusätzlich mit Daten des Fingerabdrucks ausgegeben wird, wurde die Einführung des Personalausweises zunächst auf Ende des Jahres 2009 (so die Ankündigung der Bundesregierung noch am Ende September 2007)[4] verschoben und soll nunmehr nach den Bestimmungen in Art. 7 des Gesetzes (mit Ausnahme der Vergabe von Berechtigungszertifikaten, die bereits ein halbes Jahr vorher möglich ist) zum 1. November 2010 erfolgen.

2.1 Politische Entwicklung und sonstige Ereignisse

Wichtige und in der Öffentlichkeit bekannte Zwischenschritte der politischen Diskussion und Entwicklung sind:

---

1 BGBl. I, 1346. Zur Konzeption und zum Gesetz s. *Roßnagel/Hornung/Schnabel*, DuD 2008, 168 ff.; *Roßnagel/Hornung*, DÖV 2009, 301 ff.; *Schulz*, CR 2009, 267 ff.; zu Einzelheiten s. die Kommentierungen in *Schliesky* (Hrsg.) 2009.

2 Gesetz zur Bekämpfung des internationalen Terrorismus, BGBl. I, 361.

3 S. dazu unten 3.1.2.

4 S. http://www.heise.de/newsticker/meldung/96371.

- Nach den Anschlägen des 11. September 2001 wurden in Personalausweisgesetz und Passgesetz neue Bestimmungen aufgenommen, die eine „Ankündigung“ der Aufnahme biometrischer Daten darstellten.[5]
- Ende des Jahres 2002 beauftragte das Bundesministerium für Wirtschaft und Arbeit in Zusammenarbeit mit dem Bundesministerium des Innern den Fraunhofer Verbund Mikroelektronik (VμE), Prof. Dr. *Alexander Roßnagel* als Leiter der Projektgruppe verfassungsverträgliche Technikgestaltung (provet) an der Universität Kassel und das Institut für Informatik der Universität Freiburg mit der Anfertigung einer Machbarkeitsstudie zum „Digitalen Personalausweis“, die die Verbindung aus biometrischen Daten und qualifizierter elektronischer Signaturfunktion in einem Identitätspapier aus technischer, rechtlicher und wirtschaftlicher Sicht untersuchte. Der Bericht wurde im Februar 2004 abgeschlossen und im darauffolgenden Jahr veröffentlicht.[6]
- Am 9. März 2005 wurde die Neukonzeption des Personalausweises zusammen mit der elektronischen Gesundheitskarte und dem Elektronischen Einkommensnachweis (ELENA, vormals JobCard-Verfahren) in die E-Card Strategie der Bundesregierung aufgenommen. Das Verhältnis zu den übrigen Teilen der Strategie spielte jedoch in der weiteren Debatte so gut wie keine Rolle. Die Einführung des elektronischen Personalausweises ist überdies ein Baustein der High-Tech-Strategie der Bundesregierung und wichtiger Bestandteil des E-Government-Programms 2.0.
- Im Laufe des Jahres 2007 wurde insbesondere die Konzeption des neuen elektronischen Identitätsnachweises von Akteuren im Bundesministerium des Innern und im Bundesamt für Sicherheit in der Informationstechnik (BSI) vorbereitet.
- Am 26. März 2007 fand das (erste) Berliner Gespräch „Elektronischer Personalausweis und E-Identity“ des Münchner Kreises statt.[7] Nach Impulsreferaten von *Johann Hahlen*, Staatssekretär im Bundesministerium des Innern, und *Udo Helmbrecht*, Präsident des Bundesamts für Sicherheit in der Informationstechnik, wurden insbesondere Anwendungsszenarien für den neuen Personalausweis diskutiert. Die genaue Ausgestaltung des elektronischen Identitätsnachweises – insbesondere die Struktur der Berechtigungszertifikate – blieb dabei noch unerwähnt.
- Die Konzeption wurde im Sommer 2007 durch den Referatsleiter Biometrie, Pass- und Ausweiswesen, Meldewesen im Bundesministerium des Innern, *Andreas Reisen*, so beschrieben: „Eine Kernfunktion des neuen Personalausweises ist die elektronische Authentisierung, die es Bürgerinnen und Bürgern erlaubt, sich mit ihren personenbezogenen Daten sicher gegenüber einem Geschäftspartner im Internet auszuweisen. Einen hohen Stellenwert bei der Planung dieser neuen Ausweisfunktion nimmt der Datenschutz ein: Durch die Abstufung der Zugriffsmöglichkeiten auf einzelne Datenfelder (Berechtigungszertifikate) und die Erforderlichkeit der Zustimmung des Personalausweisinhabers bei jeder Datentransaktion (PIN-Eingabe) werden wesentliche Datenschutzanforderungen umgesetzt. Die Bundesrepublik Deutschland trägt mit diesem Ansatz zur Entwicklung datenschutzfreundlicher und dennoch innovativer Identitätslösungen in Europa bei.“[8]

---

5 S. näher unten 3.1.2.

6 *Reichl/Roßnagel/Müller* 2005.

7 S. die Dokumentation der Veranstaltung: *Helmbrecht/Thielmann/Ziemer* (Hrsg.) 2007.

8 *Reisen*, Heft 8/2007 der Kommune 21, S. 18 f.

- Im weiteren Verlauf wurden die Pläne und technischen Konzeptionen auf einer Reihe von Tagungen vorgestellt.[9]
- Anfang September 2007 beauftragte das Bundesministerium des Innern die Projektgruppe verfassungsverträgliche Technikgestaltung (provet) an der Universität Kassel unter Leitung von Prof. Dr. *Alexander Roßnagel* mit der Erstellung einer Studie, die sich umfassend mit den Rechtsfragen und Rahmenbedingungen des elektronischen Personalausweises auseinandersetzt.[10] Dabei wurde auf das Projekt der Machbarkeitsstudie Digitaler Personalausweis aufgebaut, deren Ergebnisse aktualisiert und fortgeschrieben wurden. Inhaltlich befasst sich die Studie unter anderem mit den Möglichkeiten und Grenzen des elektronischen Identitätsnachweises, datenschutzrechtlichen Fragen, den Verbindungen zum Projekt Bürgerportale,[11] der Einbindung von Zertifizierungsdiensteanbietern, haftungsrechtlichen Problemen sowie Fragen des Kartellrechts und des Verbraucherschutzes. Die Studie wurde im März des Jahres 2008 abgeschlossen werden. Sie ist bislang nicht veröffentlicht.[12]
- Am 20. September 2007 besprachen die Regierungsfraktionen aus CDU/CSU und SPD die Pläne des Bundesministeriums des Innern. Im Anschluss äußerten sich verschiedene Innenpolitiker der Fraktionen, unter anderem die Innenexperten *Dieter Wiefelspütz* (SPD) und *Clemens Binninger* (CDU).[13] In den folgenden Tagen entstand eine Diskussion, die sich praktisch ausschließlich um die Einführung biometrischer Merkmale drehte. Der Bundesbeauftragte für Datenschutz und Informationsfreiheit, *Peter Schaar*, äußerte sich mehrfach ablehnend.
- Während der SPD-Innenexperte *Dieter Wiefelspütz* in seiner ersten Stellungnahme eine eindeutige Festlegung hinsichtlich der Speicherung von Fingerabdrücken vermieden hatte,[14] akzeptierten die innen- und rechtspolitischen Sprecher der SPD-Fraktion etwa zwei Wochen später auch diese Maßnahme.[15] Allerdings machten sie zur Bedingung, dass die Fingerabdrücke – wie auch beim Reisepass – ausschließlich auf den Personalausweisen selbst und nicht in zentralen Registern oder bei den Personalausweisbehörden gespeichert werden. Dies wurde von den Innenpolitikern der Union (etwa *Hans-Peter Uhl*) akzeptiert.
- In einer Antwort auf eine Kleine Anfrage der Fraktion DIE LINKE äußerte sich die Bundesregierung zur „Notwendigkeit neuer biometrischer Personalausweise aus Sicherheitsgründen“.[16] Darin beschrieb sie die Zahl der Fälschungen des bisherigen Personalausweises, die für den neuen Ausweis geplanten Sicherheitsmerkmale und patentrechtliche Fragen.[17]

---

9 Etwa von *Martin Schallbruch*, IT-Direktor im Bundesministerium des Innern, im Januar 2008 auf der Omnicard, s. http://www.heise.de/newsticker/meldung/101957; und von Ministerialrat *Andreas Reisen* auf dem Euroforum 2008, s. http://www.heise.de/newsticker/meldung/108208.

10 S. http://www.uni-kassel.de/fb7/provet/projekte/eperso/.

11 S. http://www.uni-kassel.de/fb7/provet/projekte/buergerportale/ und z.B. *Stach*, DuD 2008, 184 ff.; *Roßnagel/Hornung/Knopp/Wilke*, DuD 2009, 728 ff.

12 Für Teilergebnisse s. *Roßnagel/Hornung/Schnabel*, DuD 2008, 168 ff.; *Roßnagel/Hornung*, DÖV 2009, 301 ff.

13 In der Berliner Zeitung und der Leipziger Volkszeitung, s.a. http://www.heise.de/newsticker/meldung/96371 und http://www.heise.de/newsticker/meldung/96404.

14 S. http://www.heise.de/newsticker/meldung/96404.

15 S. http://www.heise.de/newsticker/meldung/97138.

16 BT-Drs. 16/7073.

17 http://www.heise.de/newsticker/meldung/103530.

- Im Februar des Jahres 2008 wurde in der Öffentlichkeit die Pseudonym-Funktion des neuen elektronischen Identitätsnachweises diskutiert.[18] Der parteilose BMI-Staatssekretär *August Hanning* erläuterte sie in einem Schreiben an die innenpolitische Sprecherin der FDP-Fraktion, *Gisela Piltz*. Die Funktion wurde vom Bundesbeauftragten für Datenschutz und Informationsfreiheit, *Peter Schaar*, begrüßt, der zugleich mitteilte, ihm liege das Grobkonzept zum neuen Personalausweis vor (dieses war zu diesem Zeitpunkt noch nicht öffentlich).
- Zeitgleich begründete *Martin Schallbruch*, IT-Direktor im Bundesministerium des Innern, die Einführung des neuen Personalausweises mit dem Anstieg der Fälle von Identitätsmissbrauch im Internet und dem Bedürfnis nach einer sicheren und interoperablen Identifizierungsinfrastruktur.[19] Dies wurde durch ein Positionspapier des Branchenverbands BITKOM unterstützt.[20]
- Am 6. Mai 2008 führte der Münchner Kreis ein 2. Berliner Gespräch zum Thema „Elektronischer Personalausweis und E-Identity“ durch. Neben einer detaillierten Vorstellung der Konzeption wurden insbesondere Anwendungserprobungen zum elektronischen Personalausweis erörtert.[21]
- Am 9. Mai 2008 gab es im Bundestag auf Antrag der Fraktion Bündnis 90/Die Grünen eine Debatte um einen Antrag dieser Fraktion, der explizit „Keine Einführung biometrischer Merkmale im Personalausweis“[22] betitelt war. Der Antrag richtete sich zugleich – wenn auch in relativ unspezifischer Form – gegen die Verbindung mit der qualifizierten elektronischen Signatur. In der Debatte wurde das Vorhaben von *Frank Hofmann* (SPD) und *Clemens Binninger* (CDU/CSU) gegen Angriffe der drei Oppositionsparteien verteidigt.[23]
- Nachdem die Innenpolitiker der SPD-Bundestagsfraktion die Speicherung von Fingerabdrücken im Personalausweis zunächst nicht nur akzeptiert, sondern teilweise auch gefordert hatten,[24] entstand im Frühjahr 2008 erneut Streit um diesen Punkt. Rechtspolitiker der SPD-Bundestagsfraktion, der Vorsitzende des Innenausschusses, *Sebastian Edathy*, und Bundesjustizministerin *Brigitte Zypries* lehnten die Speicherung vollständig ab. Am Ende einigte man sich Mitte Juni des Jahres 2008 auf die freiwillige Speicherung der Fingerabdrucksdaten. Dies dürfte im Gesamtprozess die schwierigste und wichtigste Entscheidung der politischen Akteure gewesen sein.
- Im Anschluss an diese Grundentscheidung wurde Anfang Juli des Jahres 2008 das schon mehrfach angekündigte technische Grobkonzept zum elektronischenh Personalausweis vorgestellt.

2.2 Gesetzgebungsverfahren

Das formale Gesetzgebungsverfahren lief wie folgt ab:

- Am 23. Juli 2008 erfolgte ein Kabinettsbeschluss der Bundesregierung über einen entsprechenden Gesetzesentwurf des Bundesministeriums des Innern, der zeitgleich ver-

---

18 S. hierzu unten 2.3.

19 http://www.heise.de/newsticker/meldung/103365.

20 S. http://www.omnicard.de/news/nl_08_02.pdf.

21 S. die Dokumentation der Veranstaltung: *Helmbrecht/Thielmann/Ziemer* (Hrsg.) 2008.

22 BT-Drs. 16/7749.

23 S. http://www.heise.de/newsticker//meldung/107691.

24 So *Dieter Wiefelspütz*, innenpolitischer Sprecher der SPD, am 21. April 2008 gegenüber WeltOnline: der Personalausweis mache nur Sinn, wenn die Fingerabdrücke eingescannt würden.

öffentlicht wurde. Soweit ersichtlich waren bis dahin auch während der Ressortabstimmung keine Details über das neue Gesetz in die Öffentlichkeit gelangt. Der Beschluss wurde von Datenschutzbeauftragten, der Opposition im Bundestag und weiteren Gruppen wie dem Chaos Computer Club (CCC) kritisiert, vom Branchenverband BITKOM dagegen begrüßt.[25]

- Der Bundesrat setzte sich am 19. September 2008 für eine Verschärfung des Regierungsentwurfs ein. Polizei- und Ordnungsbehörden sollten zur allgemeinen Gefahrenabwehr online auf die im Register gespeicherten Gesichtsdaten zugreifen dürfen.[26] Überdies sollte ein Abgleich der biometrischen Daten mit den Dateien des Bundeskriminalamtes (insbesondere dem AFIS-System) erfolgen. Beides wurde im weiteren Verfahren nicht weiter verfolgt.
- Der Gesetzesentwurf der Bundesregierung wurde am 7. Oktober 2008 als Bundestags-Drucksache veröffentlicht.[27]
- Die erste Lesung des Gesetzes erfolgte am 16. Oktober 2008.[28] *Clemens Binninger* (CDU) und *Frank Hofmann* (SPD) verteidigten den Entwurf, insbesondere unter Verweis auf den Kompromiss zu den biometrischen Fingerabdrucksdaten und dem Sicherheitsgewinn für das Electronic Government. *Gisela Piltz* (FDP), *Jan Korte* (Linke) und *Wolfang Wieland* (Bündnis 90/Die Grünen) übten deutliche Kritik.
- Am 17. Dezember 2008 erfolgten Beschlussempfehlung und Bericht des Innenausschusses des Bundestages.[29] Neben redaktionellen Änderungen wurde dabei ausdrücklich klargestellt, dass einer antragstellenden Person, die sich gegen die Aufnahme von Fingerabdrücken entscheidet, hieraus weder rechtliche noch tatsächliche Nachteile entstehen dürfen, die über die Nichtnutzung von Identifizierungsmöglichkeiten mittels Fingerabdrücken hinausgehen (nunmehr § 9 Abs. 3 Sätze 5 und 6 PAuswG).
- Am 18. Dezember 2008 wurde das Gesetz endgültig vom Bundestag verabschiedet.
- Am 13. Februar 2009 stimmte der Bundesrat zu.
- Die Veröffentlichung im Bundesgesetzblatt erfolgte am 24. Juni 2009[30].

2.3 Wesentliche Neuerungen des Gesetzes

Der neue Personalausweis wird mit dem Inkrafttreten des Gesetzes und der technischen Umsetzung drei neue Funktionen erhalten.[31] Erstens wird er wie der Reisepass[32] mit einem kontaktlosen RFID-Chip (im Gesetz korrekt „elektronisches Speicher- und Verarbeitungsmedium im Sinne von § 3 Abs. 10 und § 6c BDSG genannt)[33] ausgestattet, auf dem biometrische Daten des Gesichts gespeichert werden; die beim Pass obligatorische Speicherung auch der Fingerabdrucksdaten erfolgt allerdings gemäß § 5 Abs. 9 PAuswG nur auf Antrag.[34] Zweitens wird der Personalausweis gemäß § 22 PAuswG als sichere Signaturerstellungseinheit im Sin-

---

25 S. http://www.heise.de/newsticker/meldung/113204 und http://www.heise.de/newsticker/meldung/113284.

26 S. http://www.heise.de/newsticker/meldung/116237.

27 BT-Drs. 16/10489.

28 S. den Bericht unter http://www.heise.de/newsticker/meldung/117525.

29 BT-Drs. 16/11419.

30 BGBl. I, 1346.

31 S.a. *Schulz*, in: *Schliesky* 2009, Einf.; Vorb. Rn. 23 ff.

32 Zu den Rechtsfragen des elektronischen Reisepasses s. *Roßnagel/Hornung*, DÖV 2005, 983 ff.; *Pallasky* 2007, 30 ff.; *Hornung*, DuD 2007, 181 ff.

33 Dazu näher *Hornung* 2005, 253 ff.; *ders.*, DuD 2004, 15 ff.

34 S. *Schulz*, in: *Schliesky* 2009, § 5 Rn. 23.

ne des § 2 Nr. 10 SigG ausgestaltet und bietet damit die Möglichkeit, qualifizierte elektronische Signaturen zu erzeugen. Allerdings ist diese Funktion freiwillig und für den Ausweisinhaber mit Kosten verbunden.[35] Drittens erhält der Personalausweis einen elektronischen Identitätsnachweis, also eine technische Funktion zur elektronischen Authentisierung. Gemäß § 18 Abs. 1 Satz 1 PAuswG kann „der Personalausweisinhaber, der mindestens 16 Jahre alt ist, […] seinen Personalausweis dazu verwenden, seine Identität gegenüber öffentlichen und nichtöffentlichen Stellen elektronisch nachzuweisen“.[36]

Von diesen drei Grundfunktionalitäten wird im Folgenden der elektronische Identitätsnachweis näher erläutert, weil es sich dabei um eine echte Neuerung sowohl in technischer wie in rechtlicher Hinsicht handelt.[37] Für die Ausweisinhaber ist die Verwendung des elektronischen Identitätsnachweises in doppelter Hinsicht freiwillig. Zum einen können sie generell über das Ein- und Ausschalten entscheiden (§ 10 PAuswG), zum anderen über die Verwendung der Funktion im konkreten Einzelfall. Hierzu wird gemäß § 18 Abs. 4 PAuswG die Eingabe einer Geheimnummer (PIN) erforderlich sein.[38] Dieselbe Norm bestimmt, dass eine Datenübermittlung nur erfolgt, wenn der Diensteanbieter – also der Kommunikationspartner – ein gültiges Berechtigungszertifikat an den Ausweisinhaber übermittelt.[39] Derartige Zertifikate werden gemäß § 21 PAuswG nur an Diensteanbieter ausgestellt, deren Verarbeitungsprozesse einer datenschutzrechtlichen Prüfung standhalten. Es muss sich um einen legitimen Geschäftszweck handeln, der nicht im Adresshandel bestehen darf. Die Erforderlichkeit der Übermittlung zur Erfüllung des Geschäftszwecks ist nachzuweisen, weitere Anforderungen an Datenschutz und Datensicherheit sind zu erfüllen und es dürfen keine Anhaltspunkte für eine missbräuchliche Verwendung der Berechtigung vorliegen.

Der elektronische Identitätsnachweis verfügt über zwei weitere datenschutzfreundliche Funktionen.[40] Zum einen besteht die Möglichkeit, ein dienste- und kartenspezifisches Kennzeichen (Pseudonym) zu verwenden. Es dient gemäß § 2 Abs. 5 PAuswG der eindeutigen elektronischen Wiedererkennung eines Personalausweises durch den Diensteanbieter, für den es errechnet wurde, ohne dass weitere personenbezogene Daten übermittelt werden müssen. Zum anderen stellt er die technische Möglichkeit zur selektiven Übermittlung einzelner Datensätze bereit. Mit anderen Worten kann ein Berechtigungszertifikat auf bestimmte Datenfelder, etwa die Angabe „volljährig“[41] oder das Vorliegen eines bestimmten Wohnorts, begrenzt werden. So erfährt ein Anbieter von Diensten für Erwachsene oder für die Einwohner einer bestimmten Region lediglich, ob dieses Attribut vorliegt. Dies ermöglicht vor allem bei für den Nutzer kostenfreien (also etwa werbefinanzierten) Angeboten eine Nutzung ohne Angabe identifizierender Merkmale.

Die Aufnahme des elektronischen Speicher- und Verarbeitungsmediums in den Personalausweis und die Speicherung personenbezogener Daten in diesem Medium werden die Nutzungs-

---

35 Zu den Möglichkeiten und Herausforderungen der Kombination von Personalausweis und Signaturfunktion s. ausführlich *Roßnagel/Gitter*, in: Reichl/Roßnagel/Müller 2005, 91 ff.; 219 ff.; *Strasser/Müller/Roßnagel/Gitter*, ebd., 243 ff.; *Hornung* 2005, 319 ff.

36 Näher *Luch*, in: *Schliesky* 2009, § 18 Rn. 1 ff.

37 S. zum Folgenden bereits *Roßnagel/Hornung*, DÖV 2009, 301, 303 ff.; s.a. *Schulz*, CR 2009, 267, 268 ff.

38 Zum Einsatz wird überdies ein (kontaktloser) Kartenleser und eine Client-Software erforderlich sein, s. *Bundesministerium des Innern* 2008, 57 ff.; dort auch zum Folgenden.

39 S. hierzu ausführlich aus technischer Sicht das Grobkonzept des *Bundesministerium des Innern* 2008; zu den Sicherheitsmechanismen aus technischer Sicht *Bender/Kügler/Margraf/Naumann*, DuD 2008, 173 ff.; zur Vergabe der Berechtigungszertifikate *Schulz*, in: *Schliesky* 2009, § 21 Rn. 1 ff.

40 S. *Roßnagel/Hornung/Schnabel*, DuD 2008, 168 f., 171.

41 Durch die technische Umsetzung werden die jugendschutzrechtlichen Anforderungen an die Errichtung einer geschlossenen Benutzergruppe gemäß § 4 Abs. 2 Satz 2 JMStV erfüllt, s. *Altenhain/Heitkamp*, K&R 2009, 619 ff.; s.a. *Roßnagel/Hornung/Schnabel*, DuD 2008, 168, 169.

formen des Dokuments verändern. Die biometrischen und sonstigen Daten sind im Rahmen von hoheitlichen Kontrollen auch ohne eine PIN-Eingabe des Ausweisinhabers auslesbar. Hierzu wird eine Zugangsnummer (§ 2 Abs. 11 PAuswG) verwendet, die auf der Karte aufgedruckt sein wird. Diese muss optisch oder opto-elektronisch erfasst werden, um den Zugangsschlüssel für die kryptographische Absicherung der Daten berechnen zu können. Durch den Aufdruck der Zugangsnummer auf den Ausweis wird ein besonderes Risiko für kontaktlose Karten hervorgerufen. Denn jeder, der in der Lage ist, die Ausweisoberfläche zu lesen, kann sie zur Kenntnis nehmen. Um dieses Risiko so gering wie möglich zu halten, würde es künftig zu einem sicherheitsbewussten Verhalten des Ausweisinhabers gehören, dass er auch die auf dem Ausweis aufgedruckte Zugangsnummer im Rahmen des Möglichen vor dem Lesen durch Dritte schützt. Diesem Schutzziel widerspricht jedoch die Funktion des Personalausweises als Sichtdokument zur Identifizierung des Ausweisinhabers. In vielen Fällen ist eine Identifizierung des Ausweisinhabers durch Sichtvergleich mit dem Ausweisbild und durch Kenntnisnahme der Ausweisdaten vorgeschrieben, in noch erheblich mehr Fällen wird diese Ausweisfunktion aus Sicherheitsgründen von Behörden und Unternehmen auch ohne rechtliche Anforderung genutzt. Daher kann die in einfacher Weise auf dem Körper des elektronischen Personalausweises aufgedruckte Zugangsnummer kaum geheim gehalten werden.

Um dieses Risiko zu reduzieren, bestimmt § 1 Abs. 1 Satz 3 PAuswG, dass vom Ausweisinhaber nicht verlangt werden darf, den Personalausweis zu hinterlegen oder in sonstiger Weise den Gewahrsam aufzugeben – außer gegenüber zur Identitätsfeststellung berechtigte Behörden sowie zur Einziehung und Sicherstellung. Die Praxis, den Ausweis in Hotels abzugeben, in einer Diskothek als Pfand zu hinterlegen oder beim Besuch von Behörden an der Pforte einzubehalten,[42] wird somit in Zukunft nicht mehr zulässig sein.

2.4 Ganz oder überwiegend beibehaltene Regelungen

Die Novelle des Personalausweisgesetzes enthält mit den drei genannten Funktionen einerseits grundlegende Neuerungen des deutschen Personalausweisrechts. Andererseits wurden auch ganze Regelungsbereiche des bisherigen Personalausweisgesetzes beibehalten. Die wichtigsten dieser Bereiche sind:

- Die Ausweispflicht ab Vollendung des 16. Lebensjahres,
- Die Sichtdaten des Personalausweises und der Inhalt der maschinenlesbaren Zone (bei kleineren Abweichungen, die im vorliegenden Zusammenhang ohne Belang sind),
- Einrichtung, Inhalt und Organisation des Personalausweisregisters (bei Abweichungen hinsichtlich der Befugnisse zur Verarbeitung und Datenübermittlung sowie Ergänzungen, die aufgrund der neuen Funktion des elektronischen Identitätsnachweises erforderlich waren),
- Vielfältige Datenschutzbestimmungen insbesondere hinsichtlich der Seriennummern der Personalausweise, des Herstellungsprozesses und der Verwendung im Rahmen automatisierter Datenverarbeitungsprozesse (bei sprachlichen und gesetzessystematischen Neuerungen) und
- Die Zulässigkeit der Verwendung auch im privaten Bereich bei grundsätzlichem Verbot der Verwendung zum automatischen Abruf und zur automatischen Speicherung personenbezogener Daten (nunmehr § 20 PAuswG).[43]

Insbesondere der letzte Punkt ist erwähnenswert, weil im Rahmen der Neuregulierung versucht wurde, diese Grundsätze beizubehalten und für die Bestimmungen des elektronischen

---

[42] Vorgeschrieben z.B. in § 2 Abs. 3, Abs. 4 und Abs. 6 Nr. 3 BTHausO.

[43] Näher *Luch*, in: *Schliesky* 2009, § 20 Rn. 1 ff.

Identitätsnachweises in die elektronische Rechts- und Geschäftswelt zu „verlängern“. Zumindest insoweit geht mit dessen Einführung auch kein neues Verständnis der Funktion des Personalausweises oder gar ein neues Verständnis der staatlichen Aufgaben im Bereich des Personalausweiswesens einher.

Eine Reihe weiterer Bestimmungen hatte zwar keine Vorläufer im früheren Personalausweisgesetz des Bundes, weil dem Bund insoweit die Gesetzgebungskompetenz fehlte.[44] Entsprechende Vorgängernormen waren aber einerseits in den Personalausweisgesetzen der Länder, andererseits in analoger Form im Reisepassgesetz enthalten. Diese Regelungen wurden teilweise übernommen, teilweise durch leichte Modifikationen fortgeschrieben. Beispiele sind die nähere Ausgestaltung der Personalausweispflicht, Zuständigkeitsregelungen, Regelungen des Antrags- und Ausstellungsprozesses, Mitwirkungspflichten des Ausweisinhabers, Bestimmungen über die Ungültigkeit, Vorgaben für die Sicherstellung und Einziehung sowie Bußgeldbestimmungen.

2.5 Verbleibender Regelungsbedarf

Das neue Personalausweisgesetz ist eine grundsätzlich umfassende Regelung des deutschen Personalausweiswesens. Dennoch gibt es in zwei Bereichen weiteren Regelungsbedarf. Zum einen müssen bestimmte Normen des neuen Gesetzes durch Regelungen des Bundes näher ausgeformt werden, zum anderen gibt es (relativ schmale) Regelungsbereiche für die Länder.

Die erste Gruppe betrifft insbesondere die neuen technischen Funktionen des Personalausweises. § 34 PAuswG enthält eine umfassende Ermächtigung zum Erlass einer Rechtsverordnung für das Bundesministerium des Innern mit Zustimmung des Bundesrates und im Benehmen mit dem Auswärtigen Amt. Diese erstreckt sich unter anderem auf

- „Einzelheiten der technischen Anforderungen an die Speicherung des Lichtbildes und der Fingerabdrücke sowie den Zugriffsschutz auf die im elektronischen Speicher- und Verarbeitungsmedium abgelegten Daten“ (Nr. 2)
- „Einzelheiten […] über das Verfahren und die technischen Anforderungen für die Erfassung und Qualitätssicherung des Lichtbildes und der Fingerabdrücke, die Reihenfolge der zu speichernden Fingerabdrücke bei Fehlen eines Zeigefingers, ungenügender Qualität des Fingerabdrucks oder Verletzungen der Fingerkuppe sowie die Form und die Einzelheiten über das Verfahren der Übermittlung sämtlicher Ausweisantragsdaten von den Personalausweisbehörden an den Ausweishersteller“ (Nr. 3)
- „Einzelheiten zum elektronischen Identitätsnachweis“ (Nr. 5)
- „Einzelheiten a) der Geheimnummer, b) der Sperrung und Entsperrung des elektronischen Identitätsnachweises durch den Ausweisinhaber sowie c) der Speicherung und Löschung der Sperrmerkmale und des Sperrkennworts“ (Nr. 6)
- „Einzelheiten der Vergabe der Berechtigungen und Berechtigungszertifikate“ (Nr. 7)

Die umfangreiche (und für eine Rechtsverordnung ungewöhnlicherweise mit einer Begründung versehene)[45] Verordnung über Personalausweise und den elektronischen Identitätsnachweis (Personalausweisverordnung – PAuswV) wurde im Bundesministerium des Innern ausgearbeitet. Am 4. Juni 2010 stimmte der Bundesrat zu.[46] Neben der Rechtsverordnung nach § 34 PAuswG wird es – ebenso wie beim Pass – auch Verwaltungsvorschriften zur Ausführung

---

[44] S.u. 3.1.1.

[45] S. BR-Drs. 240/10.

[46] S. BR-Drs. 240/10(B); eine Veröffentlichung im BGBl. war bei Fertigstellung des Manuskripts noch nicht erfolgt.

des Personalausweisgesetzes geben; diese befinden sich derzeit in der Vorbereitung im Bundesministerium des Innern.

Für Ländern und Kommunen verbleiben nach der Neuregelung des Personalausweiswesens durch den Bund nur noch sehr schmale Regelungsbereiche. Für die klassischen Ausweisfunktionen einschließlich der Biometrie kommt es zu einem Gleichlauf mit dem Passrecht, es wird also im Wesentlichen nur noch die Zuständigkeit der Behörden durch Landesrecht geregelt werden. Für den elektronischen Identitätsnachweis gibt es keinerlei Regelungsmöglichkeiten für Länder oder Kommunen, hier bestehen die Handlungsoptionen im Wesentlichen in der Bereitstellung von Anwendungen des Electronic Government, die den elektronischen Identitätsnachweis nutzen. Im Bereich der qualifizierten elektronischen Signatur haben die Kommunen wegen der zurückhaltenden Regelung in § 22 PAuswG die Wahlfreiheit, ob sie mit Zertifizierungsdiensteanbietern zusammenarbeiten und etwa für diese bestimmte Funktionen im Antrags- und Ausgabeprozess qualifizierter Zertifikate übernehmen wollen.

3 Einflussfaktoren und „Pfade“ der Entwicklung

In diesem Kapitel soll die beschriebene Entwicklung vor dem Hintergrund von Einflussfaktoren und Rahmenbedingungen analysiert werden. Dabei werden die Bereiche Recht, Technik und Politik hinsichtlich der entsprechenden Pfade und Vorentscheidungen untersucht.

3.1 Recht

3.1.1 Verfassungsrecht: Gesetzgebungskompetenz

Eine wesentliche Änderung der rechtlichen Rahmenbedingungen soll vorweg erwähnt werden, weil sie für die gesamte Regelungsmaterie gilt. Die gesamte Neuordnung des Personalausweisrechts wäre vor der Föderalismusreform in der nunmehr erfolgten Art und Weise nicht möglich gewesen, weil die Rechtsmaterie der konkurrierenden Gesetzgebung unterfiel. Durch die Föderalismusreform[47] wurde die ausschließliche Gesetzgebungskompetenz für das Melde- und Ausweiswesen durch den neuen Art. 73 Abs. 1 Nr. 3 GG dem Bund zugeordnet. Dieser hat mit dem neuen Gesetz über Personalausweise und den elektronischen Identitätsnachweis von dieser Kompetenz Gebrauch gemacht.

3.1.2 Bisheriges Personalausweisrecht

Das bisherige Personalausweisrecht enthielt für den neuen Personalausweis zunächst eine im deutschen Kontext banal anmutende, im internationalen Vergleich aber durchaus relevante Vorentscheidung: Es bestimmte die Existenz eines staatlichen Personalausweises und in § 1 Abs. 1 Satz 1 des alten Personalausweisgesetzes (PersAuswG) eine allgemeine Ausweispflicht für alle Deutschen ab Vollendung des 16 Lebensjahres.[48] Anders als etwa im angloamerikanischen Raum, in dem die Existenz derartiger Identitätspapiere sehr kontrovers und oft massiv ablehnend diskutiert wird,[49] ist es deshalb kaum überraschend, dass die deutsche Diskussion diesen Punkt aussparte.

Für die neuen Funktionalitäten der qualifizierten elektronischen Signatur und des elektronischen Identitätsnachweises bestanden im bisherigen Recht keine Regelungen. Beide wurden erstmals durch das neue Gesetz eingeführt.

---

[47] Gesetz zur Änderung des Grundgesetzes vom 28.8.2006, BGBl I, S. 2034.

[48] Zu ihrer Verfassungsmäßigkeit s. *Hornung* 2005, 165 ff.

[49] S. etwa zum Stand der Diskussion um die Einführung biometrischer Ausweise im Jahre 2005 *Hornung* 2005, 93 ff.

Dagegen enthielt das bisherige Recht eine Regelung zur Biometrie. Es bestimmte, dass der Personalausweis biometrische Merkmale von Fingern oder Händen oder Gesicht enthalten „darf“ (§ 1 Abs. 4 Satz 1 PersAuswG a.F.), 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 a.F.). Diese Normen widersprachen sich gegenseitig:[50] Wenn zur Einführung biometrischer Merkmale noch ein weiteres Gesetz erforderlich war, so durfte der Personalausweis diese Merkmale gerade nicht enthalten. Aus materiellrechtlicher Sicht waren § 1 Abs. 4 Satz 1 und Abs. 5 Satz 1 PersAuswG a.F. im günstigsten Fall überflüssig, ansonsten aber schädlich, da sie in gesetzestechnischer Hinsicht vorgaben, Sicherungsmittel zu sein, ohne jedoch wirklich diese Wirkung zu haben. Ihre Verabschiedung erklärte sich daraus, dass nach den Anschlägen des 11. September 2001 eine politische Mehrheit für eine Aufnahme biometrischer Daten in Ausweisdokumente vorhanden war, diese in der Eile der Zeit aber keine konkreten Umsetzungsentscheidungen treffen konnte oder wollte. Es handelt sich also – wenn überhaupt – um eine politische, nicht um eine rechtliche Rahmenbedingung.

Im Ergebnis dürfte der Einfluss des bisherigen Personalausweisrechts auf die drei neuen Funktionen des Personalausweises eher begrenzt gewesen sein. Er beschränkt sich auf die Existenz eines staatlichen Ausweises und einen gewissen immanenten Zwang, diesen durch technische Fortentwicklung fälschungssicher zu gestalten.

3.1.3 Neuer und alter Reisepass

Das hergebrachte Passrecht hatte in einer ganzen Reihe von Regelungsbereichen eine Vorbildfunktion, die im hiesigen Kontext von untergeordneter Relevanz sind.[51] Eine größere Rolle spielten die Änderungen des Passgesetzes zur Biometrie, die zeitlich vor Verabschiedung des neuen Personalausweisgesetzes vorgenommen wurden.

Das Passgesetz war – wie bereits erwähnt – mit dem Terrorismusbekämpfungsgesetz ebenfalls hinsichtlich der Erwähnung biometrischer Daten geändert worden. Diese war wortgleich mit der Fassung des Personalausweisrechts und folglich gleich dieser ein rechtliches Nullum.[52] In der Folge schritt die Veränderung des deutschen Passrechts jedoch unter maßgeblichem Einfluss der Europäischen Union voran: Diese verabschiedete am 13. Dezember 2004 die EG-Verordnung 2252/2004 über Normen für Sicherheitsmerkmale und biometrische Daten in von den Mitgliedstaaten ausgestellten Pässen und Reisedokumenten (EG-Pass-VO).[53]

Diese gibt alle wesentlichen Details des neuen deutschen Reisepasses vor und setzte aufgrund des Grundsatzes des Vorrangs des Europarechts mit ihrem Inkrafttreten die Wirksamkeit der entgegenstehenden Normen des deutschen Passrechts außer Kraft. Ihr Gesetzgebungsverfahren soll deshalb hier kurz zusammengefasst werden.[54]

Der Vorschlag der Kommission zur Verordnung vom 18. Februar 2004[55] beschränkte sich noch auf die Verpflichtung zur Aufnahme von Gesichtsdaten und stellte die zusätzliche Speicherung von Fingerabdrücken „in interoperabler Form“ in das Ermessen der Mitgliedstaaten. Die Bestimmungen für den Datenträger beschränkten sich auf Sicherheitsanforderungen; an-

---

50 S. näher *Hornung* 2005, 174 ff.; *ders*., KJ 2004, 344, 356 f.

51 S.o. 2.4.

52 S.o. 3.1.2.

53 ABl. EU L 385/1 vom 29.12.2004; nunmehr geändert durch die Verordnung (EG) Nr. 444/2009, ABl. EU Nr. L 142 v. 6.6.2009; s. ausführlich *Roßnagel/Hornung*, DÖV 2005, 983 ff.; *Pallasky* 2007, 30 ff.

54 S. zum Folgenden bereits *Roßnagel/Hornung*, DÖV 2005, 983 ff.

55 KOM 2004(116), ABl. EU C 98 vom 23.4.2004, S. 39.

ders als in der schließlich beschlossenen Fassung fehlte das Erfordernis des Schutzes der Vertraulichkeit der Daten. Alle technischen Spezifikationen sollten geheim gehalten werden. Eine Zweckbestimmung für die biometrischen Daten fehlte noch.

Das Europäische Parlament wurde ordnungsgemäß gehört, auch wenn es offenbar durch den Rat unter erheblichen Zeitdruck gesetzt wurde.[56] Auch die Vorlage an das Parlament sah noch die lediglich fakultative Aufnahme von Fingerabdrücken vor. Dies wurde erst nach der Stellungnahme des Parlaments am 2. Dezember 2004[57] durch den Rat geändert, ohne dass die Verordnung diesem zur erneuten Stellungnahme vorgelegt wurde. Das Parlament forderte erfolgreich die Einführung einer Zweckbestimmung für die biometrischen Daten und die Vorgabe des technischen Vertraulichkeitsschutzes. Dagegen wurden weitere Vorschläge wie das Verbot einer europaweiten Passdatei und die Einbeziehung der Art. 29-Datenschutzgruppe in das Verfahren der technischen Normierung (Art. 5 EG-Pass-VO) vom Rat abgelehnt.

Auch wenn dies wegen des Vorrangs des Europarechts nicht zwingend erforderlich gewesen wäre, wurden die Normen des deutschen Passrechts der Verordnung angepasst.[58] Da die Ausgestaltung des Dokuments durch diese vorgegeben war, spielten insbesondere Fragen der Speicherung der biometrischen Daten außerhalb des Dokuments eine Rolle. Hierbei setze sich eine relativ restriktive Linie durch: Eine zentrale Datei für die biometrischen Gesichtsdaten wird nicht eingerichtet (§ 4 Abs. 3 Satz 3 PassG); die Fingerabdrucksdaten dürfen sogar nur ausschließlich für die Herstellung des Passes verwendet werden, sind im Anschluss zu löschen (§ 16 Abs. 2 Satz 3 PassG) und dürfen folglich nach der Herstellung ausschließlich im Chip des Passes gespeichert werden.

Die Normen des deutschen Passrechts haben keine rechtliche Wirkung für den Personalausweis. Überdies hatte die Europäische Union bei Verabschiedung der Pass-Verordnung keine Regelungskompetenz für den Personalausweis, weshalb sie ausdrücklich nicht für nationale Personalausweise gilt. Nach Inkrafttreten des Vertrags von Lissabon verfügt die Europäische Union gemäß Art. 77 Abs. 3 AEUV nunmehr über eine Befugnis zum Erlass von Bestimmungen für Personalausweise. Hiervon wurde bislang kein Gebrauch gemacht. Folglich bestand und besteht kein im *rechtlichen* Sinne zwingender Zusammenhang, und es handelt sich im vorliegenden Zusammenhang der Sache nach nicht um einen „rechtlichen Pfad“, sondern um einen technischen[59] und politischen.[60]

3.1.4 Signaturrecht

Das Signaturrecht schafft Rahmenbedingungen für die qualifizierte elektronische Signatur und ermöglichte auch nach altem Recht bereits den Einsatz des elektronischen Personalausweises als sichere Signaturerstellungseinheit gemäß § 2 Nr. 10 SigG. Das Signaturrecht schreibt dies jedoch nicht vor und es wurde im Zuge des neuen Gesetzes nur marginal geändert. Die Regelungen im Personalausweisgesetz beschränken sich auf die Vorgabe, den neuen Ausweis als sichere Signaturerstellungseinheit zu gestalten (§ 22 PAuswG). Die Art der Vergabe der Zertifikate, eine etwaige Mitwirkung der Personalausweisbehörden und Haftungsfragen wurden nicht geregelt. Der Antrags- und Ausgabeprozess (insbesondere hinsichtlich Schlüsselerzeugung und Kartenausgabe), der durch die Ausgestaltung des elektronischen Personalausweises als sichere Signaturerstellungseinheit voraussichtlich hervorgerufen wird, ist

---

56 S. z.B. http://www.heise.de/newsticker/meldung/53830.

57 Stellungnahme vom 2.12.2004, http://www2.europarl.eu.int/omk/sipade2?PUBREF=-//EP//TEXT+TA+P6-TA-2004-0073+0+DOC+XML+V0//DE&L=DE&LEVEL=3&NAV=S&LSTDOC=Y.

58 Zum Gesetz und dem Gesetzgebungsverfahren s. *Hornung*, DuD 2007, 181 ff.

59 S.u. 3.2.1.

60 S.u. 3.3.1.

bereits nach geltendem Signaturrecht zulässig;[61] Allerdings wurde mit § 3 Abs. 1 Satz 2 SigV ein neuer Weg der Erstidentifizierung ermöglicht (s.u.).

Zum Signaturrecht als Rahmenbedingung gehört auch, dass dieses bereits viele Jahre zuvor alle Möglichkeiten für die Ausgabe von Signaturkarten und den Einsatz der qualifizierten elektronischen Signatur geschaffen hatte. Der neue Personalausweis tritt zu dieser Infrastruktur in eine – allerdings nur teilweise – Konkurrenz. Einerseits ist er eine Alternative zu den bisher von den Zertifizierungsdiensteanbietern selbst ausgegebenen Signaturkarten, die dazu führen könnte, dass letztere in der Praxis nicht mehr verwendet beziehungsweise auch in Zukunft keine weite Verbreitung finden werden. Andererseits hat der Staat darauf verzichtet, selbst eine Zertifizierungsinfrastruktur aufzubauen oder die privaten Zertifizierungsdiensteanbieter zur Kooperation zu verpflichten.

Werden die bisherigen Ausgabeprozesse beibehalten, so wird der Erfolg des elektronischen Personalausweises als sichere Signaturerstellungseinheit deshalb wesentlich von der Kooperationsbereitschaft sowohl dieser Anbieter als auch der Personalausweisbehörden abhängen, wenn die bisherigen Abläufe einer face-to-face Identifizierung beibehalten werden sollen. Ob in diesem Verhältnis belastbare Geschäftsmodelle entstehen können (und ob die Behörden angesichts des Mehraufwandes und etwaiger Haftungsrisiken kooperationsbereit sein werden), lässt sich bisher kaum abschätzen.

Als Alternative zur bisherigen Registrierungsmethode ermöglicht deshalb § 3 Abs. 1 Satz 2 SigV nunmehr die Identifizierung des Antragstellers mittels des elektronischen Identitätsnachweises gemäß § 18 PAuswG.[62] Dies stellt eine Abkehr von der bisherigen Regelung dar, die sich aus der sicheren Erstidentifizierung bei der Ausgabe des Personalausweises begründet. Es steht zu erwarten, dass sich diese Form der Beantragung eines qualifizierten Zertifikats in der Praxis als (ein) Standardmodell durchsetzen wird. Wenn dies der Fall ist, besteht die oben beschriebene Abhängigkeit von einer Mitwirkung der Personalausweisbehörden nicht. Funktional wirken dann die Personalausweisbehörden wie dezentrale Registrierungsstellen für jede Form von Dienstleistern und eben auch für die Zertifizierungsdiensteanbieter. Die Behörden identifizieren den Ausweisinhaber für seine spätere Rolle als Signaturschlüssel-Inhaber und nehmen seine Daten auf. Der Zertifizierungsdiensteanbieter kann in seinen Geschäftsprozessen auf diese – in der Praxis sehr sichere – Identifizierung vertrauen.

Neben diesen Einzelheiten des Ausgabeprozesses ist auf eine wichtige Vorentscheidung des Gesetzgebers im Rahmen der Regulierung der qualifizierten elektronischen Signatur hinzuweisen. Die qualifizierte elektronische Signatur ist im deutschen Recht als Äquivalent zur eigenhändigen Unterschrift konzipiert.[63] Das qualifizierte Zertifikat enthält dementsprechend gemäß § 7 SigG keine behördlich vergebene eindeutige Angabe, die anderen Kommunikationspartnern aus anderen Zusammenhängen bereits bekannt wäre und deshalb bei einem Erstkontakt eine sichere Identifizierung ermöglichen würde.[64] Solange der Signaturschlüssel-Inhaber nicht einen weltweit eindeutigen Name besitzt, ist das einzige eindeutig identifizierende Datum die Zertifikatsnummer nach § 7 Abs. 1 Nr. 4 SigG. Diese ist jedoch Dritten vor einem Erstkontakt regelmäßig nicht bekannt und kann deshalb nur nach einer Anmeldung oder Bestätigung durch Dritte zur Identifizierung verwendet werden. Im Übrigen bleibt nur

---

61 S. *Roßnagel*, MMR 2006, 441 ff.

62 S.a. unten 3.2.2.

63 S. dazu *Roßnagel*, in: ders. (Hrsg.), Recht der Multimediadienste, § 2 SigG 1997 Rn. 25; *Skrobotz*, in: Manssen (Hrsg.), Telekommunikations- und Medienrecht, § 1 SigG Rn. 38 ff. m.w.N.

64 Zu diesem Problem und dem Bezug zur Verwendung von Pseudonymen s. *Hornung* 2006, 53 ff.

der Umweg einer Anfrage beim Zertifizierungsdiensteanbieter und eine nachträgliche Identifizierung des Signaturschlüssel-Inhabers nach § 14 Abs. 2 SigG.[65]

Die deutsche Konzeption schließt auch im Rahmen des bisherigen Konzepts des Signaturrechts Lösungen nicht aus, die eine sichere Identifizierung beim Erstkontakt ermöglichen. Durch die Verwendung qualifizierter Attribut-Zertifikate oder eines „elektronischen Ausweises“ (als durch die Meldebehörde qualifiziert signierter Datensatz aus Meldedaten und eigener Signatur des Signaturschlüssel-Inhabers) könnte dieses Ziel erreicht werden. Entsprechende Konzepte wurden jedoch nur in der Wissenschaft diskutiert[66] und – soweit ersichtlich – weder in der Praxis erprobt noch durch den Gesetzgeber bei der Konzeption des neuen Personalausweisgesetzes in Erwägung gezogen.

Europarechtlich ist die deutsche Lösung zulässig, aber nicht vorgeschrieben. Anhang I zur europäischen Signaturrichtlinie[67] enthält Mindestinhalte für qualifizierte Zertifikate, die in § 7 SigG umgesetzt wurden. In anderen Ländern ist es vielfach üblich, eine national vergebene Personenkennziffer in das qualifizierte Zertifikat aufzunehmen.[68] Abgesehen davon, dass eine solche in Deutschland nicht existiert und überwiegend als verfassungsrechtlich unzulässig eingestuft wird, war der deutsche Gesetzgeber um eine möglichst datensparsame Regelung bemüht. Diese ist im Geltungsbereich der Signaturrichtlinie zwar nicht singulär, führt aber mit Blick auf den elektronischen Identitätsnachweis dazu, dass zumindest zwei Gruppen von Staaten – und damit zwei Pfade der Entwicklung – zu unterscheiden sind. Denn der elektronische Identitätsnachweis des deutschen Personalausweises ist dafür konzipiert, mit der sicheren Identifizierung ein technisches Problem zu lösen, das in Staaten nicht existiert, die eine eindeutige Personenkennziffer im qualifizierten Zertifikat aufgenommen haben. Die detaillierte Konzeption des elektronischen Identitätsnachweises weicht zwar (insbesondere hinsichtlich der Berechtigungszertifikate und anderer datenschutzfreundlicher Funktionalitäten) von einer Identifizierung mittels des qualifizierten Zertifikats ab. Es bleibt aber abzuwarten, ob sich der deutsche Ansatz international durchsetzen wird.[69]

3.1.5 Elektronischer Identitätsnachweis

Die neuen Regelungen zum elektronischen Identitätsnachweis im Personalausweisgesetz haben im bisherigen Recht keine Vorläufer. Die bisher nach den Vorgaben des Signaturgesetzes ausgegebenen Signaturkarten haben in aller Regel ebenfalls eine Authentisierungsfunktion (die allerdings technisch anders funktioniert).[70] Diese ist jedoch im geltenden Recht – anders als die qualifizierte elektronische Signatur – weder hinsichtlich ihrer technischen Ausgestaltung, noch ihrer organisatorischen Rahmenbedingungen, noch ihrer Rechtsfolgen geregelt.

Im neuen Personalausweisgesetz sind Technik, Organisation und Datenverarbeitungsprozesse des elektronischen Identitätsnachweises detailliert, seine Rechtsfolgen hingegen nicht geregelt. Mutmaßlich spielten dabei zwei Punkte eine Rolle: Zum einen das Motiv, ein neues, da-

---

65 Zur Problematik des Aufdeckungsanspruchs vgl. *Roßnagel* 2003, Rn. 116 ff. m.w.N.; *ders.*, NJW 2001, 1817, 1821; *Roßnagel/Pfitzmann/Garstka*, 2001, 152. Auf die Probleme des Aufdeckungsverfahrens wurde bereits bei den Beratungen zum SigG 1997 aufmerksam gemacht, s. *Roßnagel*, in: ders. (Hrsg.), Recht der Multimediadienste, Einl. SigG Rn. 83.

66 Die Konzeption wurde entwickelt von *Roßnagel*, DuD 2002, 281, 284 f.; s.a. *Roßnagel/Gitter/Hornung*, in: Reichl/Roßnagel/Müller 2005, 240; *Hornung* 2005, 319 ff.; *ders*. 2006, 62 ff.

67 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.

68 S. im Zusammenhang mit den Plänen für den neuen Personalausweis zum Stand des Jahres 2005 *Hornung* 2005, 93 ff.

69 Standardisierungsaktivitäten werden auf europäischer Ebene im Projekt STORK durchgeführt, s. https://www.eid-stork.eu/.

70 S.u. 3.2.3.

tenschutzfreundliches Konzept für die Identifizierung im Internet zu schaffen (deshalb die detaillierten Regelungen der Datenverarbeitung und des Zugriffskonzepts), zum anderen die Analyse der Akteure, die in der starken Regulierung der Rechtsfolgen der qualifizierten elektronischen Signatur ein Hemmnis für ihre Verbreitung sahen.[71]

3.1.6 Datenschutzrecht

Hinsichtlich des Datenschutzrechts ist zwischen der verfassungsrechtlichen und der einfachgesetzlichen Ebene zu unterscheiden. Verfassungsrechtlich hat die – auch im internationalen Vergleich – relativ starke Position des Rechts auf informationelle Selbstbestimmung in mehrfacher Hinsicht zumindest mittelbaren Einfluss auf die datenschutzfreundlichen Teile der gesetzlichen Regulierung gehabt. Das betrifft bei der Biometrie den Verzicht auf die Registerspeicherung der Fingerabdrücke und die Freiwilligkeit der Speicherung von Fingerabdrucksdaten im Personalausweis, bei der qualifizierten elektronischen Signatur die Zurückhaltung des Gesetzgebers bei der Regulierung des Inhalts des qualifizierten Zertifikats und beim elektronischen Identitätsnachweis dessen technisch relativ komplexe datenschutzfreundliche Ausgestaltung. Inwieweit sich diese starke Betonung des Datenschutzes negativ auf die Nutzbarkeit des elektronischen Identitätsnachweises durch die Ausweisinhaber (Usability) und die Diensteanbieter auswirken wird, bleibt abzuwarten. Zumindest ist erkennbar, dass Diensteanbieter aus dem Bereich der Privatwirtschaft sich einem neuen Aufsichtsregime unterwerfen müssen. Insgesamt bestand offenbar im Bundesministerium des Innern der Wunsch, konstruktiv einen Prozess datenschutzfreundlich zu gestalten, statt nachträglich auf die Kritik der Datenschützer zu reagieren.

Im einfachen Datenschutzrecht ergeben sich nur sehr wenige Anknüpfungspunkte. Mit der ausdrücklichen Regelung des Ausweischips als „elektronisches Speicher- und Verarbeitungsmedium“ (§ 5 Abs. 5 PAuswG) knüpft das Gesetz an die bereits bestehenden Bestimmungen in § 3 Abs. 10 und § 6c BDSG an.[72] Außerdem werden die datenschutzrechtlichen Aufsichtsbehörden in den Prozess von Rücknahme und Widerruf des Berechtigungszertifikats eingebunden (§ 21 Abs. 5 PAuswG).

3.2 Technik

Bei der Einführung des elektronischen Personalausweises wurden und werden vielfach technische Vorentscheidungen berücksichtigt, die in anderen Bereichen getroffen wurden und jetzt auf das neue Dokument und die mit ihm interagierende Infrastruktur übertragen werden. Insoweit lässt sich hinsichtlich der drei neuen Funktionen des Personalausweises unterscheiden.

3.2.1 Biometrie

Die entscheidende Weichenstellung für die Ausgestaltung der Biometriefunktion wird durch zwei Faktoren determiniert: Zum einen die technische Ausgestaltung des neuen Reisepasses,

---

[71] Inwieweit dies zutreffend ist, soll an dieser Stelle nicht ausführlich diskutiert werden. Es spricht einiges dafür, dass nicht die starke Durchregulierung der qualifizierten Signatur das entscheidende Hemmnis in der Vergangenheit bildeten, sondern das Fehlen einerseits von attraktiven Anwendungen für die Signatur („Killer-Applikationen“), andererseits von Geschäftsmodellen, die die Kosten der Signaturerzeugung auf diejenigen Akteure abwälzen, bei denen Kostenvorteile entstehen. In den bisherigen Geschäftsmodellen wurden die Kosten dem Signaturschlüssel-Inhaber aufgebürdet, während Einsparungen vor allem auf Seiten der Diensteanbieter im Electronic Government und Electronic Commerce zu erwarten gewesen wären. Dies ist jedoch kein Problem des Signaturrechts, da dieses keine Vorgaben für die Geschäftsmodelle der Zertifizierungsdiensteanbieter macht.

[72] S. dazu *Hornung* 2005, 253 ff.; *ders.*, DuD 2004, 15 ff.

zum anderen die Entscheidung, beide Dokumente – wie bisher – hinsichtlich der Prüfumgebungen miteinander kompatibel zu halten.

Vor diesem Hintergrund konnte die Entscheidung nur für oder gegen die Aufnahme der einzelnen biometrischen Merkmale in ihrer technischen Ausgestaltung im Reisepass, nicht aber für eine vollständig andere Ausgestaltung fallen. Die Entscheidung für Biometrie an sich bedingte überdies die Entscheidung für eine kontaktlose (RFID-)Schnittstelle entsprechend der Ausstattung des neuen Reisepasses.

Der im politischen Verfahren gefundene Kompromiss der freiwilligen Speicherung der Fingerabdrucksdaten widerspricht dem Vorstehenden nicht, sondern schöpft den verbleibenden Gestaltungsspielraum aus. Der deutsche Gesetzgeber hatte die Wahl zwischen verpflichtender oder freiwilliger Einführung einer oder beider der im Reisepass verwendeten Biometrien – faktisch aber kaum die Wahl einer alternativen technischen Gestaltung. Folgerichtig wurden im Entscheidungsprozess – soweit ersichtlich – technische Alternativen hinsichtlich folgender Weichenstellungen entweder ernsthaft erwogen oder verworfen:

- Alternativen hinsichtlich des Chips als Speichermedium (Magnetstreifen, verschlüsselte Drucktechniken etc.),
- Alternativen hinsichtlich der Übertragungstechnik mittels RFID (kontaktorientierte Schnittstelle),
- Alternativen hinsichtlich der gewählten biometrischen Merkmale Gesicht und Fingerabdruck (Iris, Handflächen, Venenmuster etc.),
- Alternativen hinsichtlich der Datenformate (Speicherung als Image).

Eine gewisse Ausnahme bilden Alternativen hinsichtlich der kryptographischen Sicherungsmechanismen, die teilweise durch die ICAO, teilweise durch europäische Vorgaben standardisiert sind. Die Vorgaben zur Sicherung in § 5 Abs. 6 PAuswG entsprechen dem Wortlaut nach § 4 Abs. 3 Satz 2 PassG. Die Regelungen in der Personalausweisverordnung sind jedoch erheblich detaillierter als die in der Passverordnung und verlangen zusätzliche Schutzmechanismen. Gemäß § 14 Abs. 1 Nr. 1 PAuswV ist insbesondere sicherzustellen, dass vor der Übermittlung personenbezogener Daten die Geheimnummer, die Zugangsnummer oder die Daten der maschinenlesbaren Zone (MRZ) eingegeben werden müssen. Überdies müssen Zugriffsrechte über Berechtigungszertifikate nachgewiesen werden (§ 14 Abs. 1 Nr. 2 PAuswV), und diese sind auf zur Identitätsfeststellung berechtigte Behörden und berechtige Diensteanbieter beschränkt (§ 14 Abs. 2 PAuswV). Im Ergebnis wird deshalb das System des Extended Access Control (EAC)[73] hier – anders als beim Pass – für sämtliche auf dem Chip gespeicherte Daten verbindlich vorgeschrieben.[74] Dies stellt eine erhebliche Verbesserung des technischen Schutzes dar.

Mit dem Vorbehalt dieser Ausnahme hat die zeitlich vorgelagerte Einführung des neuen Reisepasses insgesamt zwar keine rechtliche,[75] wohl aber eine technische – und in der Folge politische[76] – Weichenstellung gegeben.

3.2.2 Qualifizierte elektronische Signatur

Auf der Basis des signaturrechtlichen Regelungssystems (Signaturgesetz, Signaturverordnung mit Anhängen, Kontrolle und technische Vorgaben durch die Bundesnetzagentur) bestand

---

[73] S. hierzu *Kügler/Naumann*, DuD 2007, 176 ff.

[74] S. die Begründung, BR-Drs. 240/10, 43.

[75] S.o. 3.1.3.

[76] S.u. 3.3.5.

bereits vor Beginn der Arbeiten am neuen Personalausweisgesetz eine vollständige technische Infrastruktur für die Ausgabe und Nutzung von Signaturkarten. Diese technischen Weichenstellungen wurden weitgehend übernommen. Die Techniken der Signaturerzeugung, Generierung der Zertifikate und Signaturprüfung sind unverändert. Zwei technische Änderungen wurden demgegenüber vorgenommen:

Zum einen wurde mit dem neuen § 3 Abs. 1 Satz 2 SigV ein verändertes Verfahren der Zertifikatsbeantragung zugelassen, die nunmehr auch im Online-Verfahren – nämlich unter Verwendung des elektronischen Identitätsnachweises – möglich ist. Dies geschah in der Hoffnung, die Zugangshürden im Rahmen der Beantragung der optionalen Signaturfunktion abzusenken. Neben der starken Regulierung der Rechtsfolgen waren die hohen Vorgaben für die Erstregistrierung von den Akteuren im Bundesministerium des Innern, vor allem aber in der Wirtschaft (und hier wiederum insbesondere von Seiten der Banken) als Hemmnis für die Verbreitung der qualifizierten elektronischen Signatur identifiziert worden. Hierfür waren bereits mit der Novelle des Signaturgesetzes im Jahre 2004[77] – in der Literatur als „Lex Deutsche Bank“ bezeichnet[78] – die entsprechenden Anforderungen abgesenkt worden, ohne allerdings einen messbaren Erfolg hinsichtlich der Verbreitung von Signaturkarten zu erzielen.[79] In gewisser Weise wird diese Absenkung der Anforderungen durch § 3 Abs. 1 Satz 2 SigV n.F. konsequent zu Ende geführt. Die Beantragung mittels des elektronischen Identitätsnachweises ist technisch und organisatorisch sicherer zu beurteilen als die Lösung des § 5 Abs. 1 Satz 2 SigG bei den Banken, die sich auf Identifizierungsdaten stützen, die mitunter Jahre zuvor erhoben wurden.

Zum anderen ist auch die Anbindung von Signaturkarten über eine kontaktlose Schnittstelle neu. Die bisherigen Signaturkarten verfügen stattdessen über eine kontaktorientierte Schnittstelle.[80] Dies geht allerdings auf eine Sicherheitsbewertung des Bundesamts für Sicherheit in der Informationstechnik zurück, die zeitgleich während des Gesetzgebungsverfahrens geändert wurde. Die neue Bewertung lässt bei entsprechenden kryptographischen Verfahren den Einsatz kontaktloser Schnittstellen zu, dies allerdings für alle Signaturkarten, nicht nur für den neuen elektronischen Personalausweis. Die Sicherheitsmechanismen, die die kontaktlose Schnittstelle gegen solche Angriffe schützen soll, sind in der Technischen Richtlinie „eCards mit kontaktloser Schnittstelle als sichere Signaturerstellungseinheit“[81] beschrieben. Danach müssen Signaturkarten mit kontaktloser Schnittstelle über Sicherheitsmechanismen verfügen, die zum einen ein Äquivalent zum bewussten Stecken der Chipkarte in ein Terminal beinhalten und zum anderen ein Abhören und Manipulieren der Kommunikation mit dem vom Benutzer gewählten Terminal durch Angreifer ausschließen.[82]

Diese Sicherheitsmechanismen soll das Protokoll „Password Authenticated Connection Establishment (PACE)“ bieten, das bereits beim aktuellen Reisepass für die Zugangssicherung zu den biometrischen Daten verwendet wird. Es fordert hierfür eine Autorisierung des Terminals, eine gegenseitige Authentifizierung von Terminal und Chip und die Vereinbarung von ge-

---

77 Erstes Gesetz zur Änderung des Signaturgesetzes, BGBl I 2005, 2.

78 *Skrobotz*, DuD 2004, 410; zum Gesetz ausführlich *Roßnagel*, NJW 2005, 385.

79 Insofern gilt für die Problematik der fehlenden Verbreitung der qualifizierten elektronischen Signatur das oben in Fn. 71 gesagte.

80 S.a. *Hornung* 2005, 354 f.

81 Bundesamt für Sicherheit in der Informationstechnik, Technische Richtlinie TR-03117, eCards mit kontaktloser Schnittstelle als sichere Signaturerstellungseinheit, Version 1.0, abrufbar unter https://www.bsi.bund.de/ContentBSI/Themen/Elekausweise/TRundSchutzprofile/TR_Spez/TRnachArtRichtlinieSpez.html.

82 TR-03117 (Fn. 81), 7; s.a. *Bender/Kügler/Margraf/Naumann*, DuD 2008, 173 ff; zur rechtlichen Bewertung *Roßnagel*, DuD 2009, 403 ff.

meinsamen Sitzungsschlüsseln für die Verschlüsselung und den Datenintegritätsschutz der Kommunikation zwischen dem Chip und dem Terminal sowie deren Anwendung.[83] Das PACE-Protokoll beruht auf einer gemeinsamen, dem Chip und dem Terminal bekannten sechsstelligen Zugangsnummer (CAN – Card Access Number).[84] Diese Nummer ist auf der Karte aufgedruckt. Der Benutzer muss also die Karte optisch lesen,[85] um die Zugangsnummer zu kennen und verwenden zu können.[86] Alternativ kann die Nummer auch in einem Display auf der Karte angezeigt werden. In diesem Fall wird die Nummer in bestimmten kurzen Zeiträumen automatisch aktualisiert.[87] Je nach Ausstattung des Terminals kann der Nutzer, statt die Zugangsnummer einzugeben, diese auch an eine Leseeinheit des Terminals halten, die die Nummer direkt optisch lesen kann.[88] Wenn die an den Ausweischip übermittelte Nummer falsch ist, also nicht mit der im Chip gespeicherten Nummer übereinstimmt, kommt mit sehr hoher Wahrscheinlichkeit keine Kommunikation zwischen Terminal und Chip zustande.[89]

Unter Berücksichtigung dieser und einiger weiterer technischer Sicherheitsmaßnahmen ist die Nutzung einer kontaktlosen Schnittstelle zur Erstellung qualifizierter elektronischer Signaturen bereits nach geltendem Signaturrecht zulässig,[90] sodass dieses insoweit keine Einschränkungen für die Entwicklung beinhaltete. Die Anforderungen des § 2 Nr. 2 c) SigG (Erzeugung der Signatur mit Mitteln, die der Signaturschlüssel-Inhaber unter seiner alleinigen Kontrolle halten kann) und des § 15 Abs. 1 Satz 1 SigV (Gewährleistung, dass der Signaturschlüssel erst nach Identifikation des Inhabers durch Besitz und Wissen oder durch Besitz und ein oder mehrere biometrische Merkmale angewendet werden kann) können durch die PACE-Absicherung im Grundsatz erfüllt werden. Um die Zugangsnummer nach Möglichkeit geheim zu halten, war allerdings die Regelung des § 1 Abs. 1 Satz 3 PAuswG erforderlich, wonach vom Ausweisinhaber nicht verlangt werden darf, den Personalausweis zu hinterlegen oder in sonstiger Weise den Gewahrsam aufzugeben – außer gegenüber zur Identitätsfeststellung berechtigte Behörden sowie zur Einziehung und Sicherstellung.[91] Das Risiko wird weiter dadurch begrenzt, dass durch den elektronischen Identitätsnachweis ein Kopieren des Ausweises weitgehend überflüssig wird. In vielen Fällen wird aber noch immer rechtlich gefordert, dass der Prüfende zur Dokumentation der Prüfung den Ausweis kopieren muss. Dies hätte zur Folge, dass die Zugangsnummer mit kopiert und bei vielen dritten Stellen gespeichert würde. Diese rechtlichen Anforderungen müssen deshalb entweder durch die Verwendung des elektronischen Identitätsnachweises ersetzt werden, oder es müssen technische Mechanismen zur Verhinderung des Kopierens der Zugangsnummer ergriffen werden (Aufdruck auf Rückseite, Einsatz nicht kopierbarer Drucktechniken oder vergleichbare Maßnahmen).[92]

3.2.3 Elektronischer Identitätsnachweis

Die besondere Bedeutung des elektronischen Identitätsnachweises kommt bereits dadurch zum Ausdruck, dass dieser im Namen des neuen Gesetzes auftaucht. Technisch ist der elektronische Identitätsnachweis ein Authentisierungsinstrument, das allerdings gegenüber der bisherigen Challenge-Response-Authentisierung, die auf vielen Signaturkarten verfügbar ist, völlig neu konzipiert wurde. Diensteanbieter müssen sich zunächst mit einem Berechtigungs-

---

83 S. hierzu auch *Bender/Kügler/Margraf/Naumann*, DuD 2008, 173 ff.

84 *Bender/Kügler/Margraf/Naumann*, DuD 2008, 173, 176: „Karten-PIN“.

85 S. TR-03117 (Fn. 81), 8.

86 S. zu vergleichbaren Sicherheitsmechanismen beim Reisepass *Kügler/Naumann*, DuD 2007, 176, 178.

87 *Bender/Kügler/Margraf/Naumann*, DuD 2008, 173, 176.

88 Dies entspricht dem technischen Ablauf bei der Kontrolle der biometrischen Daten des neuen Reisepasses.

89 S. TR-03117 (Fn. 81), 8 f.

90 Näher *Roßnagel*, DuD 2009, 403 ff.

91 S.o. 2.3.

92 S. *Roßnagel*, DuD 2009, 403, 405 f.

zertifikat gegenüber dem Ausweischip authentisieren. Im Anschluss ist die Eingabe einer PIN durch den Ausweisinhaber erforderlich, bevor die im Berechtigungszertifikat genannten Angaben übermittelt werden.

Mit dieser völligen Neukonzeption verfolgten die Akteure im Bundesministerium des Innern und den nachgeordneten Behörden (insbesondere im BSI) aus technischer und politischer Sicht, soweit erkennbar, zwei Ziele:

- Zum einen sollte das Verfahren möglichst datenschutzfreundlich ausgestaltet werden. Hierzu dient in technischer Hinsicht insbesondere die technische Kopplung der Datenübertragung an die Berechtigungszertifikat der Diensteanbieter (§ 18 Abs. 4 PAuswG) und die Vorabprüfung der Diensteanbieter vor der Ausstellung der Berechtigungszertifikate mit ihren flankierenden Maßnahmen gemäß § 21 PAuswG.[93]
- Zum anderen sollten Vorgehensweisen vermieden werden, die sich nach der Analyse der Akteure bei der Einführung der qualifizierten elektronischen Signatur als Fehler herausgestellt hatten. Das betrifft neben den rechtlichen Fragen der Regulierung (s.o.) an dieser Stelle die technische Handhabung, etwa hinsichtlich der PIN, die beim elektronischen Identitätsnachweis durch den Benutzer frei wählbar sein soll.

3.3 Politik

Auf politischer Ebene lassen sich einige Grundentscheidungen und Weichenstellungen ausmachen, die der Einführung des neuen Personalausweises vorgelagert waren.

3.3.1 Grundentscheidung für Biometrie

Eine politische Grundentscheidung für den Einsatz von Biometrie in staatlichen Identitätspapieren in Deutschland lässt sich an mindestens zwei Punkten festmachen.

Zum einen existierte der bereits erwähnte Kompromiss zur Einführung biometrischer Daten im bisherigen Personalausweisrecht.[94] Allerdings wurde – soweit ersichtlich – von keinem Befürworter der Einführung biometrischer Daten in den neuen elektronischen Personalausweis das Argument bemüht, die Entscheidung sei dem Grunde nach durch die Regelung im Personalausweisgesetz bereits gefallen. Das ist insoweit interessant, als diese Bestimmungen rechtstechnisch zwar Nicht-Regelungen sind. Gerade weil sie als politische Formelkompromisse in Gesetzesform gegossen wurden, wäre aber zu erwarten gewesen, dass sie in der neuen Diskussion argumentativ verwertet werden.

Zum anderen war die Entscheidung für den Einsatz von Biometrie im Reisepass in Deutschland – über den Umweg der Entscheidung durch die Europäische Gemeinschaft – bereits gefallen. Von einigen Millionen Bundesbürgern waren für den neuen Reisepass bereits biometrische Daten erhoben worden. Auch dies dürfte in die Diskussion im Sinne eines Gewöhnungseffekts zumindest unterschwellig beeinflusst haben. Rechtstechnisch wie politisch unterscheiden sich Pass und Personalausweis (bis zur Einführung des elektronischen Identitätsnachweises und der Signaturfunktion des neuen Personalausweises) im Grunde nur in einem wesentlichen Punkt: Während (in Deutschland) eine Pflicht zum Besitz eines der beiden Dokumente – im Regelfall der Personalausweis, § 1 Abs. 1 Satz 1 PAuswG – besteht, benötigen nur diejenigen Bürger einen Reisepass, die in ein Land außerhalb der Europäischen Union und einiger weiterer Staaten reisen wollen, in denen der deutsche Personalausweis nicht als Grenzübertrittspapier anerkannt wird.

---

93 Näher *Roßnagel/Hornung*, DÖV 2009, 301, 303 ff.

94 S.o. 3.1.2.

Auf die Biometrie gewendet bedeutet dies: Während beim Pass noch die Argumentation möglich ist, dass dieser ein freiwilliges Dokument und insoweit auch die staatliche Erhebung der biometrischen Daten freiwillig sei (obwohl dies natürlich der Sache nach in vielen Fällen wegen wichtiger Auslandsreisen bezweifelt werden kann), ist ein derartiges Ausweichen beim Personalausweis nicht möglich. Dieser führt damit in der gegenwärtigen Ausgestaltung zu einer vollständigen Pflicht aller Bürger ab Vollendung des 16. Lebensjahres zur Abgabe biometrischer (Gesichts-)Daten. Dieser Aspekt wurde in der politischen Diskussion zwar angeführt,[95] spielte aber keine entscheidende Rolle.

3.3.2 Grundentscheidung gegen bestimmte Speicherorte

Die beim Pass getroffen Entscheidung gegen eine zentrale Speicherung der biometrischen Gesichtsdaten wurde in § 26 Abs. 4 PAuswG übernommen. Gleiches gilt für die Entscheidung, eine Speicherung der biometrischen Fingerabdrucksdaten außerhalb des Passes nach Abschluss des Produktionsprozesses zu untersagen (§ 17 Satz 4 und § 26 Abs. 2, Abs. 3 Satz 2 PAuswG). Zumindest letzteres stellt offenbar innerhalb den Mitgliedstaaten der Europäischen Union eine singuläre deutsche Besonderheit dar. Wie oben erwähnt, wurde von Seiten der Befürworter einer Registerspeicherung darauf verzichtet, den beim Reisepass geschlossenen Kompromiss in Frage zu stellen.[96]

3.3.3 Grundentscheidung für privat betriebene Zertifizierungsinfrastruktur

Im Vorfeld der Verabschiedung des ersten deutschen Signaturgesetzes im Jahre 1997 wurde ausführlich die Frage erörtert, ob die Erbringung von Zertifizierungsdiensten eine staatliche Infrastrukturaufgabe sein oder privaten Anbietern überlassen werden sollte.[97] Der Gesetzgeber entschied sich letztlich für das private Modell; im europäischen Kontext sind beide Varianten zu finden. Die deutsche Grundentscheidung wurde im Gesetzgebungsverfahren von keiner Seite in Frage gestellt. Allerdings ist die Bereitstellung des elektronischen Identitätsnachweises durch staatliche Stellen (s. sogleich) eine nicht zu unterschätzende Einschränkung des Bedürfnisses nach Anwendungen der qualifizierten elektronischen Signatur.

3.3.4 Entscheidung für staatliche Infrastruktur beim elektronischen Identitätsnachweis

Anders als bei der Infrastruktur für die qualifizierte elektronische Signatur betreibt der Staat die Infrastruktur für den elektronischen Identitätsnachweis selbst: Er wird durch den staatlichen Personalausweis bereitgestellt, die Identität des Inhabers wird durch staatliche Personalausweisbehörden kontrolliert, eine staatliche Stelle (das Bundesverwaltungsamt) erbringt den Sperrdienst, die Ausgabe der Berechtigungszertifikate wird zumindest vorläufig durch eine staatliche Stelle (ebenfalls das Bundesverwaltungsamt) selbst durchgeführt und auch langfristig staatlich überwacht werden.

Der elektronische Identitätsnachweis ist immer dann ein Ersatz für die qualifizierte elektronische Signatur, wenn es um ein funktionales Äquivalent für die Vorlage eines Ausweises in der realen Welt geht. Demgegenüber ist weiterhin eine qualifizierte elektronische Signatur als Äquivalent zur eigenhändigen Unterschrift erforderlich, also hauptsächlich wenn bestimmte Formvorschriften erfüllt werden müssen oder eine Beweissicherung bestimmter Handlungen angestrebt wird.[98] Beide Anwendungen des neuen Personalausweises sind für sicheres elekt-

---

[95] So vom Bundestagsabgeordneten der Fraktion Bündnis 90/Die Grünen *Wieland*, s. http://www.heise.de/newsticker//meldung/107691.

[96] S.o. 2.1.

[97] Zur Gesetzgebungsgeschichte s. *Roßnagel*, in: ders. Recht der Multimediadienste, Einl. SigG Rn. 42 ff.

[98] S. *Roßnagel/Hornung*, DÖV 2009, 301, 304 f.

ronisches Handeln im Electronic Government und Electronic Commerce notwendig, sie haben aber zum Teil unterschiedliche, zum Teil ergänzende, zum Teil potenziell konkurrierende Funktionen. Die Praxis wird zeigen müssen, inwieweit die erste Gruppe (also diejenigen Dienste, in denen nur ein sicherer Identitätsnachweis erforderlich ist) alleine entscheidende Fortschritte für sichere Rechts- und Geschäftsprozesse im Internet anstoßen kann.

3.3.5 Technische „Zwänge“ als politische Argumente

Technische Weichenstellungen ziehen politische Argumente nach sich, und zwar in einem mehrfachen Sinn. Erstens ist es sowohl aus Sicht der Kosten wie der der Praktikabilität an Kontrollstellen unmittelbar einsichtig, dass Pass und Personalausweis mit demselben Prüfinstrumentarium handhabbar sein sollten. Zweitens dürfte es ein starkes Argument sein, eine für ein Identifizierungsdokument eingeführte neue Identifizierungstechnologie auch bei anderen Identifizierungsdokumenten zu nutzen – umso mehr, als diese auch bisher technisch weitgehend identisch ausgestaltet waren.

Nur am Rande sei angemerkt, dass die letztlich vielleicht hinsichtlich der Biometrie entscheidende Weichenstellung unter demokratietheoretischen Gesichtspunkten durchaus kritisch ist: Die europäische Passverordnung ist insoweit bereits in sich problematisch, da das Europäische Parlament im Verfahren nach Art. 67 I EGV nur konsultiert werden musste und überdies in wichtigen Grundfragen überstimmt wurde.[99] Über den Umweg der technischen Kompatibilität und ihrer politischen Verwertung erlangte diese in sich problematische Maßnahme faktisch sogar hohen Einfluss auf einen Bereich, in dem die Union keine rechtliche Kompetenz besaß.

Im Bereich des elektronischen Identitätsnachweises und der kontaktlosen Ausgestaltung der Signaturfunktion des elektronischen Personalausweises wurden hingegen technisch neue Wege beschritten. Daran wird deutlich, dass offenbar auch neue Lösungen möglich waren, wenn sie von den entscheidenden Akteuren gewollt wurden. Auch diesen Akteuren wurden mutmaßlich für ihre Neulösung technische Probleme und Zwänge genannt, die jedoch überwunden wurden. Technische Zwänge sind damit ein starkes Argument in der Diskussion, das von Akteuren ohne starke Handlungsmacht (außerparlamentarische Kritiker, Opposition im Bundestag) in der Regel nicht ausgehebelt werden kann, wohl aber von entscheidenden Akteuren in den zuständigen Ministerien, wenn sie über entsprechende politische Rückendeckung verfügen. Technischer Zwänge sind damit nur teilweise „objektiv“, sondern vorwiegend als kommunikative Figur zu sehen.

Beim neuen elektronischen Identitätsnachweis wurde dementsprechend explizit etwas Neues konstruiert. Wie bereits erwähnt, verfügen die bisherigen Signaturkarten regelmäßig über eine Authentisierungsfunktion, die jedoch technisch anders funktioniert. Es wurde erheblicher Aufwand betrieben, um den neuen elektronischen Identitätsnachweis datenschutzfreundlich auszugestalten und von der qualifizierten elektronischen Signatur technisch abzukoppeln.

Auch hinsichtlich der Signaturfunktion selbst hat sich der bereits vorhandene Technikstrang insoweit nicht durchgesetzt, wie er die Datenübertragung vom Chip des elektronischen Personalausweises betrifft. Während die bisherigen Signaturkarten durchweg mit einer kontaktorientierten Schnittstelle operieren, wird der elektronische Personalausweis in allen drei Funktionen (Biometrie, elektronischer Identitätsnachweis, qualifizierte elektronische Signatur) die Daten über eine kontaktlose Schnittstelle übermitteln.[100] Hierfür sprach die geringere Fehler-

[99] S.o. 3.1.3.

[100] S.o. 3.2.2.

anfälligkeit dieser Lösung über einen längeren Zeitraum hinweg.[101] Das Signaturrecht stellte für die Nutzung einer kontaktlosen Schnittstelle keine unüberwindlichen Hindernisse in den Weg.[102] Die bisherigen technischen Lösungen werden mit der neuen Schnittstellentechnologie nicht zwingend obsolet, dürften aber in Zukunft nicht mehr weiter verfolgt werden. Wegen der bisher kaum erfolgten Verbreitung von Signaturkarten und kontaktorientierten Kartenlesegeräten war insoweit allerdings auch kaum mit Widerstand zu rechnen. Soweit ersichtlich, protestierten weder die Zertifizierungsdiensteanbieter, die bisher kontaktorientierte Systeme vertreiben, noch Anwender, die derartige Systeme einsetzen, gegen die technische Wende hinsichtlich der Schnittstelle.

Unter dem Gesichtspunkt der Verbreitung sicherer Signaturerstellungseinheiten und der dazugehörigen Infrastruktur – und ebenso aus Sicht der Ausweisinhaber und der Anbieter von Anwendungen im Electronic Government und Electronic Commerce – dürfte die technische Entscheidung hinsichtlich der Schnittstelle keine große Rolle spielen, da bisher keine weite Verbreitung von kontaktorientieren Kartenlesegeräten erfolgt ist. Erfolgversprechend dürfte insoweit nur die subventionierte oder kostenlose Abgabe von (nunmehr kontaktlosen) Lesegeräten sein, wie sie etwa durch den Bund unter der Bezeichnung „Sicherheitskits“ im Rahmen des „Konjunkturpakets II“ vorgesehen ist.[103] Ohnehin ist die Verbreitung der Karteninfrastruktur nur eines von mehreren Problemen für den flächendeckenden Einsatz qualifizierter elektronischer Signaturen, das außerdem in der Bedeutung hinter dem Fehlen entsprechender Anwendungen und angemessener Entgeltmodelle zurücktreten dürfte.[104]

3.3.6 Förderung des Electronic Government

Eine letzte wichtige politische Grundentscheidung liegt in dem hohen Gewicht, welches das Gesamtvorhaben der Förderung des Electronic Government beimisst. Der elektronische Identitätsnachweis ist zwar von der technischen und rechtlichen Konzeption her nicht auf den Kontakt zur Verwaltung begrenzt: Personalausweisinhaber, die mindestens 16 Jahre alt sind, können ihren Personalausweis gemäß § 18 Abs. 1 Satz 1 PAuswG dazu verwenden, ihre Identität „gegenüber öffentlichen und nichtöffentlichen Stellen“ elektronisch nachzuweisen. Auch werden wichtige Anwendungsfelder des elektronischen Identitätsnachweises gerade im privaten Bereich liegen, nämlich bei der Kontoeröffnung (§ 6 GwG n.F.) und im Umfeld von Angeboten für Erwachsene.[105]

Trotz dieser Anwendungsmöglichkeiten im privaten Bereich war im Gesetzgebungs- und Konzeptionsprozess deutlich erkennbar, dass ein wichtiges Motiv der Akteure darin lag, sichere und einfache Anwendungen im Bereich des Electronic Government zu fördern. Die Verwaltung hat ein erhebliches Interesse daran, möglichst viele Verwaltungsprozesse elektronisch abzubilden. Der elektronische Identitätsnachweis verschafft ihr hierzu eine entscheidende Bedingung. Überdies dürften die Voraussetzungen für die Vergabe der Berechtigungszertifikate zum Zugriff auf die Daten des elektronischen Identitätsnachweises nach § 21 PAuswG mutmaßlich für Verwaltungsbehörden leichter zu erfüllen als für private Diensteanbieter.

---

[101] Zu den Problemen unterschiedlicher Gültigkeitszeiträume von Personalausweis, qualifiziertem Zertifikat und der verwendeten kryptographischen Algorithmen s. *Roßnagel/Gitter*, in: Reichl/Roßnagel/Müller 2005, 100 f., 221 f.; *Hornung* 2005, 330 ff.

[102] S.o. 3.2.2.

[103] S. Antwort der Bundesregierung auf die Kleine Anfrage der Fraktion der FDP, BT-Drs. 16/12420.

[104] S. die Anmerkungen in Fn. 71.

[105] In Deutschland ansässige Anbieter müssen insoweit zuverlässige Altersverifikationssysteme betreiben, um nicht gegen § 4 Abs. 2 JMStV, § 15 Abs. 2 JuSchG und § 184 StGB zu verstoßen; hierzu ist der elektronische Identitätsnachweis ein Mittel, s. *Roßnagel/Hornung/Schnabel*, DuD 2008, 168, 169; ausführlich *Altenhain/Heitkamp*, K&R 2009, 619 ff.

Die Gewichtsverschiebung von der Wirtschaftsförderung zum Electronic Government lässt sich auch an der Zuständigkeit der Ministerien ablesen. Die erste Machbarkeitsstudie zum „Digitalen Personalausweis“ wurde noch verantwortlich vom Bundesministerium für Wirtschaft und Arbeit vergeben; das Bundesministerium des Innern war lediglich beteiligt. Die Akteure aus dem Bundesministerium des Innern waren im Rahmen der ersten Studie für den Bereich der Biometrie zuständig und arbeiteten an einem vom Bundesministerium für Wirtschaft und Arbeit finanzierten Projekt mit. Für das Gesetz über den elektronischen Personalausweis war jedoch das Bundesministerium des Innern federführend, das auch ansonsten die Aktivitäten der Bundesregierung im Bereich des Electronic Government koordiniert und maßgeblich durchführt. Die entsprechende Abteilung des Bundesministeriums des Innern[106] ist inzwischen voll ausgebaut und verfügt über hinreichende personelle und finanzielle Mittel, um die Projekte selbst zu initiieren und durchzuführen.

Während der Arbeiten am Gesetzesentwurf wurde von den Beteiligten des Öfteren das Argument vorgebracht, der Nachweis der Identität sei zumindest insoweit anders als die qualifizierte elektroniche Signatur zu behandeln, als ersteres eine genuin staatliche Aufgabe sei. Insoweit wird – anders als beim qualifizierten Zertifikat nach § 7 SigG[107] – eine Funktionalität eingeführt, die schon von ihrer Grundkonzeption her eine eindeutige Identifizierung des Ausweisinhabers auch beim elektronischen Erstkontakt ermöglicht.

4 Beschreibung nach Akteuren

In diesem Kapitel wird überblicksartig die Akteursperspektive eingenommen und untersucht, welche Akteure sich von welchen Pfaden haben beeinflussen lassen, beziehungsweise welche Pfade als Argumente für sich in Anspruch genommen haben. Dabei wird kein Anspruch auf Vollständigkeit erhoben; es geht mehr um einzelne Beobachtungen.

Zunächst lässt sich für die Einführung biometrischer Daten eine Teilung in zwei Gruppen von Akteuren feststellen, die diese befürwortete oder ablehnte. Die Trennlinie verläuft tendenziell nicht zwischen den staatlichen Gewalten, sondern zwischen Akteuren, die mehr die Kontrollmöglichkeiten befürworten, und denen, die den Grundrechtsschutz höher gewichten. Mit anderen Worten wurde die Einführung sowohl vom Bundeministerium des Innern als auch von vielen Bundestagsabgeordneten der Regierungsfraktionen unterstützt, zumindest zwischenzeitlich aber vom Bundesministerium der Justiz und einigen Abgeordneten der SPD abgelehnt. Die Opposition nahm durchgängig eine ablehnende Haltung ein.

Der elektronische Identitätsnachweis hat sich de facto in der Form durchgesetzt, in der er in der ersten Planungsphase des Bundesministeriums des Innern konzipiert wurde. Offensichtlich kamen hier zwei Faktoren zusammen, nämlich einerseits ein hohes Interesse der Akteure im Ministerium hinsichtlich des elektronischen Identitätsnachweises, der als Basisfunktionalität für Electronic Government und Electronic Commerce verstanden wurde, und andererseits ein verhältnismäßig geringes Interesse anderer Akteure, diese Funktion in Frage zu stellen.

Mit dem Wechsel der Federführung vom Bundesministerium für Wirtschaft und Arbeit zum Bundesministerium des Innern ging ein Wechsel der Akteure einher. Fortan waren maßgeblich Personen beteiligt, die im Bundesministerium des Innern und den nachgeordneten Behörden einen klaren Schwerpunkt auf Fragen des Electronic Government und der IT-Sicherheit legten. Eine Rolle spielte dabei sicherlich die inzwischen voll ausgebaute und etablierte Abteilung im Bundesministerium des Innern.[108]

---

[106] Referat IT 4: Pass- und Ausweiswesen, Identifizierungssysteme.

[107] S.o. 3.1.4.

[108] Referat IT 4: Pass- und Ausweiswesen, Identifizierungssysteme; s. bereits oben 3.3.6.

Die Abweichung gegenüber dem Reisepass (nur freiwillige Speicherung der Fingerabdrücke) wurde von den Befürwortern der Speicherung biometrischer Daten, insbesondere vom Bundesministerium des Innern, ohne allzu großen Widerstand hingenommen. Dies lässt den Schluss zu, dass die Akteure nicht wegen dieses Punktes das Gesamtprojekt – insbesondere hinsichtlich der Signaturfunktion und dem elektronischen Identitätsnachweis –scheitern lassen wollten. Dies ist insbesondere vor dem Hintergrund des Zeitproblems plausibel, das bei weiteren Verzögerungen entstanden wäre. Eine fortdauernde und möglicherweise eskalierende Diskussion zwischen den politischen Akteuren hätte zu dem Risiko geführt, den Gesetzesentwurf nicht mehr in der laufenden Legislaturperiode verabschieden zu können.

Die Argumentationsmodi der Gegner des neuen Personalausweises lassen sich nur sehr schwer einem Pfad zuordnen. In Bezug auf die biometrischen Daten wurden im Wesentlichen dieselben Argumente wie zum elektronischen Reisepass vorgebracht. Die Argumente zur Signaturfunktion und zum elektronischen Identitätsnachweis beschränkten sich im Wesentlichen auf eine sehr pauschale Skepsis gegenüber der Bereitstellung einer Identifizierungsinfrastruktur durch den Staat und setzten sich an so gut wie keiner Stelle mit der Konzeption im Detail oder den Einzelheiten des Grobkonzepts auseinander.

5 Bewertung

In der Gesamtbewertung dürfte der bisherige Personalausweis nur einer von mehreren Pfaden der Entwicklung gewesen sein. Sein Charakter als am weitesten verbreitetes Identifizierungsinstrument in Deutschland hat zwar den Boden für die Weiterentwicklung zum elektronischen Personalausweis gebildet, die konkreten technischen Entwicklungen waren aber in aller Regel von anderen Faktoren beeinflusst.

Hinsichtlich der Einführung biometrischer Daten dürfte der neue Reisepass der entscheidende Pfad gewesen sein. Das betrifft die Tatsache der Einführung, die Auswahl der Merkmale (andere biometrische Merkmale als Gesicht und Fingerabdruck wurden, soweit ersichtlich, zu keinem Zeitpunkt und von keinem Akteur ins Spiel gebracht), die Wahl des Speichermediums (RFID-Chip), die kryptographischen Sicherungsmechanismen (mit Ausnahme der erweiterten Absicherung aller Daten durch das EAC-Protokoll)[109] und die Regelungstechnik (Formulierung der Bestimmungen des Personalausweisgesetzes in weitgehender Anlehnung an die des Passgesetzes).

Die Signaturfunktion des Personalausweises folgt hinsichtlich der kontaktlosen Schnittstelle nicht dem bisherigen Technologiepfad, sondern dem des bisherigen biometrischen Reisepasses. Dagegen werden mindestens zwei Pfade fortgeschrieben:

- Erstens handelt es sich um ein „Wiederaufflackern“ der Debatte um die Rolle des Staates im System der Zertifizierungsdienste.[110] Die Grundentscheidung zugunsten des privaten Betriebs von Zertifizierungsdiensten wurde zwar nicht angetastet, die verpflichtende Ausgabe sicherer Signaturerstellungseinheiten und die Rolle der Personalausweisbehörden (deren Identifizierung der Antragsteller in Folge der Ermöglichung einer Online-Beantragung des qualifizierten Zertifikats den „Sicherheitsanker“ des gesamten Systems bilden wird) stehen jedoch für eine erheblich aktivere Rolle des Staates als im bisherigen System.
- Zweitens führt die Erleichterung des Online-Zugangs zu qualifizierten Zertifikaten die Maßnahmen des Staates fort, die bereits im Rahmen des 1. Signaturgesetzänderungsgesetzes entsprechende Erleichterungen (insbesondere im Bankenbereich) ermöglicht

[109] S.o. 3.2.1.

[110] S.o. 3.3.3.

hatten.[111] Gegenüber diesen Erleichterungen weist die Beantragung mittels des elektronischen Identitätsnachweises eine höhere Sicherheit auf. Diese ähnelt eher dem bisherigen Verfahren einer direkten Identifizierung mit Personalausweis, weil in beiden Fällen der Sicherheitsanker die Identifizierung durch die Personalausweisbehörde und die Verwendung eines hoheitlichen Ausweisdokuments ist.

Am wenigsten Determinanten lassen sich für den elektronischen Identitätsnachweis ausmachen. Dieser ist in Teilen seiner Umsetzung eine Reaktion auf die Erfahrungen mit der bislang fehlgeschlagenen Verbreitung der qualifizierten elektronischen Signatur. In allen wesentlichen Grundzügen handelt es sich jedoch um eine Neukonzeption.

Einen großen Anteil an der Entwicklung des elektronischen Identitätsnachweises hatte die Konzeption des qualifizierten Zertifikats in § 7 SigG, die zumindest beim elektronischen Erstkontakt keine eindeutige Identifizierung des Signaturschlüssel-Inhabers zulässt.[112] Eine durchaus naheliegende Alternative wäre insoweit gewesen, die Regelung um eine Personenkennziffer oder die Personalausweisnummer zu ergänzen. Soweit ersichtlich, wurde dies nicht erwogen.

Mutmaßlich sind hierfür zwei Gründe ursächlich. Zum einen sind nach überwiegender Auffassung und Rechtsprechung entsprechende Daten im deutschen Verfassungs- und einfach Datenschutzrecht entweder vollständig unzulässig oder nur unter sehr eingeschränkten Bedingungen zulässig.[113] Ein derartiger Plan hätte deshalb möglicherweise erheblichen politischen Widerstand hervorgerufen. Zum anderen würde eine Erweiterung des qualifizierten Zertifikats keine Verbreitung einer Authentisierungsinfrastruktur zur Folge haben, solange dieses Zertifikat – wie in der gegenwärtigen Konzeption – beim Personalausweis freiwillig ist und für den Ausweisinhaber mit Kosten verbunden ist. Mit anderen Worten wäre das gesetzgeberische Ziel, jedem Ausweisinhaber eine Identifizierungsmöglichkeit in elektronischen Rechts- und Geschäftsprozessen zur Verfügung zu stellen, nur bei einer verpflichtenden Signaturfunktion mit gleichzeitiger Gebührenerhöhung, oder bei einer Übernahme der Zertifikatsgebühren durch den Staat erreicht worden. Diese Lösungen hätten entweder verfassungsrechtliche oder finanzielle Probleme aufgeworfen. Es ist nicht bekannt, ob diese Wege ernsthaft erwogen wurden, die genannten Probleme wären aber in jedem Fall ausreichend Grund gewesen, diese Alternativen nicht weiter zu verfolgen.

Alle Lösungen mit Verwendung der qualifizierten elektronischen Signatur hätten schließlich einen Bedeutungszuwachs der Akteure im Bundesministerium für Wirtschaft bedeutet. Das Gesamtprojekt aus elektronischem Personalausweis, Signaturfunktion und elektronischem Identitätsnachweis befindet sich demgegenüber unter ausschließlicher Zuständigkeit des Bundesministeriums des Innern. Die maßgeblichen Akteure können sich dementsprechend sicher sein, dass spätestens nach zehn Jahren jeder Ausweisinhaber über eine entsprechende Funktion verfügt oder verfügen kann.

Im Vergleich zu anderen Staaten ist auf die Spezifika der deutschen Entwicklung hinzuweisen. Da es sich bei dem vorgenannten Punkt um eine deutsche Besonderheit handelt – die europäische Signaturrichtlinie schreibt die Verwendung einer Personenkennziffer im qualifizierten Zertifikat weder vor, noch verbietet sie sie[114] –, folgt daraus für die Vergangenheit,

---

[111] S.o. 3.2.2.

[112] S.o. 3.1.4.

[113] S. BVerfGE 27, 1 (6); 65, 1, 53 (57). Ein einheitliches Personenkennzeichen wurde auch vom Rechtsausschuss des Bundestages für verfassungswidrig erklärt, s. BT-Drs. 7/5277, 3. Vgl. zur Problematik aus personalausweisrechtlicher Sicht und zu den faktischen Grenzen eines Verbots eines solchen Personenkennzeichens unter den Bedingungen moderner Datenverarbeitung *Hornung* 2005, 159 ff.

[114] S.o. 3.1.4.

dass ein entsprechender Pfad in denjenigen Ländern eher unwahrscheinlicher ist, die eine Personenkennziffer oder ein vergleichbares eindeutig identifizierendes Datum im qualifizierten Zertifikat vorgeschrieben haben. Für die Zukunft bleibt zweifelhaft, ob sich der deutsche Pfad fortsetzen wird. Allerdings ist die Bundesregierung derzeit bestrebt, die deutsche Lösung auch auf der europäischen Ebene zu propagieren.

Insgesamt handelt es sich bei dem elektronischen Identitätsnachweis insoweit tatsächlich um eine völlige rechtliche und technische Neukonstruktion, die – soweit ersichtlich – relativ autonom durch die Akteure im Bundesministerium des Innern und den nachgeordneten Behörden (insbesondere dem Bundesamt für Sicherheit in der Informationstechnik) entwickelt und von den übrigen Akteuren jenseits pauschaler Angriffe nie in grundsätzlichen Zügen in Frage gestellt wurde. Insoweit könnte man davon sprechen, dass es zwar eine Reihe „negativer“ Pfade für die Entwicklung gab (im Sinne verwandter, aber nicht erfolgreicher Vorprojekte), aber keinen „positiven“ Pfad, der sich als Vorbild beschreiben ließe.

Schlussendlich lässt sich nicht abschließend beantworten, ob der deutsche Weg insoweit nachvollziehbar ist, als die Aufgabe, jedem Bürger eine Möglichkeit zum Identitätsnachweis in elektronischen Rechts- und Geschäftsprozessen bereitzustellen, tatsächlich eine originär staatliche ist. Wo eine staatliche Stelle in anderen Staaten als alleiniger Zertifizierungsdiensteanbieter auftritt, spricht einiges dafür, dass dies so gesehen wird. Konzeptionell spricht allerdings nichts dagegen, eine derartige Funktion über Private abzuwickeln: Mit einer einfachen Erweiterung des Zertifikatsinhalts um eine staatliche Personenkennziffer bei privatwirtschaftlichem Betrieb der Zertifizierungsdienstleistungen könnte man die erörterten Probleme ebenfalls lösen oder gar nicht erst entstehen lassen.[115] Inwieweit ein solches Vorgehen international vorkommt, müsste weiter untersucht werden.

[115] Dies gilt vorbehaltlich der sonstigen Verbreitungsprobleme der qualifizierten elektronischen Signatur, s. dazu oben Fn. 71 und den zugehörigen Text.

Literaturverzeichnis

Altenhain, K. / *Heitkamp, A.*, Altersverifikation mittels des elektronischen Personalausweises, K&R 2009, 619.

Bender, J. / *Kügler, D.* / *Margraf, M.* / *Naumann, I.*, Sicherheitsmechanismen für kontaktlose Chips im deutschen elektronischen Personalausweis. Ein Überblick über Sicherheitsmerkmale, Risiken und Gegenmaßnahmen, DuD 2008, 173 (auch abrufbar unter http://www.teli.de/pdf/DuD_3_2008_Sicherheitsmechanismen_Personalausweis_pdf.pdf).

Bundesministerium des Innern, Einführung des elektronischen Personalausweises in Deutschland, Grobkonzept - Version 2.0, o.O., Stand 2. Juli 2008, abrufbar unter http://www.bmi.bund.de/cae/servlet/contentblob/122648/publicationFile/9170/Grobkonzept_Personalausweis.pdf;jsessionid=1335CA26A4BB480AC69B7EA44DB59A6A.

Helmbrecht, U. / *Thielmann, H.* / *Ziemer, A.* (Hrsg.), Elektronischer Personalausweis und E-Identity, Gespräch des Münchner Kreises, München 2007.

Helmbrecht, U. / *Thielmann, H.* / *Ziemer, A.* (Hrsg.), Elektronischer Personalausweis und E-Identity. 2. Berliner Gespräch des Münchner Kreises, München 2008.

Hornung, G., Datenschutz für Chipkarten. Die Anwendung des § 6c BDSG auf Signatur- und Biometriekarten, DuD 2004, 15 (auch abrufbar unter http://www.uni-kassel.de/fb7/provet/hornung/dud_2004_01_15-20_datenschutz_chipkarten.pdf).

Hornung, G., Biometrische Systeme - Rechtfragen eines Identifikationsmittels der Zukunft, KJ 2004, 344.

Hornung, G., Die digitale Identität. Rechtsprobleme von Chipkartenausweisen: digitaler Personalausweis, elektronische Gesundheitskarte, JobCard-Verfahren, Baden-Baden, 2005 (auch abrufbar unter http://kobra.bibliothek.uni-kassel.de/handle/urn:nbn:de:hebis:34-2007113019808).

Hornung, G., Elektronische Zertifikate, Ausweise und Pseudonyme - Voraussetzungen der Selbstbestimmung, in: Roßnagel, A. (Hrsg.), Allgegenwärtige Identifizierung? Neue Identitätsinfrastrukturen und ihre rechtliche Gestaltung, Baden-Baden 2006, 53.

Hornung, G., Fingerabdrücke statt Doktortitel: Paradigmenwechsel im Passrecht, DuD 2007, 181 (auch abrufbar unter http://www.uni-kassel.de/fb7/provet/hornung/dud_2007_03_181-185_paradigmenwechsel_passrecht.pdf).

Kügler, D. / *Naumann, I.*, Sicherheitsmechanismen für kontaktlose Chips im deutschen Reisepass, DuD 2007, 176 (auch abrufbar unter https://www.bsi-fuer-buerger.de/cae/servlet/contentblob/480204/publicationFile/31113/dud_03_2007_kuegler_naumann_pdf.pdf).

Manssen, G. (Hrsg.), Telekommunikations- und Medienrecht. Kommentar, Loseblatt, Berlin.

Pallasky, A., Datenschutz in Zeiten globaler Mobilität. Eine Untersuchung des Verhältnisses von Datenschutz und Gefahrenabwehr im Reisebereich, Baden-Baden 2007.

Reichl, H. / *Roßnagel, A.* / *Müller, G.*, Digitaler Personalausweis. Eine Machbarkeitsstudie, Wiesbaden 2005.

Reisen, A., „Nicht ohne Datenschutz“, Heft 8/2007 der Kommune 21, 18.

Roßnagel, A., (Hrsg.), Recht der Multimediadienste. Kommentar zum IuKDG und zum MDStV, Loseblatt, München 1999 ff.

Roßnagel, A., Das neue Recht elektronischer Signaturen. Neufassung des Signaturgesetzes und Änderung des BGB und der ZPO, NJW 2001, 1817.

Roßnagel, A., Der elektronische Ausweis. Notwendige und mögliche Identifizierung im E-Government, DuD 2002, 281.

Roßnagel, A., Datenschutz in Signaturverfahren, in: ders. (Hrsg.), Handbuch zum Datenschutzrecht. Die neuen Grundlagen für Wirtschaft und Verwaltung, München 2003, Kapitel 7.7.

Roßnagel, A., Elektronische Signaturen mit der Bankkarte? Das Erste Gesetz zur Änderung des Signaturgesetzes, NJW 2005, 385.

Roßnagel, A., Die Ausgabe sicherer Signaturerstellungseinheiten, MMR 2006, 441.

Roßnagel, A., Der elektronische Personalausweis als sichere Signaturerstellungseinheit. Können Signaturkarten kontaktlos genutzt werden?, DuD 2009, 403.

Roßnagel, A. / *Hornung, G.*, Reisepässe mit elektronischem Gesichtsbild und Fingerabdruck. Die EG-Verordnung 2252/2004 über Normen für Sicherheitsmerkmale und biometrische Daten in von den Mitgliedsstaaten ausgestellten Pässen und Reisedokumenten, DÖV 2005, 983.

Roßnagel, A. / *Hornung, G.*, Ein Ausweis für das Internet. Der neue Personalausweis erhält einen "elektronischen Identitätsnachweis", DÖV 2009, 301.

Roßnagel, A. / *Hornung, G.* / *Schnabel, C.*, Die Authentisierungsfunktion des elektronischen Personalausweises aus datenschutzrechtlicher Sicht, DuD 2008, 168 (auch abrufbar unter http://www.uni-kassel.de/fb7/provet/hornung/dud_2008_03_168-172_authentisierung_eperso.pdf).

Roßnagel, A. / *Hornung, G.* / *Knopp, M.* / *Wilke, D.*, De-Mail und Bürgerportale. Eine Infrastruktur für Kommunikationssicherheit, DuD 2009, 728 (auch abrufbar unter http://cms.uni-kassel.de/unicms/fileadmin/groups/w_030405/Gerrit_Hornung/Rossnagel_Hornung_Knopp_Wilke__De-Mail_und_Buergerportale__DuD_2009__728.pdf).

Roßnagel, A. / *Pfitzmann, A.* / *Garstka, H.*, Modernisierung des Datenschutzrechts. Gutachten im Auftrag des Bundesministeriums des Innern, Berlin 2001 (auch abrufbar unter http://www.computerundrecht.de/media/gutachten.pdf).

Schliesky, U. (Hrsg.), Gesetz über Personalausweise und den elektronischen Identitätsnachweis. Kommentar, Kiel 2009.

Schulz, S., Der neue "E-Personalausweis" - elektronische Identitätsnachweise als Motor des E-Government, E-Commerce und des technikgestützten Identitätsmanagement?, CR 2009, 267.

Skrobotz, J., Lex Deutsche Bank: Das 1. SigÄndG. Anmerkungen zum Entwurf eines Ersten Deutschen Gesetzes zur Änderung des Signaturgesetzes (Stand 1. April 2004), DuD 2004, 410.

Stach, H., Mit Bürgerportalen für einfach sichere, vertrauliche und verbindliche elektronische Kommunikation, DuD 2008, 184.

Abkürzungsverzeichnis

ABl. EG	Amtsblatt der Europäischen Gemeinschaften
ABl. EU	Amtsblatt der Europäischen Union
Abs.	Absatz
AEUV	Vertrag über die Arbeitsweise der Europäischen Union
a.F.	alte Fassung
AFIS	Automatisches Fingerabdruck-Identifizierungssystem
Art.	Artikel
BDSG	Bundesdatenschutzgesetz
BGBl.	Bundesgesetzblatt
BITKOM	Bundesverband Informationswirtschaft, Telekommunikation und Neue Medien e.V.
BMI	Bundesministerium des Innern
BR-Drs.	Bundesrats-Drucksache
BSI	Bundesamt für Sicherheit in der Informationstechnik
BT-Drs.	Bundestags-Drucksache
BTHausO	Hausordnung des Deutschen Bundestages
BVerfGE	Entscheidungen des Bundesverfassungsgerichtes
CCC	Chaos Computer Club
CDU	Christlich Demokratische Union Deutschlands
CR	Computer und Recht (Zeitschrift)
CSU	Christlich-Soziale Union in Bayern e.V.
ders.	derselbe
DÖV	Die öffentliche Verwaltung (Zeitschrift)
DuD	Datenschutz und Datensicherheit, bis 1995: Datenschutz und Datensicherung (Zeitschrift)
EAC	Extended Access Control
ebd.	ebenda
EG	Europäische Gemeinschaft
EG-Pass-VO	EG-Verordnung 2252/2004 über Normen für Sicherheitsmerkmale und biometrische Daten in von den Mitgliedstaaten ausgestellten Pässen und Reisedokumenten
EGV	Vertrag über die Europäische Gemeinschaft
Einf.	Einführung
Einl.	Einleitung
ELENA	Elektronischen Einkommensnachweis
EU	Europäische Union
f.	folgend(e)
FDP	Freie Demokratische Partei Deutschlands
ff.	fortfolgende
Fn.	Fußnote
GG	Grundgesetz
GwG	Gesetz über das Aufspüren von Gewinnen aus schweren Straftaten („Geldwäschegesetz“)
Hrsg.	Herausgeber
ICAO	International Civil Aviation Organisation
IT	Informationstechnologie
JMStV	Staatsvertrag über den Schutz der Menschenwürde und den Jugendschutz in Rundfunk und Telemedien (Jugendmedienschutz-Staatsvertrag)

JuSchG	Jugendschutzgesetz
KJ	Kritische Justiz (Zeitschrift)
K&R	Kommunikation und Recht (Zeitschrift)
MMR	Multimedia und Recht (Zeitschrift)
m.w.N.	mit weiteren Nachweisen
n.F.	neue Fassung
NJW	Neue Juristische Wochenschrift (Zeitschrift)
Nr.	Nummer
PACE	Password Authenticated Connection Establishment
PassG	Passgesetz
PAuswG	Personalausweisgesetz
PAuswV	Personalausweisverordnung
PersAuswG	Personalausweisgesetz (Abkürzung der a.F. bis 2009)
PIN	Persönliche Identifikationsnummer
provet	Projektgruppe verfassungsverträgliche Technikgestaltung
RFID	Radio Frequency Identification
Rn.	Randnummer(n)
s.	siehe
S.	Seite
s.a.	siehe auch
SigG	Signaturgesetz
SigV	Signaturverordnung
s.o.	siehe oben
SPD	Sozialdemokratische Partei Deutschlands
StGB	Strafgesetzbuch
s.u.	siehe unten
v.	vom
vgl.	vergleiche
Vorb.	Vorbemerkung
z.B.	zum Beispiel