Ute Vogt
Mitglied des Deutschen Bundestages

Jörg Tauss
Mitglied des Deutschen Bundestages

Entwurf für ein Eckwerte-Papier der SPD-Bundestagsfraktion: Modernes Datenschutzrecht für die (globale) Wissens- und Informationsgesellschaft[*]*

Immer mehr Lebensbereiche in der sich entfaltenden Wissens- und Informationsgesellschaft werden von den neuen Informations- und Kommunikationstechniken durchdrungen. Mit der zunehmenden Bedeutung der neuen Informations- und Kommunikationstechniken und der zunehmenden Abhängigkeit vieler gesellschaftlicher Bereiche von diesen Techniken wächst auch das Bewußtsein um die damit einhergehenden Gefahren.[1][1] In einer Gesellschaftsformation, die den Umgang und die Verarbeitung von Daten und Informationen als Markierung des gesellschaftlichen Wandels bereits im Namen trägt, wird die Sicherheit und der Schutz von Informationen und Daten von entscheidender Bedeutung sein. Notwendig ist eine dieser Gesellschaftsformation angemessene „neue Politik zum Schutz der Privatsphäre", denn „ohne einen besseren Schutz der Privatsphäre wird es keine demokratisch verantwortbare Informationsgesellschaft geben."[2][2]

Die Herausforderungen, mit denen das Datenschutzrecht konfrontiert wird, sind vielfältig. Zum einen muß das Datenschutzrecht auf ein gänzlich entgegengesetztes Technikszenario reagieren, als es ursprünglich in den 70er und 80er Jahren konzipiert wurde. Zum anderen soll mit der EU-Datenschutzrichtlinie ein weiterer – und nicht zu unterschätzender – Schritt in Richtung Harmonisierung des Rechts gegangen werden, der für die demokratische Verankerung der Europäischen Gemeinschaft von fundamentaler Bedeutung ist: Für die europäische Integration ist die EU-Datenschutzrichtlinie ein wesentliches Element ihrer grundrechtlichen

* Dieses Papier entstand in Zusammenarbeit mit Johannes Kollbeck, Jan Mönikes und Dr. Matthias Schrumpf und basiert auf den Ergebnissen der Beratungen des „Expertenkreises Datenschutz", an dem teilgenommen haben: Dr. Helmut Bäumler, Dr. Johann Bizer, Dr. Ulf Brühann, Prof. Dr. Alfred Büllesbach, Dr. Ulrich Damann, Dr. Alexander Dix, Prof. Dr. Hansjürgen Garstka, Prof. Dr. Alexander Roßnagel, Prof. Dr. Spiros Simitis, Bettina Sokol, Ministerialrat Klaus Stoltenberg und Dr. Stefan Walz. Wir danken den Teilnehmern des Expertenkreises Datenschutz für die gute Zusammenarbeit und die vielen wertvollen Anregungen.

[1] Vgl. hierzu den Schlußbericht „Deutschlands Weg in die Informationsgesellschaft" (BT-Drs. 13/11004) und den Vierten Zwischenbericht „Sicherheit und Schutz im Netz" (BT-Drs. 13/11002) der Enquete-Kommission „Zukunft der Medien in Wirtschaft und Gesellschaft – Deutschlands Weg in die Informationsgesellschaft".

[2] Bäumler, Helmut (1998): Wir brauchen eine neue Politik zum Schutz der Privatsphäre. In: DuD 6/1998: 312-313.

Fundierung. Damit ist jedoch nur ein erster Schritt getan, denn die weltweite Vernetzung macht weltweite Regelungen notwendig, die es zu entwickeln und zu formulieren gilt.[3][3] All dies macht deutlich, daß das traditionelle Datenschutzrecht nicht ausreichen kann, um das Recht auf informationelle Selbstbestimmung in Zukunft zu wahren – notwendig ist ein „neuer Datenschutz“ für die Informations- und Wissensgesellschaft von morgen.[4] [4]

Herausforderungen an das Datenschutzrecht durch neue Techniken

Die Risiken und Gefährdungen in der entstehenden Informations- und Wissensgesellschaft im Hinblick auf das Grundrecht auf informationelle Selbstbestimmung sind vielfältig. Immer wieder gehen Meldungen durch die Presse, die die Privatsphäre durch die neuen Techniken gefährdet erscheinen lassen: Nachrichten über unberechtigte Zugriffe auf scheinbar sichere Datenbestände und deren Manipulation[5][5], über Programme, die in Telekommunikationsnetzen sensible Daten wie Kreditkartennummern ‚abfangen‘, oder über Software, die über Datennetze unbemerkt auf der Festplatte des Nutzers installiert wird, um von dort aus Informationen in das weltweite Datennetz zu kopieren.[6][6] Fast drängt sich dabei der Eindruck auf, das Orwellsche Schreckensszenario vom „gläsernen Menschen“ rücke mit dem Übergang von der Industrie- zur Informations- und Wissensgesellschaft in bedrohliche Nähe.[7][7]

[3] Vgl. Siegele, Ludwig/Wernicke, Christian (1998): Alarm im Netz. Europa und die USA streiten über wirksamen Datenschutz. Eine Blockade der Informationsströme droht. In: Die ZEIT Nr. 44 vom 22. Oktober 1998: 28/29.

[4] Bausteine für einen solchen „neuen Datenschutzes“ finden sich in dem von Helmut Bäumler herausgegebenen Sammelband: Bäumler, Helmut (Hrsg.) (1998): Der neue Datenschutz. Datenschutz in der Informationsgesellschaft von morgen. Neuwied, Kriftel, Berlin.

[5] Vgl. beispielsweise Die Zeit vom 23.8.1997: Räuber im Netz. Das weltweite Internet öffnet dem Datenmißbrauch Tür und Tor – die nationalen Kontrolleure sind machtlos.

[6] Vgl. zu möglichen Risiken und zu bisher bekannt gewordenen Fällen ausführlich die Berichtsteile „IT-Sicherheit“ und „Datenschutz“ des vierten Zwischenberichtes „Sicherheit und Schutz im Netz“ (BT-Drs. 13/11002) der Enquete-Kommission „Zukunft der Medien in Wirtschaft und Gesellschaft – Deutschlands Weg in die Informationsgesellschaft“ des 13. Deutschen Bundestages.

[7] Vgl. dazu Der Spiegel 36/1996: Lauscher im Datenreich. Die Welt der Computer ist ein Paradies für Spione aller Art. PC verraten vertrauliche Daten durch hochfrequente Abstrahlung. Geheimdienste überwachen den internationalen Datenverkehr und unterhöhlen zielstrebig alle Schutzvorkehrungen. Selbst das gutgesicherte Netz der Banken haben Profi-Lauscher angezapft; vgl. auch Computer-Zeitung vom 3.7.1997: Das Data-Warehouse-Konzept schürt die Angst vor dem gläsernen Bürger.

Dadurch ausgelöste, objektiv nicht unbegründete, Befürchtungen könnten den weiteren Ausbau der Informationsgesellschaft und die Nutzung der durch die neuen Informations- und Kommunikationstechniken entstehenden Vorteile und Chancen ernsthaft behindern. Eine aufgrund der Besorgnis um den Schutz der Privatsphäre ablehnende Haltung gegenüber den neuen Informations- und Kommunikationstechniken hätte mit großer Wahrscheinlichkeit auch erhebliche wirtschaftliche Konsequenzen: Bei fehlendem Vertrauen in die neuen Informations- und Kommunikationstechniken blieben die immensen ökonomischen Potentiale Makulatur – seien es Erwartungen in Milliardenhöhe beim electronic commerce, seien es Erwartungen für den Arbeitsmarkt durch Telearbeit oder seien es die erwarteten Umsätze der Informationswirtschaft.[8][8]

Insofern wird ein wirksamer Datenschutz auch ein wesentlicher Wettbewerbsfaktor der globalen Informationsgesellschaft sein.[9][9] Das ist inzwischen auf nationaler und internationaler Ebene erkannt: Sowohl die G7 [10][10], die OECD[11][11] und die Europäische Kommission[12][12] als auch die Regierung der Vereinigten Staaten[13][13] halten den Schutz der Privat-sphäre in den weltumspannenden Datennetzen für eine der wichtigsten Voraussetzungen für die Akzeptanz und die Nutzung der neuen Informations- und Kommunikationstechniken. Inzwischen hat auch die Welthandelsorganisation (WTO), die den Datenschutz vorrangig unter dem Stichwort

[8] Vgl. zu den Erwartungen in diesen Bereichen die Berichtsteile Arbeit 21 und Wirtschaft 21 des Abschlußberichtes „Deutschlands Weg in die Informationsgesellschaft“ (BT-Drs. 13/11004) der Enquete-Kommission „Zukunft der Medien in Wirtschaft und Gesellschaft – Deutschlands Weg in die Informationsgesellschaft“ des 13. Deutschen Bundestages.

[9] Vgl. Büllesbach, Alfred (1997): Datenschutz und Datensicherheit als Qualitäts- und Wettbewerbsfaktor. Tagungsband 20. DAFTA (1996). Köln.

[10] Vgl. die Ergebnisse der G7-Ministerkonferenz über die Informationsgesellschaft am 25. und 26. Februar 1995 in Brüssel, abrufbar unter [http://www.ispo.cec.be/g7/keydocs/G7en.html].

[11] Vgl. Report of the Ad Hoc Meeting of Experts on Information Infrastructures. Issues Related to Security of Information Systems and Protection of Personal Data and Privacy. Paris 1996 (OECD/GD(96)74). Neuester Stand bei der OECD sind die Ergebnisse der Ottawa-Konferenz vom Oktober 1998. Vgl. XXX

[12] Vgl. Europäische Initiative für den elektronischen Geschäftsverkehr. Mitteilung an das Europäische Parlament, den Rat, den Wirtschafts- und Sozialausschuß und den Ausschuß der Regionen vom 14.4.1997. KOM (97) 157: 21 f.; zuvor schon: Europe and the Global Information Society. Recommendations to the European Council. Brüssel, 26. Mai 1994. Kapitel 3 unter Privacy, Europe`s Way to the Information Society. An action plan. Luxemburg 1995. Kapitel I.6.

[13] Vgl. die Erklärung des U.S.-Präsidenten Bill Clinton „A Framework for Global Electronic Commerce“, abrufbar unter [http://www.whitehouse.gov].

„elektronischer Handel“ behandelt, hat auf Vorschlag der Europäischen Kommission den Schutz der Privatsphäre in den zu behandelnden Fragenkatalog aufgenommen.

Auch das Beratungsgremium der alten Bundesregierung, der Rat für Forschung, Technologie und Innovation, geht bei seinen 1995 veröffentlichten Empfehlungen davon aus, daß ein konsequenter Datenschutz zu den zentralen Akzeptanzvoraussetzungen der Informationsgesellschaft zählt.[14][14] Die bestehenden Datenschutzgesetze, die vor dem Hintergrund eines inzwischen weitgehend überholten Technikszenarios entstanden sind, das von zentralen Großrechneranlagen ausging, geraten angesichts der rasanten technischen Entwicklung – Stichworte Dezentralisierung und Vernetzung – immer mehr an ihre Grenzen. Aus diesem Grund empfahl der Technologierat der Bundesregierung bereits 1995: „Eine Novellierung des Bundesdatenschutzgesetzes sollte aufgrund der technischen Veränderungen, die geprägt sind von Vernetzung und Dezentralisierung, möglichst bald erfolgen.“[15][15]

Erst vor wenigen Wochen hat die Enquete-Kommission des Deutschen Bundestages „Zukunft der Medien in Wirtschaft und Gesellschaft – Deutschlands Weg in die Informationsgesellschaft“ in ihrem vierten Zwischenbericht und in ihrem Schlußbericht die Bedeutung des Datenschutzes betont und angemahnt, daß die anstehende Umsetzung der EU-Datenschutzrichtlinie „zu einer umfassenden Novellierung des Bundesdatenschutzgesetzes und anderer datenschutzrechtlicher Regelungswerke genutzt werden sollte“.[16][16]

Herausforderungen an das Datenschutzrecht durch die europäische Integration

[14] Vgl. Rat für Forschung, Technologie und Innovation (1995): Informationsgesellschaft. Chancen, Innovationen und Herausforderungen. Bonn. Vgl. hierzu besonders Empfehlungen Nr. E 22 bis E 27. Die Empfehlungen des Rates sind auch abrufbar unter [http://www.iid.de].

[15] Vgl. Rat für Forschung, Technologie und Innovation (1995): Informationsgesellschaft. Chancen, Innovationen und Herausforderungen. Bonn. Empfehlung E 22.

[16] Vgl. dazu ausführlich den Zwischenbericht „Sicherheit und Schutz im Netz“ (BT-Drs. 13/11002) und den Schlußbericht „Deutschlands Weg in die Informationsgesellschaft“ (BT-Drs. 13/11004) der Enquete-Kommission „Zukunft der Medien in Wirtschaft und Gesellschaft – Deutschlands Weg in die Informationsgesellschaft“ des 13. Deutschen Bundestages; hier zitiert aus dem Zwischenbericht „Sicherheit und Schutz im Netz“ (BT-Drs. 13/11002): 108.

Neben die neuen Herausforderungen durch Technik ist die Herausforderung der europäische Integration und die dadurch notwendige Harmonisierung des Rechts getreten: Nach langen und schwierigen Verhandlungen – ein erster Entwurf lag bereits im Jahr 1990 vor – hat das Europäische Parlament am 24. Oktober 1995 die „Richtlinie zum Schutz personenbezogener Daten und zum freien Datenverkehr" verabschiedet. Mit dieser Richtlinie sollen ein einheitliches Datenschutzniveau geschaffen und einheitliche Maßstäbe für die Erhebung und Verarbeitung von Daten in der Europäischen Union festgelegt werden. Unter diesem Gesichtspunkt leistet die Richtlinie vor allem einen wichtigen Beitrag für den Aufbau eines „Europas der Bürger".[17][17]

Zwar stellt die Richtlinie keinen konzeptionellen Neuentwurf aus „einem Guß" dar, sondern ein „patchwork aus unterschiedlichen einzelstaatlichen Datenschutzsystemen"[18][18]. Dennoch orientiert sie sich in einigen Teilen stark am deutschen Datenschutzsystem. Grundsätzlich gibt die EU-Datenschutzrichtlinie folgende Rahmenbedingungen vor:

- Vereinheitlichung der Vorschriften für den öffentlichen und nicht-öffentlichen Bereich; von einigen Detailbestimmungen abgesehen wird auf die Unterscheidung zwischen öffentlicher und nicht-öffentlicher Datenverarbeitung verzichtet.[19][19]
- Die Richtlinie ordnet die Zweckbindung der Datenverarbeitung an(20)[20], verpflichtet datenverarbeitende Stellen generell zur Aufklärung und Information der Betroffenen[21][21] und gibt letzteren ein Recht auf die Kontrolle der Verarbeitung ihrer personenbezogenen Daten.[22][22]

[17] Bizer, Johann (1998): BDSG – quo vadis? In: DuD 22/1998: 349.

[18] Walz, Stefan: Datenschutz-Herausforderung durch neue Technik und Europa. In: DuD 3/1998: 150-154, hier 150.

[19] Vgl. dazu Schild, Hans Hermann: Die EU-Datenschutzrichtlinie. In: EuZW 1996: 549-554, hier 550.

[20] Vgl. Art. 6 Abs. 1 lit. b-e, Abs. 2 EU-Datenschutzrichtlinie.

[21] Vgl. Art. 10, 11 EU-Datenschutzrichtlinie.

[22] Vgl. Art. 12 EU-Datenschutzrichtlinie.

- Der EU-Datenschutzrichtlinie zufolge ist Selbstregulierung zu fördern: Die Mitgliedsstaaten haben vorzusehen, daß Berufsverbände und anderen Vereinigungen Verhaltensregeln ausarbeiten und Verfahren entwickeln.[23][23]
- Im Gegensatz zum deutschen Datenschutzrecht sieht die EU-Richtlinie bestimmte Daten als besonders sensibel an; sie verpflichtet die Mitgliedsstaaten daher dazu, die Verarbeitung personenbezogener Daten über die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, die Gewerkschaftszugehörigkeit sowie von Gesundheitsdaten und Daten über das Sexualleben zu untersagen.[24][24] Zugleich läßt sie jedoch eine Reihe Ausnahmen zu.[25][25]
- Für den Datenverkehr von erheblicher Bedeutung sind die in Art. 25 ff. der Richtlinie aufgestellten Regelungen des Datenexports in Drittländer. Diesen zufolge ist die Datenübermittlung in ein Drittland untersagt, wenn dieses kein angemessenes Datenschutzniveau aufweist.[26][26] Wann dies der Fall ist, soll in einem besonderen Verfahren geklärt werden können, um sicherzustellen, daß die Mitgliedsstaaten von einer gemeinsamen Beurteilung ausgehen.[27][27] Eine wichtige Einschränkung des grundsätzlichen Verbots des Exports von Daten in Drittländer ohne angemessenes Schutzniveau enthält Art. 26 Abs. 2 der Richtlinie. Danach können die Mitgliedsstaaten der EU einen Datenexport in solche Länder dann genehmigen, wenn die für die Datenverarbeitung Verantwortlichen ausreichende Garantien für den Schutz der Privatsphäre, der Grundrechte und der Grundfreiheiten der betroffenen Personen bieten. Solche Garantien sollen sich insbesondere durch entsprechende Klauseln in einem Vertrag mit dem für die Datenverarbeitung in dem Drittstaat Verantwortlichen ergeben können. In Drittländer exportiert werden dürfen personenbezogene Daten darüber hinaus unter anderem dann, wenn die betroffene Person ihre

[23] Vgl. Art. 27 EU-Datenschutzrichtlinie.
[24] Vgl. Art. 8 Abs. 1 EU-Datenschutzrichtlinie.
[25] Vgl. Art. 8 Abs. 2-5 EU-Datenschutzrichtlinie.
[26] Vgl. Art. 25 Abs. 1 EU-Datenschutzrichtlinie.
[27] Vgl. Art. 25 Abs. 2-6 EU-Datenschutzrichtlinie.

Einwilligung gegeben hat oder die Datenübermittlung aufgrund eines Vertrages zwischen der betroffenen Person und der datenverarbeitenden Stelle erfolgt.[28][28]

- Daneben stellt die EU-Datenschutzrichtlinie Anforderungen auch an den technischen Datenschutz. Die Mitgliedsstaaten haben Vorschriften zu erlassen, die dazu verpflichten, angemessene technische und organisatorische Maßnahmen zum Schutz gegen den unberechtigten Zugang zu personenbezogenen Daten sowie gegen deren unberechtigte Änderung und Weitergabe zu ergreifen.[29][29]
- Verbesserung der Datenschutzkontrolle unter dem Gesichtspunkt der Unabhängigkeit und Effektivität sowie die Stärkung der Rolle behördlicher und betrieblicher Datenschutzbeauftragter, die zudem mit umfassenden Untersuchungs- und wirksamen Einwirkungsbefugnissen ausgestattet sind.[30][30] Die EU-Richtlinie gibt vor, daß in den Mitgliedsstaaten eine oder mehrere öffentliche Kontrollstellen „in völliger Unabhängigkeit" errichtet werden, die neben weitreichenden Untersuchungs- und Einwirkungsbefugnissen auch mit einem Klage- oder Anzeigerecht, einen Beratungs- und Berichterstattungsauftrag ausgestattet sein sollen.

Die Richtlinie macht erhebliche Anpassungen und Änderungen des BDSG notwendig – über die Reichweite der Reform herrscht jedoch alles andere als Einigkeit. Zwischen „Minimalismus" und „Modernisierung"[31][31] – so kann die derzeitige politische Debatte über die Zukunft des Datenschutzes wohl zusammengefaßt werden.

[28] Vgl. Art. 26 Abs. 1 lit a, b EU-Datenschutzrichtlinie.

[29] Vgl. Art. 17 Abs. 1 EU-Datenschutzrichtlinie.

[30] Vgl. Art. 28 Abs. 1-7 EU-Datenschutzrichtlinie.

[31] Landesbeauftragter für den Datenschutz (LfD) der Freien Hansestadt Bremen: 20. Jahresbericht. Vorgelegt zum 31. März 1998: 6.

Globale Herausforderungen an das Datenschutzrecht

Bei der Debatte um die Umsetzung der EU-Richtlinien in Deutschland darf jedoch nicht außer acht gelassen werden, daß die Harmonisierung europäischer Datenschutzsysteme zwar einen wichtigen ersten Schritt darstellt, daß mittelfristig jedoch weit über Europa hinausgehende Regelungen gefunden werden müssen. Den Globalisierungstendenzen in allen gesellschaftlichen Bereichen, wie sie beispielsweise im Wirtschaftssystem seit einiger Zeit beobachtet werden können und die durch die weltweite Digitalisierung und Vernetzung erheblich beschleunigt werden, muß auch eine Globalisierung von Regelungssystemen folgen. Bislang stehen sich auf internationaler Ebene sehr unterschiedliche einzelstaatliche Datenschutzsysteme und Datenschutzniveaus gegenüber. Sie reichen von Staaten mit einem relativ starken und elaborierten Regelungsgefüge zum Schutz der Privatsphäre bis hin zu Rechtssystemen, die den Datenschutz nur marginal oder überhaupt nicht garantieren.

International ist es bisher vor allem im Rahmen des Europarates, der Vereinten Nationen und der Organisation für wirtschaftliche Zusammenarbeit gelungen, *Mindeststandards* festzuschreiben, die sich jedoch inhaltlich und vor allem hinsichtlich ihrer Durchsetzbarkeit unterscheiden:[32][32]

- **Europarat:** Das Europarats-Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten vom 28. Januar 1981 stellt u.a. ein datenschutzrechtliches Zweckbindungsgebot auf und verlangt Sicherungsmaßnahmen gegen den unbefugten Zugang zu Datenbeständen.[33][33]

[32] Vgl. zum folgenden auch den Vierten Zwischenbericht „Sicherheit und Schutz im Netz“ der Enquete-Kommission „Zukunft der Medien in Wirtschaft und Gesellschaft – Deutschlands Weg in die Informationsgesellschaft“ (BT-Drs. 13/11002: 105f.).

[33] Europarat: Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten. Konvention 108. Abgedruckt in: Simitis, Spiros/Dammann, Ulrich/Mallmann, Otto/Reh, Hans-Joachim: Dokumentation zum Bundesdatenschutzgesetz. Band 2. Ausland und Internationales. Abschnitt D 3.3. Baden-Baden. Stand: August 1997. Ergänzt wurde das Übereinkommen durch mehrere Empfehlungen und Entschließungen des Europarates, die am gleichen Ort abgedruckt sind: So gab der Europarat Empfehlungen und Entschließungen zum Schutz der Privatsphäre natürlicher Personen gegenüber elektronischen Datenbanken im öffentlichen und nichtöffentlichen Bereich (D 3.1 und D 3.2), zum Schutz personenenbezogener Daten beim wissenschaftlichen Umgang (D 3.4), für Zwecke der Direktwerbung (D 3.5), für Zwecke der sozialen Sicherheit (D 3.7), bei der Nutzung von Daten im Polizeibereich (D. 3.8), für Beschäftigungszwecke (D 3.9), für Zahlungszwecke (D 3.10), für die Übermittlung der von öffentlichen Stellen gespeicherten personenbezogenen

Derzeit werden Ergänzungen des Übereinkommens vorbereitet, die Regelungen aus der EU-Richtlinie übernehmen sollen, beispielsweise das Errichtung einer unabhängigen Kontrollinstanz.

- **Vereinte Nationen:** 1990 wurden von der Generalversammlung der Vereinten Nationen die Richtlinien betreffend personenbezogener Daten in automatisierten Dateien beschlossen. Diese Richtlinien legen für die Erhebung und Verarbeitung von personengebunden Daten in automatisierten Dateien die Grundsätze der Richtigkeit und der Zweckbestimmung und -gebundenheit fest und räumen den Betroffenen ein Informationsrecht ein.
- **OECD:** Die Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD) hat 1980 „Leitlinien für den Schutz des Persönlichkeitsbereichs und den grenzüberschreitenden Verkehr personenbezogener Daten“ verabschiedet. Sie enthalten an die Mitgliedsstaaten gerichtete Empfehlungen, denen zufolge unter anderem die Grundsätze von Zweckbindung, Transparenz und der Beteiligung des Betroffenen bei der Datenverarbeitung zu beachten sind. Insgesamt können die Leitlinien als Ausdruck eines internationalen Konsenses über Datenschutzprinzipien zu Beginn der Computerrevolution angesehen werden.[34][34] 1985 wurden sie ergänzt um eine Erklärung über den grenzüberschreitenden Datenverkehr.[35][35] 1992 verabschiedete die OECD Leitlinien für die Sicherheit von Informationssystemen[36][36], die ebenfalls unter anderem dem Schutz der Vertraulichkeit und der Privatsphäre dienen sollen. 1996 veröffentlichte die OECD einen Expertenbericht über die Sicherheit von Informationssystemen und Datenschutz, in dem sie weiteren Handlungsbedarf konstatiert.[37][37] Auch in den im Oktober 1998 in Ottawa verabschiedeten Aktionsplan zum Elektronischen Handel wird dem Schutz der

Daten an Dritte (D 3.11) und auf dem Gebiet der Telekommunikationsdienste, unter besonderer Bezugnahme auf Telefondienste (D 3.12).

[34] Vgl. Information Policy Committee der National Information Task Force: Options for Promoting Privacy on the National Information Infrastructure, Draft for Public Comment, Executive Summary, April 1997, unter I.1.

[35] Declaration on Transborder Data Flow, abrufbar unter [http://www.oecd.org/dsti/iccp/legal/d-flow-e.html].

[36] Guidelines for the Security of Information Systems, abrufbar unter [http://www.oecd.org/dsti/iccp/legal/secur-en.html].

personenbezogenen Daten in weltweiten Datennetzen große Bedeutung zugeschrieben.[38][38]

- ***WTO*** – Die Welthandelsorganisation hat sich im Mai dieses Jahres auf ein ausführliches Arbeitsprogramm zum Thema „Elektronischer Geschäftsverkehr" geeinigt. Auf Vorschlag der Europäischen Kommission wurde der Schutz der Privatsphäre in den Fragenkatalog aufgenommen, wobei jedoch hier mit schnellen Lösungen nicht zu rechnen ist.

Die vorherige Bundesregierung hat sich leider nicht mit der notwendigen Intensität an internationalen Internet-Aktivitäten und an der Debatte über Regulierungsvorhaben beteiligt. Notwendig ist es vor allem, daß eine SPD-geführte Bundesregierung die internationale Zusammenarbeit deutlich intensiviert und auf der Grundlage bereits bestehender Übereinkünfte sich verstärkt um die Entwicklung weltweiter und durchsetzbarer Regelungen zur Wahrung des Rechtes auf informationelle Selbstbestimmung bemüht.

Novellierung des Datenschutzrechts: ‚Alter Wein in neuen Schläuchen' oder (Weiter-)Entwicklung eines zeitgemäßen Datenschutzrechts als gesellschaftliches Modernisierungsprojekt?

Die anstehenden Umsetzungen der EU-Datenschutzrichtlinie und der neuen Richtlinie 97/66/EU über den Datenschutz in der Telekommunikation leisten nicht nur einen enormen Beitrag zur europäischen Integration, sie sind zugleich auch zu verstehen als „Aufforderungen und Chance, den Datenschutz fortzuentwickeln"[39][39]. Die Weiterentwicklung des traditionellen Datenschutzes erweist sich jedoch nicht nur hinsichtlich der technischen und europäischen Herausforderungen als notwendig, sondern ist darüber hinaus Grundvoraussetzung zur Wahrung des Grundrechts auf

[37] Report of the Ad Hoc Meeting of Experts on Information Infrastructures: Issues Related to Security of Information Systems and Protection of Personal Data and Privacy (OCDE/GD (96)74).

[38] OECD Ministerial Conference „A Borderless World: Realising the potential of global electronic commerce". OECD Action Plan for electronic commerce. 7-9 october 1998, Ottawa, Canada. SG/EC (98)9/REV 5. Abrufbar unter [http:www.ottawaoecdconference.org].

[39] DuD 7/1996: 425f.

informationelle Selbstbestimmung und damit Voraussetzung zur aktiven Teilhabe der Bürgerinnen und Bürger an der entstehenden Wissens- und Informationsgesellschaft. Die Weiterentwicklung des Datenschutzes ist gleichzeitig erforderlich, um die erheblichen Potentiale zur Modernisierung von Staat und Verwaltung, zur Verwirklichung von Transparenz und zur Legitimierung staatlichen Handelns zu nutzen.[40][40]

Hierbei stellt sich zunächst die Frage, welche Erwartungen die Menschen hinsichtlich des Schutzes ihrer personenbezogener Daten an die Politik richten. Empirische Untersuchungen belegen eine – nicht nur in Deutschland – wachsende Sensibilität für den Schutz der Privatsphäre vor durch die neuen Medien bedingten Gefahren. So sind einer im Auftrag der Europäischen Kommission erstellten repräsentativen Untersuchung zufolge zwei Drittel der EU-Bürger über Datenspuren in Telekommunikationsnetzen besorgt; die weit überwiegende Mehrheit würde die neuen Technologien nicht oder nur mit Einschränkungen nutzen, wenn die Gefahr besteht, daß personenbezogene Daten ausgeforscht und zu Zwecken verwendet werden, mit denen sie nicht einverstanden sind.[41] [41]

Der Bürger hat gemäß der EU-Richtlinie zum Datenschutz einen Anspruch darauf, über die Speicherung und die Weitergabe seiner Daten unterrichtet zu werden. Damit dieses Recht auf informationelle Selbstbestimmung auch in Zukunft gewahrt bleibt, muß jeder einzelne zunächst erst einmal wissen, welche Institution seine personenbezogenen Daten „benutzt". Hierbei erweist sich jedoch das Problem, daß der „Bürger sich im institutionellen Daten-Dschungel kaum mehr zurecht findet".[42][42] Eine 1998 vom BAT-Freizeit-Forschungsinstitut in Deutschland durchgeführte Repräsentativbefragung läßt zudem ein großes Mißtrauen der Bevölkerung

[40] Vgl. dazu Kapitel 7 „Bürger und Staat" (S. 78ff.) und das Sondervotum der Fraktion Bündnis 90/Die Grünen „Elektronische Demokratie" (S. 137ff.) des Schlußberichtes „Deutschlands Weg in die Informationsgesellschaft" der Enquete-Kommission „Zukunft der Medien in Wirtschaft und Gesellschaft – Deutschlands Weg in die Informationsgesellschaft" (BT-Drs. 13/11004).

[41] Vgl. Eurobarometer 46.1: Information Technology and Data Privacy. Report produced for the European Commission, Directorate General „Internal Market and financial services". Brüssel 1997.

[42] Opaschowski, Horst unter Mitarbeit von Duncker, Christian: Der gläserne Konsument? Multimedia und Datenschutz. BAT-Freizeit-Forschungsinstitut: Hamburg.

gegenüber Institutionen erkennen.[43][43] Die überwiegende Mehrheit ist der Ansicht, daß man den Institutionen im Hinblick auf den zuverlässigen Umgang mit Daten *nicht* vertrauen kann.[44][44] Die BAT-Studie stellt fest, daß nach Ansicht der Befragten weniger „Gesetzeslücken" als vielmehr *Naivität*, *Sorglosigkeit* und vor allem *Unwissenheit* die Ursache für dieses fehlende Vertrauen sind. Gleichwohl wünscht sich mehr als die Hälfte der Befragten von der Politik und der Wirtschaft einen verstärkten Schutz der persönlichen und geschäftlichen Daten.[45][45]

Nun wird die Politik dem einzelnen die Verantwortung für den sorgsamen Umgang mit seinen personenbezogenen Daten weder abnehmen können noch sollen. Dennoch muß jeder Bürger und jede Bürgerin nicht nur bereit, sondern auch in der Lage sein, diese Verantwortung für den Schutz seiner persönlichen Informationen zu übernehmen. Dabei wird man sich in der entstehenden Informations- und Wissensgesellschaft weniger auf die Verantwortung der anderen verlassen können, als vielmehr auf einen aktiven Selbstschutz setzen müssen. Dieser Ansatz setzt allerdings voraus, daß der Gesetzgeber seiner Strukturverantwortung gerecht wird und die Voraussetzungen für diesen Selbstschutz schafft. Unverzichtbar ist daher eine aktive und informierte Öffentlichkeit.

[43] Opaschowski, Horst unter Mitarbeit von Duncker, Christian: Der gläserne Konsument? Multimedia und Datenschutz. BAT-Freizeit-Forschungsinstitut: Hamburg. Im Rahmen dieser Studie wurden 3.000 Perosnen ab 14. Jahren repräsentativ befragt, in welchen Institutionen ihres Wissens nach persönliche Informationen über sie „gespeichert sind und verarbeitet werden". Die umfangreichsten Datenspeicher vermutet die Bevölkerung bei den Krankenkassen (90%) und den Meldeämtern (89%); auch Versicherungen (87%), Banken (87%), Ärzte (87%) und Finanzämter (80%) werden mehrheitlich genannt. Bei der Einschätzung der Finanzämter ist jedoch fast jeder sechste Befragte (16%) davon überzeugt, daß „sein" Finanzamt „keine" personenbezogenen Daten gespeichert hat. Zwei Drittel der Bevölkerung (62%) gehen davon aus, daß der Adreßhandel Geschäfte mit ihren persönlichen Daten macht. Ein großer Unterschied zwischen Ost und West wird bei der Frage deutlich, ob die Polizei und der Verfassungsschutz personenbezogene Daten der Befragten speichern und verarbeiten: Während beispielsweise etwa jeder zweite Westdeutsche (54%) von einer Datenspeicherung bei der Polizei ausgeht, sind des in Deutschland-Ost fast drei Viertel (73%) der Bevölkerung. Fast jeder zweite Bundesbürger (47%, in Deutschland-Ost 54%, in Deutschland-West 45%) hat den Eindruck, daß der Verfassungsschutz persönliche Daten über ihn gespeichert hat. Hochgerechnet wären das fast *30 Millionen* Bundesbürger, die sich vom Verfassungsschutz „erfaßt" fühlen. Vgl. S. 22f. und Graphik S. 59.

[44] Das größte Vertrauen im Umgang mit personenbezogenen Daten genießen die Ärzte (56%), lediglich 42% trauen den Meldeämtern einen sorgsamen Umgang mit Daten zu, 41% gehen von einem sorgsamen Umgang mit personenbezogenen Daten beim Verfassungsschutz aus, während knapp die Hälfte der Bevölkerung (49%) überzeugt ist, daß die Polizei verantwortungsvoll mit diesen Daten umgeht. Nur knapp ein Drittel (30%) der Bevölkerung vertraut beim Schutz ihrer Daten den Versicherungen und nur acht von hundert Befragten trauen dem Adreßhandel. Vgl. Opaschowski, Horst unter Mitarbeit von Duncker, Christian: Der gläserne Konsument? Multimedia und Datenschutz. BAT-Freizeit-Forschungsinstitut: Hamburg. S. 23f. und Graphik S. 60.

[45] Vgl. Opaschowski, Horst unter Mitarbeit von Duncker, Christian: Der gläserne Konsument? Multimedia und Datenschutz. BAT-Freizeit-Forschungsinstitut: Hamburg. S. 30.

Damit wird deutlich, daß der Zugang zu Informationen und der Schutz von Informationen zwei Seiten derselben Medaille darstellen, die jedoch auch in einem Spannungsverhältnis stehen. So hat das Recht auf informationelle Selbstbestimmung nicht nur eine abwehrrechtliche Funktion zur Zurückweisung staatlicher Eingriffe in die Freiheitsausübung des einzelnen. Der Grundrechtskatalog insgesamt normiert vielmehr einen „bürgerlichen Status, der – neben der Möglichkeit, sich gegen den Staat abzuschirmen – davon ausgeht, daß Bürgerinnen und Bürger ihr Leben frei und selbstverantwortlich gestalten und an den Angelegenheiten des Gemeinwesens mitwirken sollen."[46] Der Schutz des Grundrechts auf informationelle und kommunikative Selbstbestimmung [47] dient somit nicht nur der Eingriffsabwehr im Sinne einer grundsätzlichen Verfügungsbefugnis über die individualisierten Daten oder zumindest dem Wissen über deren Verwendung, sondern ebenso dem Ziel, die Kommunikations- und Handlungsfähigkeit des Menschen gegenüber der Gesellschaft und auch gegenüber staatlichen Stellen zu gewährleisten. Das Bundesverfassungsgericht hat mit Bezug auf Artikel 5 GG klargestellt: „Der Kommunikationsprozeß, den Art. 5 Abs. 1 GG im Interesse der freien individuellen und öffentlichen Meinungsbildung schützen will [...], wäre nur unvollkommen erfaßt, wenn die Informationsaufnahme von dem Schutz ausgenommen wäre."[48]

Zusammengefaßt kann festgestellt werden, daß das Recht auf informationelle Selbstbestimmung in seiner datenschutzrechtlichen Ausprägung *und* daß die Sicherstellung des Informationszugangs die Teilhabe des Menschen an der Gesellschaft erst ermöglichen und garantieren. Ein so verstandenes erweitertes Datenschutzrecht könnte damit einen erheblichen Beitrag zur Modernisierung von Gesellschaft, Staat und Verwaltung leisten: Der so garantierte Schutz der personenbezogenen Daten und der gleichzeitige Schutz des Zugangs zu Informationen – beides Grundvoraussetzungen zur aktiven gesellschaftlichen Teilhabe – könnte dazu beitragen, Akzeptanz in die neuen Informations- und Kommunikationsmöglichkeiten aufzubauen, staatliches Handeln transparent zu machen und die aus dem Mißtrauen gegenüber (staatlichen) Institutionen möglicherweise erwachsenden Legitimationsdefizite abzubauen bzw. zu verhindern.

Hinzu kommt, daß die neuen Informations- und Kommunikationsmöglichkeiten auch die Partizipationsmöglichkeiten der Bürgerinnen und Bürger erheblich ausweiten können – Stichwort könnte sein: *electronic government mit begleitendem Datenschutz.*

Diese Chancen des wichtigen „Zukunftsfaktors" Datenschutz zur Weiterentwicklung eines zentralen Grundrechts und zur Modernisierung von Staat und Verwaltung sind jedoch – zumindest in der politischen Diskussion – noch immer nicht hinreichend gewürdigt. Eine konstruktiv-kritische Analyse der (neuen) Bedingungen moderner Datenverarbeitung und der damit einher gehenden Modernisierungspotentiale fand bisher nicht statt, weder bei der Debatte über die Richtlinienvorgaben, noch bei der Debatte um die Novellierung des BDSG.

Zwar hat ein Beratungsgremium der vorherigen Bundesregierung, der Rat für Forschung, Technologie und Innovation, bereits 1995 festgestellt, daß es notwendig sei, das traditionell normativ ausgerichtete Datenschutzrecht um Datenschutztechnologie zu ergänzen und Bestimmungen, die einen Grundstandard an organisatorischen und technischen Sicherheitsmaßnahmen gewährleisten, zu erarbeiten.[49] Außerdem ist es erforderlich, das Datenschutzrecht mehr und mehr darauf auszurichten, den Selbstschutz der Nutzer und den Systemdatenschutz zu unterstützen, indem es etwa datensparende und datenvermeidende Technik privilegiert. All dies fand in den Entwürfen der alten Bundesregierung keinen Eingang, vielmehr zeigen diese das Bestreben, das deutsche Datenschutzrecht möglichst wenig zu verändern und möglichst gar nicht mit neuen Regelungen bzw. Regelungen anderer Datenschutzsysteme zu konfrontieren.[50]

Die Frist für die Anpassung des deutschen Datenschutzrechts an die EU-Richtlinie 95/46/EU („Datenschutzrichtlinie") lief am 24. Oktober 1998 ab. Zwar kursierte bereits im Frühsommer 1997 ein erster Arbeitsentwurf aus dem zuständigen Referat des BMI, über den Anfang 1998 vorgelegten Referentenentwurf (Stand: 08.12.1997) zur Novellierung des Bundesdatenschutzgesetzes konnte jedoch innerhalb der alten Bundesregierung nicht einmal mehr Einigkeit erzielt werden. Hinzu kam, daß dieser Entwurf angesichts der mangelnden Bereitschaft, innovative und wirksame

Instrumente in das Datenschutzrecht einzubauen, bereits im Vorfeld auf heftige Kritik gestoßen ist. Die Novellierung des Datenschutzrechts wurde somit kurzerhand von der Tagesordnung gestrichen und auf die Zeit nach die Bundestagswahl im Herbst 1998 vertagt. Die Entwicklung eines zeitgemäßen und der entstehenden Informationsgesellschaft angemessenen Datenschutzkonzeptes ist damit offensichtlich im allgegenwärtigen „Reformstau“ steckengeblieben. Gleiches gilt für den noch immer fehlenden Arbeitnehmerdatenschutz. Zwar wurden hier gesetzliche und außergesetzliche Regelungen immer wieder angekündigt, jedoch ist es bei den Ankündigungen geblieben.

Einem modernen und wirksamen Datenschutz kommt jedoch – nicht nur im Hinblick auf den Ablauf der Umsetzungsfrist – in der sich entfaltenden Wissens- und Informationsgesellschaft eine herausragende Bedeutung zu. Will die Gesellschaft beim Übergang zur Wissens- und Informationsgesellschaft am Ziel eines freiheitlich-demokratischen Gemeinwesens festhalten, kommt sie nicht umhin, auch in einer vernetzten und digitalisierten Welt das Grundrecht auf informationelle und kommunikative Selbstbestimmung zu bewahren. Die Entwicklung eines modernen Datenschutzkonzeptes ist damit ein zentrales Reform- und Modernisierungsprojekt[51] der nächsten Jahre und hat von daher auch Eingang in die Koalitionsvereinbarung zwischen der SPD und Bündnis 90/Die Grünen gefunden.[52] Mit diesem Papier legen wir für die SPD-Bundestagsfraktion erste Eckwerte vor, die die (Weiter-)Entwicklung eines modernen Datenschutzkonzeptes – nun in der Regierungsverantwortung – maßgeblich leiten und beschleunigen sollen.

Bausteine eines modernen Datenschutzrechts:

Die aufgrund der Umsetzung der EU-Datenschutzrichtlinie notwendige Novellierung oder Neuformulierung datenschutzrechtlicher Rahmenbedingen sollte als Chance erkannt werden, auch auf neue Technikrisiken zu reagieren, wie dies auch die Datenschutzbeauftragten des Bundes und der Länder gefordert haben.[53] Dabei darf jedoch auch bei der Debatte um eine umfangreiche Novellierung die Gefahr einer Verengung auf die Ebene rechtlicher Regulierung nicht unterschätzt werden.

Es gilt zu vermeiden, daß „juristische Sandkastenspiele“[54] stattfinden, die ohne nennenswerten Einfluß auf die Zukunft der Informationsgesellschaft bleiben. Die Formulierung eines zeitgemäßen Datenschutzkonzeptes ist eine wichtige Querschnittsaufgabe, was auch in der Erarbeitungsphase und in der politischen Verantwortlichkeit bzw. Zuständigkeit Konsequenzen haben muß.

Das traditionell normative Datenschutzkonzept muß um technikrechtliche und außerrechtliche Regelungen sowie möglicherweise um selbstregulative Aspekte ergänzt werden. Dabei sind als Ergänzung der traditionellen Elemente vor allem zu nennen:[55]

- **Datenschutz durch Technik:** Die neuen technischen Möglichkeiten stellen nicht nur eine Gefährdung für die Grundrechte dar, sondern können auch im Dienste der Grundrechte eingesetzt werden. Hierzu müssen Anforderungen zur datenschutzfreundlichen Ausgestaltung von Informations- und Kommunikationstechnik entwickelt werden. Dazu gehören vor allem die Prinzipien Datensparsamkeit und Datenvermeidung. Datenschutzfreundliche Technik kann sicher nicht als „Königsweg“ eines modernen Datenschutzkonzeptes angesehen werden, sie kann dazu beitragen, „wertorientierten Grundrechtsschutz durchsetzen helfen, nicht aber ihn ersetzen“[56]. Hieraus ergeben nicht nur immense Chancen für Innovationen im Bereich der Informations- und Kommunikationstechnik, sondern auch neue Zielsetzung für eine vernünftige Forschungs- und Förderpolitik im Bereich der IT-Sicherheit und des Datenschutzes. Aufgabe der Politik wird es sein, verstärkt datenschutzfreundliche Technik zu normieren. So könnten beispielsweise rechtliche Vorgaben entwickelt werden, die einen Anbieter, der einen bestimmte Dienstleistung anbieten will (z.B. e-commerce) verpflichtet, auch bestimmte technische Möglichkeiten bereitzustellen und umfassend darüber zu informieren. [Denkbar wäre auch, dies über eine Änderung des Haftungsrechts zu konzipieren.]
- **Ermöglichung anonymer und pseudonymer Nutzung:** Um die Gebote der Datensparsamkeit und Datenvermeidung zu erfüllen, müssen anonyme und pseudonyme Nutzungsmöglichkeiten entwickelt und gefördert werden, um den

Betroffenen ein Höchstmaß an Schutz der Privatsphäre gegenüber Netzbetreibern und Dienstleistungsanbietern zu garantieren.

- **Selbstschutzinstrumente:** Angesichts der zunehmenden Ohnmachtserfahrungen des Staates[57] bei der Durchsetzung von Normen in der globalen Informationsgesellschaft kommt den Möglichkeiten des Selbstschutzes enorme Bedeutung zu. Eine Einschränkung der Nutzungsmöglichkeiten dieser Instrumente, beispielsweise kryptographischer Verfahren, wäre unverhältnismäßig und verfassungsrechtlich bedenklich. Jedoch darf die Debatte nicht bei der Frage um Regulierung vs. Nichtregulierung von kryptographischen Verfahren stehen bleiben. Notwendig ist eine Aufklärung über die Gefährdungen bei der Nutzung der neuen Informations- und Kommunikationstechniken und über die Möglichkeiten des Selbstschutzes. Betroffene müssen zunächst erst einmal wissen, wie sie sich gegen Überwachung und Profilbildung zu Wehr setzen können, welche technischen Möglichkeiten es hierfür gibt und wie man diese einsetzt. Hier besteht ein erheblicher Beratungsbedarf im Hinblick auf die Möglichkeiten des Selbstschutzes. Gefordert sind nicht zuletzt die Medienpädagogik sowie die universitäre Ausbildung der Informatik.
- **Datenschutzaudit:** Ein wesentlicher Bestandteil eines modernen Datenschutzkonzeptes wird in der Möglichkeit einer freiwilligen Auditierung zur Stärkung der Selbstkontrolle und zur Stimulierung von Wettbewerb liegen.[58] Ursprünglich war ein solches Datenschutzaudit im Mediendienste-Staatsvertrag der Bundesländer und im Informations- und Kommunikationsdienstegesetz (IuKDG) des Bundes vorgesehen, im letzteren wurde dies aber von Seiten der Bundesregierung im Rahmen der parlamentarischen Beratung des IuKDG leider wieder herausgenommen. Dabei ist das Audit weltweit ein wesentlicher Baustein neuer Regelungsansätze: In anderen Ländern, beispielsweise in den USA, sind derartige Auditierungsverfahren zum Teil schon eine Selbstverständlichkeit, z.B. bei der Normierung technischer Standards. Unternehmen, die sich dem kanadischen Industriestandard (Datenschutz) anschließen, verpflichten sich, sich einmal jährlich einem solchen Auditierungsverfahren zu stellen. Dabei ist eine

zentrale Ausgangsüberlegung die Tatsache, daß ein solches Audit – auch aus wirtschaftlicher Perspektive – einen wesentlichen Wettbewerbsvorteil darstellen kann, wenn man als Unternehmen damit belegen kann, den vergleichsweise hohen Datenschutzregelungen in Europa bzw. Deutschland zu entsprechen – angesichts der immensen Unsicherheiten bei der Nutzung der weltweiten Datennetze ein nicht zu unterschätzendes „Qualitätsiegel". Auch die deutschen Erfahrungen mit dem Umweltaudit belegen dies.

- **Selbstregulierung:** Die EU-Datenschutzrichtlinie verpflichtet die Mitgliedsstaaten, im nationalen Datenschutzrecht Möglichkeiten der Selbstregulierung vorzusehen, und durch Verbände und Organisationen unterhalb der gesetzlichen Ebene bereichsspezifisch zu konkretisieren. Hintergrund dieser Verpflichtung ist der Versuch, dieses Instrument für den Schutz des Rechts auf informationelle Selbstbestimmung fruchtbar zu machen. Entstehen könnte so ein „Regelungsmix" aus „Entgesetzlichung" bei funktionierender Selbstkontrolle auf der einen Seite und Gesetzgebung als Sanktionsmittel für fehlende oder versagende Selbstkontrolle auf der anderen Seite.

(Erste) Eckwerte für die weitere Diskussion

Die neuen Informations- und Kommunikationstechniken und der dadurch beschleunigte Wandel zur Wissens- und Informationsgesellschaft zwingen zu einer Neuorientierung und Weiterentwicklung des Datenschutzrechts. Dabei erweist sich die Entwicklung eines der Informationsgesellschaft zeitgemäßen Datenschutzes als eine der zentralen Querschnittsaufgaben der neuen Legislaturperiode. Die umzusetzenden EU-Richtlinien geben der Politik Instrumente an die Hand, die es erlauben, auf die immensen Herausforderungen durch neue Informations- und Kommunikationstechniken und auf die Herausforderungen der europäischen Harmonisierung zu reagieren und die damit einher gehenden gesellschaftlichen Modernisierungspotentiale zu nutzen. Die SPD-Bundestagsfraktion formuliert für das Reform- und Modernisierungsprojekt Datenschutz folgende Eckwerte, die als

Ausgangspunkt für die Entwicklung und Formulierung von gesetzlichen und außergesetzlichen Regelungsansätzen dienen sollen:[59]

1. Die SPD-Bundestagsfraktion hält – auch der Koalitionsvereinbarung entsprechend[60] – die anstehende Umsetzung der EU-Richtlinien für eine wichtige Chance, die zu einer umfassenden Novellierung des Bundesdatenschutzgesetzes und anderer datenschutzrechtlicher Regelungswerke genutzt werden sollte. Aufgrund der unterschiedlichen Zuständigkeiten ist hierbei eine effektive Bund-Länder-Koordination unabdingbar. Die Umsetzung sollte - in einem zweiten Schritt - auch auf die bereichsspezifischen Regelungen erstreckt werden, für die es keine Umsetzungspflicht gibt. Nur so können Wertungswidersprüche und sachlich nicht gerechtfertigte unterschiedlich hohe Datenschutzstandards im bereichsspezifischen Datenschutzrecht vermieden werden.

2. Der Austausch personenbezogener Daten zwischen den Mitgliedsstaaten der Europäischen Union in den Bereichen Polizei, Zoll und Justiz wird - was im Interesse der Kriminalitätsbekämpfung zu begrüßen ist - zunehmend intensiviert und ausgeweitet. Das macht auf der anderen Seite aber auch flankierende datenschutzrechtliche Regelungen erforderlich, da die Datenschutzrichtlinie insoweit nicht gilt. Deshalb sind dieser Richtlinie entsprechende Rahmenregelungen für den 3. Pfeiler anzustreben.

3. Mit der notwendigen Novellierung des Datenschutzrechts, die sich aufgrund der Umsetzung der EU-Richtlinien ergibt und mit der eine Harmonisierung einzelstaatlicher Datenschutzrechtordnungen innerhalb der europäischen Gemeinschaft gelingen soll, muß eine „selbstkritische Evaluation des eigenen nationalen Datenschutzsystems“[61] einher gehen. Entscheidend hierfür ist die Frage nach dem *tatsächlich* von staatlichen Stellen und anderen Institutionen praktizierten Datenschutz. Notwendig ist hierfür eine interdisziplinäre Zusammenarbeit zwischen Politik, Rechts-, Technik- und Sozialwissenschaft, Datennutzern, Datenkontrolleuren und Betroffenen.

4. Wirksame Kontrolle ist die Voraussetzung eines erfolgreichen Datenschutzes. Wenn man Datenschutz zunehmend als Querschnittsaufgabe begreifen will, muß dies auch institutionelle Folgen haben. Um die – auch von der Richtlinie geforderte – vollständige Unabhängigkeit der Datenschutzinstanzen zu stärken und um Interessenkonflikte zu vermeiden, sollte der Bundesbeauftragte für Datenschutz nicht dem Innenministerium, sondern (ähnlich der Wehrbeauftragten des Bundestages) direkt dem Parlament zugeordnet werden.

5. Die gleiche Problematik stellt sich beim Bundesamt für Sicherheit in der Informationstechnik (BSI). Angesichts der Bedeutung, die diesem Bundesamt beim Aufbau einer nationalen Sicherungsinfrastruktur zukommt, sollte dies – vor allem im Hinblick auf die notwendige Neutralität im Spannungsverhältnis zwischen Datenschutz und öffentlicher Sicherheit – nicht dem Bundesinnenministerium, sondern beispielsweise dem Forschungs- und Technologieressort oder dem Wirtschaftsressort angegliedert werden. Dabei müssen zunächst die widersprüchlichen Aufgaben, die dem BSI mit dem BSIG zugewiesen wurden, beseitigt werden. Um das notwendige Vertrauen in dieses wichtige Amt zu erreichen, wäre eine Trennung des BSI in ein unabhängiges „ziviles“ Amt und ein davon getrenntes Amt für die sogenannten „Bedarfsträger“ ein möglicher Ansatz.[62]

6. Die Möglichkeiten der informationstechnischen Sicherheit – etwa im Sinne eines technischen Datenschutzes mittels Firewalls, digitale Signaturen, Kryptographie – müssen als ein zentrales Instrument zur Umsetzung eines „neuen Datenschutzes“ verstanden werden. Um zu einem wirklich effektiven Datenschutz zu kommen, muß das Zusammenwirken zwischen Datenschutz (Datenschutzbeauftragte des Bundes und der Länder) und Datensicherheit (Bundesamt für Sicherheit in der Informationstechnik) intensiviert werden. Neue Formen eines „institutionalisierten Dialogs“ zwischen Datenschutz und Datensicherheit – unter Einbeziehung von Datenkontrolleuren und –nutzern, Verbraucherverbänden, etc. – könnten hier ein öffentliches Form zur Sicherung der Privatsphäre im Informationszeitalter herstellen.

7. Angesichts der Unübersichtlichkeit und Kompliziertheit des Datenschutzrechts sollte im Interesse von datenverarbeitenden Stellen und Nutzern eine erhebliche Vereinfachung und Verschlankung des Datenschutzrechts im Vordergrund stehen. Dies darf jedoch nicht zu einer Aufweichung der verfassungsrechtlich garantierten Rechte oder zur Einschränkung oder Abschwächung bewährter Verfahren des Datenschutzes führen. Eine Vereinfachung und Verschlankung erweist sich aber vor allem deshalb als notwendig, um zu widerspruchsfreien, einheitlichen, praktikablen und vor allem auch verständlichen Regelungen zu gelangen.

   - *Vereinfachung:* Im Datenschutzrecht verstellen außerordentlich komplizierte Regelungen den Blick auf das eigentliche Grundanliegen des Datenschutzes, den Menschen und sein informationelles Selbstbestimmungsrecht auch in einer „vernetzten Gesellschaft“ zu schützen.[63] Werden diese Regelungen in Zukunft auch auf private Datenverarbeitung, also auch auf kleine und mittelständische Unternehmen Anwendung finden, müssen sie schon aus diesem Grund erheblich vereinfacht und klarer formuliert werden, um den Regulierungsaufwand in Grenzen zu halten. Entwickelt werden müssen präzise und verständliche Regelungen. Hierbei ist vor allem eine Differenzierung zwischen Bereichen, in denen solche bewährte Verfahren bereits existieren und Bereichen, in denen neue Verfahren entwickelt und eingesetzt werden müssen, notwendig.

   - *Verschlankung*: Selbst die Datenschutzexperten klagen über eine kaum noch zu überblickende Normenflut auf dem Gebiet des Datenschutzrechts. Das allgemeine und das bereichsspezifische Datenschutzrecht bedarf daher einer Durchforstung und Überprüfung. So hat in den vergangenen Jahren die Bedeutung des Bundesdatenschutzgesetzes durch immer neue bereichsspezifische Regelungen tendentiell abgenommen.[64] Mit der Umsetzung der EU-Richtlinie ergibt sich die Möglichkeit, durch Aufwertung des BDSG die Menge der bereichsspezifischen Regelungen deutlich zu reduzieren.

8. Das Datenschutzrecht insgesamt sollte – soweit dies möglich ist – auf getrennte Regelungen für öffentliche und private Stellen verzichten. Es sollte ferner, wie von der EU-Richtlinie vorgesehen, den allgemeinen Grundsatz der Datenvermeidung festschreiben, die Verantwortlichkeit für die Einhaltung der Datenschutzregeln, insbesondere für Datenverarbeitung und -übermittlung im Internet klarstellen und die Rechte der Betroffenen und die Pflichten der Verantwortlichen für die Verarbeitung in technikunabhängiger Weise regeln, damit sie auch auf neue technologische Entwicklungen flexibel angewendet werden können. Zudem soll ein neues Datenschutzrecht die Transparenz der Datenverarbeitung durch Stärkung der Pflicht zur Information des Betroffenen über die wesentlichen Merkmale der Verarbeitung von Daten über ihn (insbesondere: Identität des Verantwortlichen, Zwecke der Verarbeitung, Übermittlung der Daten, Rechte des Betroffenen) und der Pflicht zur Vorhaltung allgemeiner Informationen über die vorgenommen Verarbeitungen verbessern. Im Hinblick auf die neuen technologischen Entwicklungen sollte das Datenschutzrecht die Rechte der Betroffenen stärken sowie neue Rechte (allgemeines Widerspruchsrecht aus berechtigten Gründen, Auskunft über den logischen Aufbau der Verarbeitung, Verbot automatischer Entscheidungen) mit rechtlichen Auswirkungen einführen. Schließlich soll gemäß der EU-Richtlinie die Datenschutzkontrolle unter dem Gesichtspunkt der institutionellen und organisatorischen Unabhängigkeit gewährleistet und die Rolle der behördlichen und betrieblichen Datenschutzbeauftragten gestärkt werden.

9. Eine große Bedeutung kommt den Möglichkeiten des Selbstschutzes für den einzelnen Nutzer zu. Dazu bedarf es insbesondere der weiteren Entwicklung von Selbstschutzinstrumenten (z.B. Digitale Signatur, Verschlüsselungssoftware), was zugleich eine Herausforderung an eine zukunftsgerichtete Forschungsförderpolitik ist. Außerdem ist der Aufbau einer Sicherungsinfrastruktur für die Nutzung dieser Selbstschutzmechanismen unabdingbar, wofür die Politik Rahmenbedingungen formulieren muß. Notwendig ist darüber hinaus die Förderung des Bewußtseins um die Möglichkeiten des Selbstdatenschutzes und des Systemdatenschutzes. Dies

kann zum einen durch Maßnahmen zur Aufklärung über die Chancen und Risiken der neuen Informations- und Kommunikationstechniken geschehen, zum anderen aber auch dadurch, daß die öffentliche Verwaltung entsprechende Techniken einsetzt und Ansätze zu „electronic government“ gezielt gefördert werden. Ziel sollte es sein, den Datenschutz zu einem Thema der gesellschaftlichen Debatte zu machen.

10. Die Möglichkeiten der Nutzer zum Selbstschutz durch kryptografische Verfahren darf rechtlich nicht eingeschränkt werden. Eine Einschränkung der freien Verwendung solcher Verfahren kann bei einer Abwägung von Nutzen und Schaden nicht gerechtfertigt werden und wäre verfassungsrechtlich bedenklich. Denn während sie rechtstreue Unternehmen und Bürger bei ihrem Bemühungen, vertraulich zu kommunizieren, erheblich einschränkten, dürfte der Nutzen aufgrund der Umgehungsmöglichkeiten für die staatliche Sicherheit gering sein. Verschlüsselungsprogramme, die eine Entschlüsselung verschlüsselter Inhalte durch Dritte ermöglichen, sollten als solche gekennzeichnet werden müssen.

11. Um die Gebote der Datensparsamkeit und der Datenvermeidung zu erfüllen, sollten die Systeme der Diensteanbieter nach dem Prinzip des Systemdatenschutzes organisiert werden. Die informationsverarbeitenden Systeme sollten so konstruiert werden, daß sie möglichst wenig personenbezogene Daten verarbeiten müssen (und können), um ihre jeweilige Aufgabe zu erfüllen. So könnten beispielsweise Netzbetreiber, Inhalteanbieter und Inkassostellen so getrennt werden, daß jede Stelle nur den jeweils notwendigen Teil der personenbezogenen Informationen zur Verfügung hat.[65]

12. Grundlegende Bedeutung kommt der pseudonymen Nutzungsmöglichkeit der neuen Dienste als Mittel des Selbstdatenschutzes zu, die gefördert werden sollte. Mit einer pseudonymen Nutzungsmöglichkeit werden die personenbezogenen Daten zwar nicht reduziert, jedoch wird damit die Zurückverfolgung der gespeicherten und verarbeiteten Daten zu einer tatsächlichen Person wirksam verhindert – außer im Streitfall. Dies ist der

wirksamste Weg, um Mißbräuchen mit personenbezogenen Daten vorzubeugen, die in den Datennetzen anfallen.[66] Allerdings setzt dieses Instrument eine Infrastruktur zur Ausgabe, Verwaltung und Aufdeckung von Pseudonymen voraus, die nach Prinzipien des Systemschutzes organisiert sein sollte.

13. Nach jahrelangen Ankündigungen müssen endlich – unter Einbeziehung aller Beteiligten – Regelungen zum Arbeitnehmerdatenschutz ausgehandelt und formuliert werden. Bei der Entwicklung zu computergestützter Arbeit im Betrieb und im Rahmen von Telearbeit wachsen die Leistungs- und Verhaltensdaten über Arbeitnehmer und Arbeitnehmerinnen in Umfang und Qualität stark an, ohne daß sie in angemessener Weise geschützt sind und einer angemessenen Kontrolle unterliegen. Lediglich die Ausweitung des Fernmeldegeheimnisses auch auf innerbetriebliche Kommunikation hat in den letzten Jahren zu einem Zuwachs an Schutz geführt. Die SPD-Bundestagsfraktion muß dafür eintreten, den Schutz bei der Erhebung und Verarbeitung von Arbeitnehmer-Daten weiterzuentwickeln, wobei dem informationellen Selbstbestimmungsrecht auch im Betrieb Geltung zu verschaffen ist. Gerade in diesem Bereich sind neue Erhebungs- und Verarbeitungsformen wie etwa digitale Videoüberwachung oder intelligente Haussysteme einzubeziehen. Dies muß nicht ausschließlich gesetzlich geregelt sein, sondern könnte auch hier teils gesetzlich, teils durch neue, andere Regelungen konzipiert werden.

14. Erforderlich ist eine Überarbeitung der Technischen Maßnahmen nach der Anlage zu § 9 BDSG, die zehn Regeln zum technischen und organisatorischen Schutz personenbezogener Daten aufstellt. In einem ersten Schritt ist dieser Katalog dahingehend zu überprüfen, ob er den Anforderungen moderner vernetzter Systeme noch genügt. In einem zweiten Schritt ist seine Kompatibilität mit international anerkannten Sicherheitsmaßnahmen zu überprüfen. Gegebenenfalls muß der Maßnahmenkatalog nach der Anlage zu § 9 BDSG grundlegend überarbeitet und auch erweitert werden, um seine praktische Anwendung durchzusetzen und internationale Akzeptanz zu

erreichen. Schließlich sind Modelle exemplarischer Sicherheitsanforderungen zu entwickeln, um ihre praktische Durchsetzung zu erleichtern.

15. Ein moderner Datenschutz muß der gestiegenen Bedeutung des Outsourcing im öffentlichen wie im nicht-öffentlichen Bereich für eine wirtschaftliche und effiziente Aufgabenerfüllung Rechnung tragen. Der Datenschutz soll der Optimierung von Arbeitsabläufen nicht entgegenstehen; er darf aber auch nicht seinerseits durch Outsourcing vermindert oder ausgehebelt werden. Um dies zu erreichen, ist vor allem sicherzustellen, daß der durch Berufs- oder besondere Amtsgeheimnisse garantierte gesteigerte Schutz auch im Falle des Outsourcing erhalten bleibt.

16. Die in der EU-Datenschutzrichtlinie enthaltene Verpflichtung, im nationalen Datenschutzrecht ergänzende Möglichkeiten der Selbstregulierung vorzusehen, sollte nicht als unvereinbare „Systemwidrigkeit“, sondern als Chance begriffen werden, dieses Instrument für den Schutz des Rechts auf informationelle Selbstbestimmung fruchtbar zu machen. Entsprechende Regelungen sollten sich an den Erfahrungen von Staaten orientieren, die bereits Erfahrungen mit Selbstregulierung im Bereich des Datenschutzes gesammelt haben. So können auch mögliche Schwächen im Hinblick auf Repräsentativität und Umsetzung in den jeweiligen Branchen, die diese „codes of conduct“ haben, erkannt und vermieden werden. Selbstregulierungsmechanismen setzen jedoch gesetzliche Rahmenbedingungen voraus, für den Fall, daß diese versagen – die Betroffenen dürfen in einem solchen Fall nicht schutzlos sein.

17. Ein wesentliches Element eines modernen Datenschutzrechtes stellt die Möglichkeit einer freiwilligen Auditierung dar und sollte auch im Datenschutzrecht vorgesehen werden. Eine solche Auditierung trägt dazu bei, die Ergebnisse der Selbstregulierung transparent zu machen. Zugleich könnte sie die Wahrnehmung des Datenschutzes als Qualitäts- und Wettbewerbsfaktor stärken und damit deutlich machen, daß Datenschutz nicht nur als Kostenfaktor für Unternehmen anzusehen ist, sondern vor allem einen – wenn auch nicht kurz- so aber doch längerfristig – entscheidenden Wettbewerbs- und

Standortvorteil darstellen kann. Eine solche Zertifizierung, mit der die Unternehmen werben könnten, hätte nicht nur die unmittelbare Folge, daß aus Perspektive des Datenschutzes unbedenkliche Produkte auf den Markt kommen, sondern könnte ebenfalls das Bewußtsein um die Bedeutung des Datenschutzes in der Informationsgesellschaft erhöhen. Aufgabe der Politik ist es, gesetzliche Regelung zur Durchführung und Kontrolle eines solchen Auditierungsverfahrens zu entwickeln, mit denen bestimmte Verhaltensregeln und Mindeststandards vorgegeben werden.

18. Die SPD-Bundestagsfraktion ist – wie dies bereits bei der parlamentarischen Beratung des Informations- und Kommunikationsdienste-Gesetzes (IuKDG) deutlich wurde – der Auffassung, daß mit dem Teledienstedatenschutzgesetz (TDDSG) des Bundes und den datenschutzrechtlichen Bestimmungen im Mediendienstestaatsvertrag der Bundesländer ein wichtiger erster Schritt in Richtung eines modernen Datenschutzrechts getan worden ist, das den Anforderungen einer globalen Informationsgesellschaft gerecht werden kann. Als notwendig erweist es sich jedoch, aufmerksam zu beobachten, ob sich die Regelungen im internationalen Vergleich als sachgerecht, den Bürgerrechten dienlich, wettbewerbsfördernd oder als zu restriktiv erweisen. Gleichzeitig sollte überprüft werden, wie sich Abgrenzungsprobleme und die inhaltliche Feinabstimmung zwischen den beiden Regelungswerken und zum Telekommunikationsgesetz auswirken und ob hier gegebenenfalls Anpassungsbedarf besteht.[67] Darüber hinaus muß umgehend Teil 11 des Telekommunikationsgesetzes (TKG) an die neuen datenschutzrechtlichen Instrumente des Teledienstedatenschutzgesetzes (TDDSG) angeglichen werden.

19. Die Gesetzgeber in Bund und Ländern haben in § 3 Abs. 4 Teledienstedatenschutzgesetz und § 12 Abs. 5 Mediendienstestaatsvertrag einen ersten und richtungsweisenden Ansatz formuliert, das Datenschutzrecht um technikrechtliche Elemente der datenminimierenden Gestaltung und Auswahl von Einrichtungen der Informations- und Kommunikationstechnik zu

ergänzen. Diese Steuerungselemente sind zu verallgemeinern und um die Anforderungen zu ergänzen, die im Zusammenhang mit organisatorischen, technischen und rechtlichen Vorkehrungen zur Erhöhung der Datensicherheit (IT-Sicherheit) in der Informations- und Kommunikationstechnik entwickelt worden sind.

20. Prinzipien des Datenschutzes sollten nach Möglichkeit integraler Bestandteil von Dienstleistungen und Produkten auf dem Gebiet der Informations- und Kommunikationstechnik werden. Entsprechende Forschungs- und Entwicklungsarbeiten, beispielsweise die Entwicklung datenschutzfreundlicher Software, sollten verstärkt gefördert und unterstützt werden. Dies gilt auch für die Bemühungen um eine internationale Standardisierung von technischen Datenschutzfunktionen.

21. Bei der Schaffung neuer datenschutzrechtlicher Regelungen ist die Dynamik des Veränderungsprozesses der Informations- und Kommunikationstechnik zu berücksichtigen. Regelungen des Datenschutzes sollten daher ebenso wie andere IuK-bezogene Normen in regelmäßig Abständen evaluiert werden. Mit den Entschließungsanträgen zum Informations- und Kommunikationsdienstegesetz (IuKDG) wurde in der 13. Legislaturperiode in Bezug auf dieses Gesetz ein entsprechender Auftrag an die Bundesregierung erteilt. Ebenso sollte auch bei der anstehenden Novellierung des Bundesdatenschutzgesetzes vorgegangen werden.

22. Die in den letzten Jahren eingeführten Regelungen, die eine Erweiterung der Eingriffsbefugnisse der Sicherheitsbehörden zum Ziel hatten, bedürfen einer baldigen Evaluierung hinsichtlich ihrer Notwendigkeit und Wirksamkeit.[68] Dies kommt auch im SPD-Regierungsprogramm zum Ausdruck: "Bestehende Gesetze und Verordnungen sind auf ihre Notwendigkeit zu überprüfen."[69]

23. Da nationales Recht zunehmend an seine Grenzen stößt, bedarf es europäischer und globaler Datenschutzstandards, die es fortlaufend zu entwickeln und zu verbessern gilt. Wenn keine global geltende Datenschutzstandards entwickelt werden, besteht die Gefahr, daß die

Sammlung und Verarbeitung von Daten in Staaten ausgelagert wird, in denen kein oder nur ein schwaches Datenschutzniveau existiert.[70]

24. Die Herausbildung einer globalen Informationsgesellschaft tangiert verschiedene Grundrechte, beispielsweise das Telekommunikationsgeheimnis. Der Schutz des Fernmeldegeheimnisses als Grundvoraussetzung des Schutzes in Netzen ist auszubauen. Dabei ist besonders dem Umstand Rechnung zu tragen, daß Eingriffsmöglichkeiten in das Telekommunikationsgeheimnis durch "berechtigte" Stellen auch mißbräuchliche Eingriffe durch unberechtigte Dritte mit fatalen Folgen bis hin zu Wirtschaftskriminalität und Datenterrorismus haben können.

25. Der Schutz gegenüber Medienunternehmen ist zu verbessern. Der besondere Rang der Presse- und Meinungsfreiheit ist dabei zu beachten. Dazu müssen die Rechte des Betroffenen entsprechend angepaßt werden. Einer nahezu vollständigen Freistellung von den materiellen Schutzvorschriften, wie im geltenden Recht enthalten, bedarf es nicht.

26. Die berechtigten Interessen der unabhängigen Forschung und das Recht auf informationelle Selbstbestimmung sind durch angemessene Regelungen zu einem Ausgleich zu bringen. Besonderes Gewicht gewinnen hierbei verfahrensrechtliche Vorkehrungen, die die Zweckbindung und die Vertraulichkeit dieser Daten sicherstellen und auf diese Weise auch die Akzeptanz der Forschung mit personenbezogenen Daten erhöhen können. Zentrale Bedeutung in diesem Zusammenhang hat die Einführung eines Forschungsdatengeheimnisses einschließlich einem Zeugnisverweigerungsrechts für Forscher, das die von Forschern erhobenen und verknüpften personenbezogenen Daten vor dem Zugriff der Sicherheitsbehörden sicherstellt.

27. Notwendig ist auch im Bereich des Datenschutzes eine Intensivierung und Förderung einer interdisziplinären Technikfolgenabschätzung, um mögliche Datenschutzrisiken frühzeitig erkennen und Schutzstrategien entwickeln zu können. Notwendig ist eine interdisziplinäre Technikfolgenabschätzung auch

deshalb, weil über die Risikoeinschätzung der Bevölkerung im Hinblick auf den Datenschutz noch immer ein erhebliches Wissensdefizit herrscht.

28. Von der gegenwärtigen politischen Diskussion um die Novellierung des Datenschutzrechts noch gänzlich abgekoppelt ist die Frage nach dem Informationszugang. Wie das Recht auf informationelle Selbstbestimmung ist der Zugang zu Informationen eine zentrale Voraussetzung einer entwickelten Informationsgesellschaft.[71] Der Schutz des Grundrechts auf informationelle Selbstbestimmung dient nicht nur der Eingriffsabwehr im Sinne einer grundsätzlich eigenen Verfügungsbefugnis über die individualisierten Daten oder wenigstens dem Wissen über deren Verwendung durch staatliche Stellen, sondern ebenso dem Ziel, die Kommunikations- und Handlungsfähigkeit der einzelnen Menschen innerhalb der Gesellschaft wie auch gegenüber staatlichen Stellen sicherzustellen.[72] Mit einem Informationsfreiheitsgesetz unter Berücksichtigung des Datenschutzes - wie dies auch im Koalitionsvertrag vereinbart wurde[73] - sollen die Informationszugangsrechte der Bürgerinnen und Bürger gewährleistet werden. Zu prüfen ist, ob eine gesetzliche Regelung den Datenschutzbeauftragten auch die Funktion von Beauftragten für den Informationszugang zuweisen sollte, wie dies im Land Brandenburg bereits der Fall ist.