BEITRÄGE

ALEXANDER ROßNAGEL

Modernisierung des Datenschutzrechts für eine Welt allgegenwärtiger Datenverarbeitung

Allgegenwärtige Datenverarbeitung wird die Verwirklichungsbedingungen für das Grundrecht auf informationelle Selbstbestimmung so verändern, dass dessen Schutzprogramm, wie es im geltenden Datenschutzrecht umgesetzt ist, nicht mehr greifen wird. Daher ist es dringend notwendig, dieses Schutzprogramm so fortzuentwickeln, dass es den neuen Risiken gerecht wird. Dies darf jedoch nicht isoliert in eigenen gesetzlichen Vorschriften erfolgen, sondern muss sich einbetten in eine systematische Modernisierung des gesamten Datenschutzrechts. Der Beitrag benennt diese Aufgabe (I.), stellt die neuen Herausforderungen dar (II.) und zeigt, wie eine adäquate Fortentwicklung des Datenschutzrechts möglich wäre (III.).

I. Aktuelle Aufgabe: Modernisierung des Datenschutzrechts

Das deutsche und europäische Datenschutzrecht entstand in Auseinandersetzung mit den Gefährdungen informationeller Selbstbestimmung, die von einer bestimmten Stufe technischer Entwicklung sowie gesellschaftlicher und wirtschaftlicher Techniknutzung ausgingen. Diese waren in den 70er-Jahren geprägt durch die Datenverarbeitung in Rechenzentren. In dieser Welt der Datenverarbeitung wurden die Grundprinzipien des Datenschutzrechts entwickelt, die noch heute das Datenschutzrecht prägen, wie Transparenz durch Unterrichtung und Benachrichtigung, Begrenzung der Datenverarbeitung auf einen bestimmten Zweck und auf die erforderlichen Daten und Verarbeitungsphasen, Korrekturrechte des Betroffenen und Kontrolle durch Datenschutzbeauftragte.[1] Sie wurden nicht wesentlich verändert, als in den 80er-Jahren die Datenverarbeitung auch in verteilte PCs wanderte. Als diese in den 90er-Jahren durch das Internet weltweit vernetzt wurden, erhielt das Datenschutzrecht durch das TDDSG und den MDStV zwei konzeptionelle Ergänzungen.[2] Zum einen wurde das Erforderlichkeitsprinzip durch das Gebot der Datenvermeidung und -sparsamkeit ergänzt. Zum anderen wurde ein erster Schritt zu einem Datenschutz durch Technik unternommen, indem die Konzepte des Selbstdatenschutzes[3] und Systemdatenschutzes[4] eingeführt wurden. Im Wesentlichen ist das gegenwärtig gültige Datenschutzrecht noch immer durch die Prinzipien und Strukturen geprägt, die es in den 70er-Jahren erhalten hat.[5]

Daher ist es nicht verwunderlich, wenn angesichts der revolutionären Veränderungen der Informations- und Kommunikations(IuK)-Technik und ihrer Nutzung eine Modernisierung des Datenschutzrechts gefordert,[6] vorgeschlagen[7] und diskutiert wird.[8] Diese soll zum einen das Datenschutzrecht einfacher und verständlicher machen, zum anderen aber vor allem das Schutzprogramm für das Grundrecht auf informationelle Selbstbestimmung risikoadäquat fortentwickeln. Zu den neuen Herausforderungen, denen das Datenschutzrecht gerecht werden muss, gehört die zunehmende mobile Datenverarbeitung und perspektivisch die allgegenwärtige Datenverarbeitung.

II. Neue Herausforderung: Mobile und allgegenwärtige Datenverarbeitung

Das Neue dieser Herausforderungen ist die Verknüpfung von körperlicher und virtueller Welt. Mobile Datenverarbeitung und Kommunikation beziehen den jeweiligen Aufenthaltsort des Nutzers in die Datenverarbeitung mit ein.[9] Wireless Internet erlaubt an diesem Ort Daten aus der virtuellen Welt anzubieten und umgekehrt Daten aus der körperlichen Welt in die virtuelle Welt aufzunehmen.[10] Ubiquitous oder Pervasive Computing verbindet Sensor-, Kommunikations- und Rechnertechnik in allen möglichen Alltagsgegenständen und verschafft diesen so etwas wie ein „Gedächtnis“ und eine beschränkte „Intelligenz“.[11] Diese „smarten“ Alltagsgegenstände begleiten die Men-

1) S. *Simitis*, BDSG-Komm., 2003, Einl. Rdnr. 1 ff.; *Abel*, Geschichte des Datenschutzes, in: Roßnagel (Hrsg.), Handbuch Datenschutzrecht, 2003, Kap. 2.7, S. 199 ff.

2) S. *Roßnagel*, Datenschutz in Tele- und Mediendiensten, in: ders. (o. Fußn. 1), Kap. 7.9, S. 1280 ff.

3) S. *Roßnagel*, Konzepte des Selbstdatenschutzes, in: *ders.* (o. Fußn. 1), Kap. 3.4, S. 325 ff.

4) S. *Dix*, Konzepte des Selbstdatenschutzes, in: *ders.* (o. Fußn. 1), Kap. 3.5, S. 363 ff.

5) *Simitis* (o. Fußn. 1), Rdnr. 105 ff.; *ders.*, DuD 2000, 714 ff.; *Roßnagel*, Einleitung, in: *ders.* (o. Fußn. 1) Kap. 1, S. 7.

6) S. BT-Drs. 14/9709 v. 3.7.2002; BT-Sten.Ber. 14/25258 ff.; Koalitionsvertrag zwischen *SPD* und *Bündnis 90/Die Grünen* v. 16.10.2002, S. 55.

7) *Roßnagel/Pfitzmann/Garstka*, Modernisierung des Datenschutzrechts, Gutachten i.A. des BMI, 2001.

8) S. z.B. auch *Simitis*, DuD 2000, 714; *Roßnagel/Pfitzmann/Garstka*, DuD 2001, 253; *Roßnagel*, RDV 2002, 61; *Ahrend/Bijok u.a.*, DuD 2003, 433; *Bizer*, DuD 2004, 6; *Kilian*, Rekonzeptualisierung des Datenschutzrechts durch Technisierung und Selbstregulierung? Zum Modernisierungsgutachten 2002 für den Bundesminister des Innern, in: Bizer/Lutterbeck/Rieß (Hrsg.), Umbruch von Regelungssystemen in der Informationsgesellschaft, FS Büllesbach, 2002, S. 151 ff.; *Tauss/Kollbeck/Fazlic*, Modernisierung des Datenschutzes, Wege aus der Sackgasse, in: Bizer/v. Mutius/Petri/Weichert (Hrsg.), Innovativer Datenschutz – Wünsche, Wege, Wirklichkeit, FS Bäumler, 2004, S. 41.

9) S. *Ranke*, M-Commerce und seine rechtsadäquate Gestaltung, 2004, S. 71 ff., 173 ff.

10) S. hierzu z.B. *David*, Mobiles Internet, in: Sommerlatte (Hrsg.), Angewandte Systemforschung, 2002, S. 157 ff.

11) *Coroama u.a.*, Szenarien des Kollegs: Leben in einer smarten Umgebung – Auswirkungen des Ubiquitous Computing, 2003, www.inf.ethz.ch/research/publications/; *Mattern*, Vom Verschwinden des Computers, in: ders. (Hrsg.), Total vernetzt, 2003, S. 3 ff.; *Roßnagel*, Datenschutz im Jahr 2015 – in einer Welt des Ubiquitous Computing, in: FS Bäumler (o. Fußn. 8), S. 335 ff.

■ Prof. Dr. Alexander Roßnagel ist Universitätsprofessor für öffentliches Recht an der Universität Kassel, dort Leiter der Projektgruppe verfassungsverträgliche Technikgestaltung (provet) im Forschungszentrum für Informationstechnikgestaltung (ITeG) und wissenschaftlicher Direktor des Instituts für Europäisches Medienrecht (EMR), Saarbrücken. Der Beitrag entstand i.R.d. von der Daimler-Benz-Stiftung geförderten Kollegs „Living in a Smart Environment“, http://www.smart-environment.de.

schen bei ihren Tätigkeiten und unterstützen sie scheinbar mitdenkend in einer sich selbst organisierenden Weise.[12] Sie können sich gegenseitig identifizieren, sich ihre Zustände mitteilen, Umweltvorgänge erkennen und kontextbezogen reagieren.[13]

1. Neue Risiken: Datenverarbeitung auf Vorrat und Personenprofile

Wird der Einzelne durch die Datenverarbeitung in seiner Umgebung und in den von ihm genutzten Alltagsgegenständen allgegenwärtig begleitet, wird sie unmerklich Teil seines Verhaltens und seines Handelns. Durch mobile und allgegenwärtige Datenverarbeitung wird auch er Gegenstand der datenerhebenden und -verarbeitenden Vorgänge.[14] Diese ermöglichen, sehr feingranulare Profile über seine Handlungen, Bewegungen, sozialen Beziehungen, Verhaltensweisen, Einstellungen und Präferenzen in der körperlichen Welt zu erzeugen.[15] Mit der allgegenwärtigen Datenverarbeitung wird eine potenziell perfekte Überwachungsinfrastruktur aufgebaut.[16] Wer von den vielen potenziellen Interessenten[17] diese nutzen kann, wird von deren Ausgestaltung abhängen. Da diese potenziell die gesamte körperliche Welt erfasst, gibt es für den Einzelnen keine Möglichkeit, der Datenverarbeitung zu entgehen. Damit stellt sich das Problem des Datenschutzes mit einer ganz neuen Dringlichkeit.[18]

2. Neuer Schutzbedarf: Versagen des bisherigen Schutzprogramms

Die Problematik wird dadurch verschärft, dass in einer Welt mobiler und allgegenwärtiger Datenverarbeitung das in den 70er- und 80er-Jahren entwickelte Schutzprogramm für das Grundrecht auf informationelle Selbstbestimmung[19] in keinem seiner Bestandteile mehr richtig greift.[20] Das Gebot der Transparenz stößt an objektive und subjektive Grenzen. Die hohe Komplexität der Systeme, deren vielfältigen Zwecke und die Fülle der Datenverarbeitungsvorgänge in allen Lebensbereichen übersteigen die mögliche Aufmerksamkeit um ein Vielfaches. Soll die allgegenwärtige Rechnertechnik gerade im Hintergrund und damit unmerklich den Menschen bei vielen Alltagshandlungen unterstützen, kann sie nicht zugleich dem Betroffenen bewusst gegenwärtig sein.

Eine Einwilligung für jeden Akt der Erhebung, Verarbeitung und Nutzung zu fordern, würde angesichts der Fülle und Vielfalt der Vorgänge und der Unzahl von verantwortlichen Stellen zu einer Überforderung aller Beteiligten führen. Noch weniger umsetzbar wäre es, hierfür die geltenden Formvorschriften – Schriftform oder elektronische Form – zu fordern. Selbst eine Einwilligung in der für das Internet gedachten Form des § 4 Abs. 2 TDDSG und § 18 Abs. 2 MDStV[21] dürfte unter diesen Umständen meist unpraktikabel sein.

Das Ziel von Ubiquitous Computing, den Nutzer unbemerkt, spontan und in komplexer Weise zu unterstützen, widerspricht diametral dem Ziel der Zweckbindung, die Datenverarbeitung zu begrenzen. Soll sich für eine „Ad-hoc-Kommunikation" die Infrastruktur jeweils situationsabhängig und ständig wechselnd mit Hilfe der Endgeräte der Kommunikationspartner und unbeteiligter Dritter bilden, kann nicht vorherbestimmt werden, welche Beteiligten zu welchen Zwecken welche Daten erhalten und verarbeiten. Wenn viele Anwendungen ineinander greifen, Daten aus anderen Anwendungen übernehmen, für den Nutzer Erinnerungsfunktionen für künftige Zwecke erfüllen sollen, die noch nicht bestimmt werden können, sind Datenspeicherungen auf Vorrat nicht zu vermeiden. Wenn die Umgebungssysteme kontextsensitiv und selbstlernend sein sollen, werden sie aus den vielfältigen Datenspuren, die der Nutzer bei seinen Alltagshandlungen hinterlässt, und seinen Präferenzen, die seinen Handlungen implizit entnommen werden können, vielfältige Profile erzeugen müssen.

Da das Prinzip der Erforderlichkeit am Zweck der Datenverarbeitung ausgerichtet ist, erleidet es in einer Welt allgegenwärtiger Datenverarbeitung die gleiche Schwächung wie das Prinzip der Zweckbindung. Soll die Datenverarbeitung im Hintergrund ablaufen, auf Daten zugreifen, die durch andere Anwendungen bereits generiert wurden, und gerade dadurch einen besonderen Mehrwert erzeugen, wird es schwierig sein, für jede einzelne Anwendung eine Begrenzung der zu erhebenden Daten oder deren frühzeitige Löschung durchzusetzen. Die Idee, die Gegenstände mit einem „Gedächtnis" auszustatten, um dadurch das löchrige Gedächtnis des Nutzers zu erweitern, lässt das Prinzip der Datensparsamkeit leer laufen. Sensoren, die den Nutzer direkt wahrnehmen, können diesen vielfach auch bei anonymer oder pseudonymer Nutzung identifizieren.[22]

Mitwirkungs- und Korrekturrechte des Betroffenen werden wegen der Vervielfachung und Komplexität der Datenverarbeitung im Alltag, die oft unmerklich stattfinden wird, an Durchsetzungsfähigkeit verlieren. Außerdem werden die Vielzahl der beteiligten Akteure, die spontane Ver- und Entnetzung sowie der ständige Rollenwechsel zwischen Datenverarbeiter und betroffener Person zu einer Zersplitterung der Verantwortlichkeit für die datenverarbeitenden Vorgänge führen. Schließlich werden die verantwortlichen Stellen selbst oft nicht wissen, welche personenbezogenen Daten sie verarbeiten. Vorgänge aber zu protokollieren, um Auskunfts- und Korrekturrechte erfüllen zu können, wäre in vielen Fällen im Hinblick auf Datensparsamkeit kontraproduktiv.

Mobile und allgegenwärtige Datenverarbeitung gefährdet somit die informationelle Selbstbestimmung, weil sie de-

---

12) S. *Mattern*, Allgegenwärtiges Rechnen – Eine Einführung, in: Taeger/Wiebe (Hrsg.), Mobilität-Telematik-Recht, 2005, i.E.

13) S. z.B. *Langheinrich/Mattern*, Digitalisierung des Alltags. Was ist Pervasive Computing?, Aus Politik und Zeitgeschichte 2003, B 42, 6 ff.; *Mattern* (o. Fußn. 12).

14) S. zu RFID und Datenschutz z.B. *Müller*, DuD 2004, 215; *Kelter/Wittmann*, DuD 2004, 331; *v. Westerholt/Döring*, CR 2004, 710; *Müller/Handy*, DuD 2004, 655; *Langheinrich*, Die Privatsphäre im Ubiquitous Computing – Datenschutzaspekte der RFID-Technologie, www.vs.inf.eth.ch/publ/papers/langhein2004rfid.pdf.

15) S. hierzu auch *Mattern*, Allgegenwärtige Informationstechnik – Soziale Folgen und Konsequenzen für die Menschenrechte, in: Kirchschläger u.a. (Hrsg.), Menschenrechte und Terrorismus, 2004, S. 313 ff., www.vs.inf.eth.ch/publ/papers/mattern2004_menschenrechte.pdf, S. 13 f.; *Langheinrich* (o. Fußn. 14), S. 9.

16) S. hierzu auch *Langheinrich* (o. Fußn. 14), S. 8 f.; *Mattern* (o. Fußn. 15), S. 14.

17) Vor diesem Hintergrund erhalten die gegenwärtigen Diskussionen um die Pflicht von TK- und Internetanbietern zur Vorratsdatenspeicherung eine ganz neue Dimension – s. hierzu z.B. der Entwurf des *Bundesrats*, BT-Drs. 15/2316, 120 f.; *Thiede*, Kriminalistik 2004, 106; *Ohlenburg*, MMR 2003, 85; *Breyer*, DuD 2003, 491; *Dix*, DuD 2003, 234; *Roßnagel*, Sicherheit für Freiheit? Grundlagen und Fragen, in: *ders.* (Hrsg.), Sicherheit für Freiheit – Riskante Sicherheit oder riskante Freiheit in der Informationsgesellschaft, 2003, S. 34 ff.

18) S. *Roßnagel*, Das rechtliche Konzept der Selbstbestimmung in einer Welt mobiler Datenverarbeitung, in: Taeger/Wiebe (o. Fußn. 12).

19) S. insb. BVerfGE 65, 1, 42 ff.

20) S. zum Folgenden ausf. *Roßnagel/Müller*, CR 2004, 625; aus informationstechnischer Sicht *Langheinrich* (o. Fußn. 14), S. 9 ff.

21) S. zu dieser *Roßnagel/Banzhaf/Grimm*, Datenschutz im Electronic Commerce, 2003, S. 162 f.

22) S. *Langheinrich* (o. Fußn. 14), S. 11 f.

ren gegenwärtiges Schutzprogramm leer laufen lässt. Es wäre jedoch eine Illusion zu glauben, diese Entwicklung könnte deshalb aufgehalten oder gar verboten werden. Ein solcher Versuch würde den Datenschutz jeder Akzeptanz berauben. Vielmehr wird davon auszugehen sein, dass die Nutzung allgegenwärtiger Informationstechnik überwiegend von den Betroffenen gewollt ist. Zwar wird es auch Situationen geben, in denen die Datenverarbeitung dem Betroffenen aufgezwungen wird, wenn etwa alle Handelsketten RFID-„getagte" Waren einführen und ihren Kunden keine Wahlmöglichkeit lassen. Die meisten Anwendungen werden aber von den Betroffenen selbst gewählt und gern genutzt, weil sie ihnen Erweiterungen ihrer geistigen und körperlichen Fähigkeiten bieten, sie bei Routineaufgaben unterstützen, ihnen Entscheidungen abnehmen und ihr Leben bequemer machen. Die Nutzer werden individualisierte Dienste und Geräte fordern, die sich ihnen anpassen. Wie bisher auch werden sie informationelle Selbstbestimmung zwar abstrakt hoch achten, im konkreten Fall aber – mehr oder weniger notgedrungen – damit einverstanden sein, dass die Hintergrundsysteme die notwendige Kenntnis über ihre Lebensweise, Gewohnheiten, Einstellungen und Präferenzen erhalten.[23]

III. Neue Schutzstrategien: Sechs Thesen zur Modernisierung des Datenschutzrechts

Durch die mobile und allgegenwärtige Datenverarbeitung wird nicht die Notwendigkeit informationeller Selbstbestimmung in Frage gestellt. Im Gegenteil – wenn die Welt human und lebenswert sein soll, muss Selbstbestimmung mehr noch als heute gewährleistet sein. Allerdings muss das Schutzprogramm für dieses Grundrecht den neuen Risiken angepasst sein.

Dies kann nicht dadurch erreicht werden, dass jetzt für die neuen Risiken ein weiteres, eigenes Datenschutzgesetz geschaffen wird. Dies würde das schwer verständliche Datenschutzrecht nur noch unübersichtlicher machen. Auch wäre es nicht zielführend, die Grundsätze des bisherigen Schutzprogramms vollständig aufzugeben. Denn sie sind ja aus der Zielsetzung der informationellen Selbstbestimmung abgeleitet. Notwendig ist vielmehr eine umfassende Modernisierung des Datenschutzrechts, die dem Datenschutz insgesamt eine neue Struktur gibt, dabei aber angemessen auf die neuen Gefährdungen ausgerichtet ist. Im Gutachten zur Modernisierung des Datenschutzrechts aus dem Jahr 2001 wurden die Bedingungen der allgegenwärtigen Datenverarbeitung bereits berücksichtigt.[24] Inzwischen ist aber klarer absehbar, welchen Risiken die informationelle Selbstbestimmung ausgesetzt sein dürfte. Daher ist es für die weitere Diskussion hilfreich, die damals vorgetragenen Empfehlungen zur Modernisierung zu spezifizieren und zu erweitern.

Wie ein Schutzprogramm für die informationelle Selbstbestimmung bei allgegenwärtiger Datenverarbeitung in der Modifikation und Ergänzung bisheriger Datenschutzgrundsätze aussehen könnte, soll im Folgenden in Form von sechs Thesen zur notwendigen Neuorientierung angedeutet werden.[25]

1. Stärkere Gestaltungs- und Verarbeitungsregeln statt Zulassungskontrollen

Bisher erfolgt Datenschutz normativ vor allem dadurch, dass lange vor der Datenverarbeitung diese nach einer einmaligen abstrakten Überprüfung durch Einwilligung oder gesetzliche Erlaubnis zugelassen wird. Statt das Schwergewicht auf eine einmalige Zulassungsentscheidung durch Zwecksetzung des Gesetzgebers oder der betroffenen Person zu legen, sollte Datenschutz künftig vorrangig durch Gestaltungs- und Verarbeitungsregeln bewirkt werden, die permanent zu beachten sind.[26]

So könnte z.B. Transparenz statt auf einzelne Daten stärker auf Strukturinformationen bezogen sein und statt durch eine einmalige Unterrichtung oder Benachrichtigung durch eine permanent einsehbare Datenschutzerklärung im Internet gewährleistet werden.[27] Eine andere Transparenzforderung könnte sein – entsprechend dem Gedanken der §§ 6b Abs. 2 und 6c Abs. 3 BDSG –, von allen datenverarbeitenden Alltagsgegenständen eine technisch auswertbare Signalisierung zu fordern, wenn sie Daten erheben.[28]

Die Einwilligung könnte eine Aufwertung erfahren, wenn sie auf ein technisches Gerät der betroffenen Person „delegiert" werden könnte,[29] das bei jedem signalisierten Verarbeitungsvorgang im Hintergrund die Datenschutz-Policies prüft, akzeptiert oder verwirft.[30] Dies setzt allerdings voraus, dass die Datenschutzpräferenzen zumindest für Normalfälle spezifizierbar sind. Hierfür könnten Datenschutzbeauftragte, Datenschutzvereinigungen, sonstige Verbände und Organisationen Empfehlungen in Form direkt einsetzbarer Präferenzmuster geben. Als ein Opt-in könnte auch anzusehen sein, wenn eine betroffene Person bewusst und freiwillig ihre individuellen Fähigkeiten unterstützende und verstärkende Techniksysteme und Dienste nutzt. Im Gegenzug müssten diese so gestaltet sein, dass sie über Datenschutzfunktionen verfügen, die die betroffene Person auswählen und für sich konfigurieren kann.

Je stärker das Zusammenspiel zwischen enger Zwecksetzung und strenger Erforderlichkeit bei individualisierten adaptiven Systemen an Grenzen stößt, desto stärker muss das Datenschutzrecht die datensparsame Systemgestaltung in den Blick nehmen und Möglichkeiten sinnvollen anonymen und pseudonymen Handelns einfordern. Außerdem muss in diesen Fällen Zweckbindung stärker auf Missbrauchsvermeidung und Erforderlichkeit stärker auf Löschungsregeln hin konzentriert werden. Die Umsetzung dieser Ziele sollte vor allem durch ein Datenschutzmanagementsystem erreicht werden: Ein Bestandteil dieses Systems sollte die Pflicht der verantwortlichen Stelle sein, in ihrem Datenschutzkonzept nachzuweisen, dass sie die Gestaltungsziele erreicht hat.[31]

Vereinfacht und zugleich effektiviert würde der Datenschutz für viele Anwendungen der allgegenwärtigen Datenverarbeitung, wenn als zulässiger Zweck relativ weit das Erbringen einer rein technischen Funktion anerkannt, dafür aber als Ersatz die Verwendung der Daten strikt auf diese Funktion begrenzt würde. Dies könnte erreicht werden, wenn zwischen einer Datenverarbeitung mit und oh-

23) S. zu Einstellungen zum Datenschutz z.B. *Opaschowski*, in: Roßnagel (o. Fußn. 1), Kap. 2.1, S. 43 ff.
24) S. *Roßnagel/Pfitzmann/Garstka* (o. Fußn. 7), S. 15, 22 f., 28, 42, 60, 63, 113 und 115.
25) S.a. zum Folgenden *Roßnagel* (o. Fußn. 18).
26) S. *Roßnagel/Pfitzmann/Garstka* (o. Fußn. 7), S. 70 ff.
27) S. *Roßnagel/Pfitzmann/Garstka* (o. Fußn. 7), S. 86 f.
28) S. a. hierzu *Langheinrich* (o. Fußn. 14), S. 10.
29) Zur Delegation von Willenserklärungen auf Softwareagenten s. z.B. *Gitter/Roßnagel*, K&R 2003, 64.
30) S. hierzu auch *Langheinrich* (o. Fußn. 14), S. 11.
31) S. *Roßnagel/Pfitzmann/Garstka* (o. Fußn. 7), S. 102.

ne gezielten Personenbezug unterschieden würde.[32] Eine Datenverarbeitung ohne gezielten Personenbezug betrifft die Verarbeitung personenbezogener Daten, die zur Erfüllung – vor allem technischer – Dienstleistungen technisch notwendig ist, ohne dass es dem Verarbeiter auf den Personenbezug ankommt. Die Anforderungen für diese Art der Datenverarbeitung sollten risikoadäquat und effizienzsteigernd spezifiziert werden. Sie sollten insofern verschärft werden, als die Daten auf das erforderliche Minimum begrenzt, während ihrer Verarbeitung gegen Zweckentfremdung geschützt und nach der Verarbeitung sofort gelöscht werden müssen. Die Daten sollten außerdem einer strengen Zweckbindung (wie nach § 31 BDSG) unterliegen und durch ein Verwertungsverbot geschützt sein. Werden diese Anforderungen nicht erfüllt, wird vor allem ein weitergehender Zweck mit diesen Daten verfolgt, gelten für sie von Anfang an alle Anforderungen für die Datenverarbeitung mit gezieltem Personenbezug. Erleichterungen sollten insoweit vorgesehen werden, als auf eine vorherige Unterrichtung der betroffenen Personen verzichtet wird und ein Anspruch auf Auskunft über einzelne Daten für die kurze Zeit ihrer Speicherung nicht besteht, um kontraproduktive Protokollverfahren zu vermeiden. Die notwendige Transparenz sollte vielmehr durch eine veröffentlichte Datenschutzerklärung über die Struktur des Datenverarbeitungsverfahrens hergestellt werden.

2. Mehr Datenschutz durch Technik statt durch Verhaltensregeln

Die Beispiele haben schon gezeigt, dass diese Gestaltungs- und Verarbeitungsregeln auf eine technische Umsetzung angewiesen sind. In einer durch und durch technisierten Welt hat Selbstbestimmung nur dann eine Chance, wenn sie ebenfalls technisch unterstützt wird.[33] Wenn allgegenwärtige Datenverarbeitung überall, zu jeder Zeit, im Hintergrund und auf breite und vielfältige Infrastrukturen gestützt, automatisch, unbemerkt und beiläufig stattfindet, dann muss dies für den künftigen Datenschutz auch gelten. Selbstbestimmung muss überall und jederzeit möglich sein. Sie muss durch Infrastrukturen unterstützt werden, die ermöglichen, auf Gefährdungen automatisch zu reagieren, ohne dass dies aufdringlich oder belästigend wirkt. Zwei Beispiele sollen dies verdeutlichen:

Die Einhaltung von Verarbeitungsregeln zu kontrollieren, darf nicht eine permanente persönliche Aufmerksamkeit erfordern, sondern muss automatisiert erfolgen. Wenn die datenverarbeitenden Alltagsgegenstände ein Signal aussenden, kann dies von einem Endgerät des Betroffenen erkannt werden und zu einer automatisierten Auswertung der zugehörigen Datenschutzerklärung führen. Entsprechend der voreingestellten Datenschutzpräferenzen kann ein P3P[34]-ähnlicher Client eine Einwilligung erteilen oder ablehnen.[35] In Zweifelsfällen kann das Gerät je nach Voreinstellung den Betroffenen warnen und ihm die Erklärung in der von ihm gewählten Sprache anzeigen oder akustisch ausgeben. Die Hinweis- und Warndichte muss einstellbar sein.[36]

Die Durchsetzung von Verarbeitungsregeln muss im Regelfall durch Technik und nicht durch persönliches Handeln des Betroffenen erreicht werden. Zum einen muss der Systemdatenschutz dazu führen, dass – soweit möglich – die technischen Systeme nur das können, was sie dürfen.[37] Zum anderen müssen Endgeräte des Betroffenen in der Lage sein, die Datenerfassung durch fremde Geräte zu beeinflussen,[38] nach den Präferenzen des Nutzers Kommunikation zu ermöglichen oder abzublocken,[39] Pseudonyme und andere Identitäten zu wechseln und zu verwalten,[40] Datenweitergaben zu protokollieren und Löschungsrechte automatisch geltend zu machen.

Technischer Datenschutz hat gegenüber rein rechtlichem Datenschutz gewisse Effektivitätsvorteile. Was technisch verhindert wird, muss nicht mehr verboten werden. Gegen Verhaltensregeln kann verstoßen werden, gegen technische Begrenzungen nicht. Datenschutztechnik kann so Kontrollen und Strafen überflüssig machen.[41]

3. Ergänzende Vorsorgeregelungen statt Beschränkung auf Gefahrenabwehr

Wie in anderen Rechtsbereichen auch muss Vorsorge die Gefahrenabwehr ergänzen. Diese Vorsorge könnte eine zweifache Ausprägung annehmen: zum einen die Reduzierung von Risiken und zum anderen präventive Folgenbegrenzungen potenzieller Schäden. Die Risiken für die informationelle Selbstbestimmung sind in einer Welt allgegenwärtiger Datenverarbeitung nicht mehr ausreichend zu bewältigen, wenn nur auf die Verarbeitung personenbezogener Daten abgestellt wird. Vielmehr sind im Sinn vorgreifender Folgenbegrenzung auch Situationen zu regeln, in denen noch keine personenbezogenen Daten entstanden sind oder verarbeitet werden. So bedürfen z.B. die Sammlungen von Sensorinformationen, Umgebungsdaten oder von pseudonymen Präferenzen einer vorsorgenden Regelung, wenn die Möglichkeit oder gar die Absicht besteht, sie irgendwann einmal mit einem Personenbezug zu versehen.[42]

Auch sind zur Risikobegrenzung Anforderungen an eine transparente, datensparsame, kontrollierbare und missbrauchsvermeidende Technikgestaltung zu formulieren. Ebenso entspricht es dem Vorsorgegedanken, die einzusetzenden Techniksysteme präventiven (freiwilligen) Prüfungen ihrer Datenschutzkonformität zu unterziehen und diese Prüfung zu dokumentieren.[43]

4. Neue Regelungsadressaten statt allein Regelungen für verantwortliche Stellen

Hinsichtlich der Regelungsadressaten ist die zunehmende Verantwortungsdiffusion zur Kenntnis zu nehmen. An der Datenverarbeitung sind oft viele Akteure mit spontanen, kurzfristigen Aktionen beteiligt, die in ihrem – vielleicht nicht intendierten – Zusammenwirken erst die zu gestaltenden Wirkungen verursachen. Zwischen Datenverarbeitern und Betroffenen findet ein permanenter Rollenwechsel statt. Daher dürfte eine Regelung, die sich nur an „verantwortliche Stellen" richtet, viele Gestaltungsziele nicht erreichen.

In viel stärkerem Maß sind daher künftig die Technikgestal-

---

32) S. näher *Roßnagel/Pfitzmann/Garstka* (o. Fußn. 7), S. 68 ff., 113 ff.
33) S. *Köhntopp* und *Nedden*, Datenschutz und „Privacy Enhancing Technologies", in: Roßnagel (Hrsg.), Allianz von Medienrecht und Informationstechnik?, 2001, S. 55 ff. und 67 ff.
34) Platform for Privacy Preferences – s. näher www.w3c.org/P3P.
35) S. z.B. *Langheinrich*, Privacy by Design – Principles of Privacy-Aware Ubiquitous Systems, in: Abowd et al. (Eds.), Proceedings of Ubicomp 2001, S. 273 ff.
36) S.a. hierzu , allerdings auch mit skeptischen Hinweisen *Langheinrich* (o. Fußn. 14), S. 10.
37) S. *Dix* (o. Fußn. 4), S. 368 ff.
38) S. *Roßnagel/Müller*, CR 2004, 629.
39) S. *Müller/Handy*, DuD 2004, 655.
40) S. z.B. *Hansen/Krasemann/Rost/Genghini*, DuD 2003, 551.
41) *Roßnagel*, Allianz von Medienrecht und Informationstechnik: Hoffnungen und Herausforderungen, in: *ders.* (o. Fußn. 33), S. 17 ff.
42) S. hierzu näher *Roßnagel/Scholz*, MMR 2000, 728.
43) S. hierzu näher *Roßnagel/Pfitzmann/Garstka* (o. Fußn. 7), S. 130 ff.

ter als Regelungsadressaten anzusprechen. Viele Gestaltungsanforderungen können von den „verantwortlichen Stellen" gar nicht erfüllt werden. Ihnen fehlen meist das technische Wissen, die Gestaltungskompetenz und vor allem der (legale) Zugriff auf Hard- und Software. Statt Regelungsadressaten ohne Einfluss zu wählen, sollten diejenigen verpflichtet werden, die auch die entsprechenden Handlungsmöglichkeiten haben.

Die Technikentwickler und -gestalter sollten vor allem Prüfpflichten für eine datenschutzkonforme Gestaltung ihrer Produkte, eine Pflicht zu Dokumentation dieser Prüfungen für bestimmte Systeme und Hinweispflichten für verbleibende Risiken treffen.[44] Auch sollten sie verpflichtet werden, ihre Produkte mit datenschutzkonformen Defaulteinstellungen auszuliefern.[45]

5. Stärkere Anreize und Belohnungen statt Ge- und Verbote

Die datenschutzgerechte Gestaltung der künftigen Welt mobiler und allgegenwärtiger Datenverarbeitung ist durch herkömmliche Command-and-Control-Ansätze nicht zu erreichen. Sie fordert die aktive Mitwirkung der Entwickler, Gestalter und Anwender. Sie werden nur für eine Unterstützung zu gewinnen sein, wenn sie davon einen Vorteil haben. Daher sollte die Verfolgung legitimen Eigennutzes in einer Form ermöglicht werden, die zugleich auch Gemeinwohlbelangen dient. Datenschutz muss daher zu einem Werbeargument und Wettbewerbsvorteil werden.

Dies ist möglich durch die freiwillige Auditierung von Anwendungen,[46] die Zertifizierung von Produkten[47] und Präsentation von Datenschutzerklärungen. Werden diese von Datenschutzempfehlungen à la „Stiftung Warentest", von Datenschutzrankings oder durch die Berücksichtigung von Auditzeichen oder Zertifikaten bei der öffentlichen Auftragsvergabe begleitet, kann ein Wettbewerb um den besseren Datenschutz entstehen. Dann werden die Gestaltungsziele beinahe von selbst erreicht.[48]

Hier könnten auch Datenschutzbeauftragte und -verbände eine neue Rolle finden, indem sie den Schwerpunkt ihrer Praxis von einer repressiven Kontrolle zu einer konstruktiven Unterstützung von Datenschutz verlegen. Sie erhielten ein ganz neues Image, wenn sie Empfehlungen aussprechen, Beratungen durchführen, Best Practice-Beispiele publizieren und Preise für gute Datenschutzlösungen vergeben.[49]

6. Stärkere institutionalisierte statt individualisierte Grundrechtskontrolle

Der Schutz der informationellen Selbstbestimmung bedarf einer objektiven Ordnung, die in der Praxis mehr und mehr an die Stelle individueller Rechtewahrnehmung tritt. Die Einhaltung von Datenschutzvorgaben kann künftig immer weniger von der individuellen Kontrolle des Betroffenen abhängig gemacht werden. Sie muss in noch viel stärkerem Maß stellvertretend Kontrollverfahren und Kontrollstellen übertragen werden, die das Vertrauen der Betroffenen genießen. Dies sind zum einen die Datenschutzbeauftragten, denen weitergehende Eingriffsbefugnisse für grobe Missbrauchsfälle zuerkannt werden müssen.[50] Auch wird Verantwortung für die adäquate Technikgestaltung stärker zu institutionalisieren sein – etwa in Form von Verantwortlichen der Geschäftsleitung und der betrieblichen Datenschutzbeauftragten. Schließlich werden anerkannte Datenschutzverbände eine Art Ombudsfunktion wahrnehmen und mit entsprechenden Klagebefugnissen ausgestattet sein müssen.[51]

Gegenstand der Kontrolle müssen Systeme mit ihren Funktionen und Strukturen sein, nicht so sehr die individuellen Daten. Ziel der Kontrolle muss es sein, die individuellen und gesellschaftlichen Wirkungen der technischen Systeme zu überprüfen und diese datenschutzgerecht zu gestalten.

IV. Chancen der Selbstbestimmung in der mobilen Gesellschaft

Informationelle Selbstbestimmung wird als normatives Konzept immer wichtiger, je größer die Risiken für die freie Entfaltung von Individuen und die demokratische Entwicklung der Gesellschaft durch eine Datenverarbeitung werden, die immer stärker in den alltäglichen Lebensvollzug eindringt und Angaben aus allen Lebensbereichen und Situationen aufnimmt und nutzt. Allerdings müssen die Konzepte und Instrumente des Datenschutzes der Allgegenwärtigkeit der Datenverarbeitung angepasst werden. Notwendig ist daher ein modifiziertes und ergänztes Schutzprogramm. Notwendig ist eine objektivierte Ordnung der Datenverarbeitung und -kommunikation bei professioneller Kontrolle, mit vorsorgender Gestaltung von Strukturen und Systemen, der Inpflichtnahme von Herstellern zur Umsetzung von Datenschutz in Technik sowie der Nutzung von Eigennutz durch Anreize zu datenschutzgerechtem Handeln.

Ob mit solchen Veränderungen die informationelle Selbstbestimmung in einer Welt allgegenwärtiger Datenverarbeitung gewährleistet werden kann, muss bis zum Beweis durch die Praxis als offen gelten. Sie sind eine notwendige, aber keine hinreichende Bedingung für einen Schutz der informationellen Selbstbestimmung. Hinzukommen muss bei den einzelnen Bürgern ebenso wie in der politischen Meinungsbildung der Wunsch, informationelle Selbstbestimmung als ein hohes, aber gefährdetes Gut bewahren zu wollen, und die politische Kraft, die hierfür erforderlichen Strukturänderungen zu einer adäquaten Modernisierung des Datenschutzes auch durchzusetzen.

---

44) S. näher *Roßnagel/Pfitzmann/Garstka* (o. Fußn. 7), S. 143 ff.
45) S. *Roßnagel* (o. Fußn. 41), S. 24.
46) S. z.B. *Roßnagel*, Datenschutzaudit, in: ders. (o. Fußn. 1), S. 439 ff.
47) S. z.B. *Schläger*, DuD 2004, 459; *Bäumler*, DuD 2004, 80; *ders.*, DuD 2002, 325.
48) S. hierzu ausf. *Roßnagel*, Datenschutzaudit – Konzeption, Durchführung, gesetzliche Regelung, 2000, S. 3 ff.; *ders.*, Marktwirtschaftlicher Datenschutz – eine Regulierungsperspektive, in: FS Büllesbach (o. Fußn. 8) , S. 131 ff.; *Bäumler/v. Mutius*, Datenschutz als Wettbewerbsvorteil, 2002.
49) S. z.B. *Weichert*, Datenschutzberatung – Hilfe zur Selbsthilfe, in: Bäumler (Hrsg.), Der neue Datenschutz, 1998, S. 213 ff.
50) S. näher *Roßnagel/Pfitzmann/Garstka* (o. Fußn. 7), S. 194 ff.
51) S. näher *Roßnagel/Pfitzmann/Garstka* (o. Fußn. 7), S. 130 ff., 143 ff. und 205 ff.