Jörg Tauss[1]

Modernisierung des Datenschutzrechtes – eine Art Zwischenbilanz

Wer immer sich in den vergangenen Jahren mit der Modernisierung des Datenschutzes beschäftigte, wird bald auf die Beiträge des ehemaligen Landesdatenschutzbeauftragten der Hansestadt Bremen und heutigen Konzerndatenschutzbeauftragten der DaimlerChrysler AG, Professor Alfred Büllesbach, gestoßen sein. Doch nicht die aktuelle Debatte um die Modernisierung des Datenschutzrechtes hat Alfred Büllesbach entscheidend mitgeprägt, vielmehr sind seine Beiträge bereits seit vielen Jahren für die nicht immer einfachen Datenschutzdebatten unverzichtbar. Als Beleg mag der von der SPD-Fraktion am 13. 12. 1988 eingebrachte Gesetzentwurf eines »Bundes-Informationsschutzgesetzes« dienen (BT-Drs. 11/3730), an dessen Formulierung Alfred Büllesbach maßgeblich beteiligt war.[2]

In der Person Alfred Büllesbach kommen zwei Besonderheiten zum Ausdruck: Zum einen gelingt es ihm auf hervorragende Art und Weise, die Perspektive der Wissenschaft und Wirtschaft zu bündeln. Auf der anderen Seite ist er aufgrund seines beruflichen Werdeganges wie kaum ein anderer in der Lage, die Fragen des Datenschutzes sowohl für den öffentlichen als auch für den nichtöffentlichen Bereich einschätzen und bewerten zu können. So ist es auch kein Zufall sondern ein Glücksfall, dass er sowohl im Arbeitskreis »Datenschutz« der SPD-Bundestagsfraktion, der bei der Erstellung des Eckwerte-Papiers »Modernes Datenschutzrecht für die (globale) Wissens- und Informationsgesellschaft«[3] im Jahr 1998 einen erheblichen Anteil hatte, als auch im Begleitausschuss »Modernisierung des Datenschutzrechtes«, der die Koalitionsfraktionen bei der Erarbeitung und Beratung des Gutachtens »Modernisierung des Datenschutzrechtes«[4] beraten hat und bei der Umsetzung dieses Reformvorhabens unterstützen soll, maßgeblich beteiligt war.[5]

Rückblickend wird – aus der Perspektive der um wissenschaftliche Beratung ersuchenden Politik – vor allem eines deutlich: Wissenschaftliche Politikberatung bedeutet in erster Linie Position beziehen. Um ein konkretes Beispiel zu nennen: Noch während der parlamentarischen Beratung des Informations- und Kommunikationsdienstegesetzes (IuKDG), mit dem seitens des Bundesgesetzgebers erste vorsichtige Schritte zu einer Modernisierung des Datenschutzrechtes im Bereich der Neuen Medien versucht werden sollten, und inmitten der aufgeheizten Kryptodebatte hat Alfred Büllesbach 1997 im Auftrag der Friedrich-Ebert-Stiftung ein Gutachten unter dem Titel »Datenschutz bei Informations- und Kommunikationsdiensten« vorgelegt (Büllesbach 1997). Die Kernaussagen dieses Gutachtens haben noch immer Bestand und lauten kurzgefasst: Die Fortentwicklung der Informationsgesellschaft verlangt, Datenschutz und IT-Sicherheit als zentrale Akzeptanzvoraussetzung zu begreifen. Der bestehende Rechtsrahmen eignet sich angesichts der immensen Herausforderungen nur noch bedingt zur Verwirklichung eines angemessenen Datenschutzes. Dies sei vor allem auf die zergliederten be-

reichsspezifischen Regelungen (einschließlich der zu diesem Zeitpunkt auf der Agenda stehenden neuen Gesetze) zurückzuführen, die für Datenschutz und IT-Sicherheit eine überschneidende Überregulierung und eine strukturelle Unübersichtlichkeit für Nutzer, Verbraucher und Normadressaten schaffen. Notwendig sind darüber hinaus neue Instrumente wie Selbstschutz und Systemschutz. Diese wiederum setzen die freie und uneingeschränkte Verfügbarkeit kryptographischer Verfahren voraus (vgl. hierzu Huhn/Pfitzmann 1998).

Gerade die Debatte um die immer wieder geforderte Einschränkung kryptographischer Verfahren hat überdeutlich gezeigt, wie wichtig es ist, Position zu beziehen – zumal wenn es darum geht, die aus den unterschiedlichen Perspektiven jeweils durchaus berechtigten Interessen sorgsam gegeneinander abzuwägen. In seinem Gutachten für die Friedrich-Ebert-Stiftung hat Alfred Büllesbach eine – sowohl aus der Perspektive der Wissenschaft als auch aus der Perspektive der Wirtschaft – eindeutige Position mit der Feststellung bezogen, dass »eine Regulierung des Einsatzes kryptographischer Verfahren zum Zwecke des Abhörens durch Ermittlungs- und Sicherheitsbehörden unverhältnismäßig« wäre und dass die »deutsche Wirtschaft den freien Zugang zu kryptographischen Verfahren, denen sie vertrauen kann«, braucht (Büllesbach 1997: 8). Ohne derartige richtungsweisende Stellungnahmen seitens der Wissenschaft und seitens der Wirtschaft wäre die Politik kaum in der Lage gewesen, eine sachgerechte und angemessene Abwägung bei der Bewertung der Kryptofreiheit vorzunehmen und durchzusetzen.

Vor dem Hintergrund dieses Engagements ist der Anlass dieser Freundesgabe für Alfred Büllesbach Grund genug, auf die umfassenden Herausforderungen der Modernisierung des Datenschutzrechts näher einzugehen (1.). Die SPD-geführte Bundesregierung und die Koalitionsfraktionen haben sich darauf verständigt, das gesamte Datenschutzrecht in einem zweistufigen Verfahren umfassend zu modernisieren. In einem ersten Schritt wurde mit einer ersten Novellierung des Bundesdatenschutzgesetzes (BDSG) die längst überfällige Umsetzung der EG-Datenschutzrichtlinie in deutsches Recht erreicht. In einem zweiten Schritt sollte das gesamte Datenschutzrecht einschließlich der bereichsspezifischen Regelungen auf den Prüfstand gestellt werden. Aufgezeigt werden sollen hier der Stand der politischen Diskussion am Ende der 14. Legislaturperiode des Deutschen Bundestages (2.). Hierbei sind natürlich auch die furchtbaren Ereignisse des 11. September 2001 in New York und Washington zu thematisieren, die zwangsläufig nicht nur die Prioritätenliste politischer Aktivitäten grundlegend verschoben haben, sondern vielmehr auch die politische Debatte insgesamt und vor allem die sicherheitspolitische Diskussion verändert haben. Schließlich sollen die zentralen Eckpunkte für die Umsetzung der zweiten Stufe der Modernisierung des Datenschutzrechtes benannt werden, die sich in vielen Punkten auf das vom Bundesministerium des Innern in Auftrag gegebenen Gutachten berufen können (3.).

1. Herausforderungen an das Datenschutzrecht

Die Herausbildung einer globalen Informations- und Wissensgesellschaft stellt für die Verwirklichung des Rechtes auf informationelle und kommunikative Selbstbestimmung eine doppelte Herausforderung dar. Zum ersten geraten Fragen der Datensicherheit und des Datenschutzes um so stärker in den Blick, je tiefer sämtliche Lebensbereiche durch die neuen Informations- und Kommunikationstechnologien durchdrungen und in zunehmendem Maße sensible Daten und vertrauliche Inhalte aus allen Bereichen in IuK-Netzwerke eingespeist und übermittelt werden. Mit der Bedeutung elektronischer Informations- und Kommunikationsinfrastrukturen für die individuelle Lebens- und Berufswelt, aber auch für gesellschaftliche und wirtschaftliche Organisationen und deren Kommunikation wächst zugleich das Bewusstsein um die neuen Gefahren, die mit den spezifischen Merkmalen elektronischer Datenverarbeitung in globalen Netzwerken einher gehen. Unaufhörlich entstehen bei der komplexen digitalen Signalübermittlung und -verarbeitung Datenspuren, deren Verknüpfung ebenso vielfältige wie neuartige Möglichkeiten der unbefugten Kenntnisnahme, Überwachung und Verarbeitung personenbezogener Daten eröffnen, genannt seien hier lediglich Profilbildung oder Data-Mining. Das zunehmende Aufkommen personenbezogener Daten, die Dezentralisierung der Datenerhebung und die Dezentralisierung der Datenverarbeitung in komplexen Netzwerken macht allein die Feststellung sämtlicher potentiell sensibler Verarbeitungsprozesse unmöglich, von einer wirkungsvollen Aufsicht oder Kontrolle ganz zu schweigen (vgl. Enquete-Kommission 1998 und DuD 5/2000).

Aufgrund der digitalen Universalsprache ist die Integrität und Authentizität der elektronischen Kommunikation nicht ohne aufwendige Maßnahmen sicherzustellen, da sie die nicht nachvollziehbare Manipulation von Informationen und vertraulichen Inhalten ermöglicht. Zudem entstehen hinsichtlich der physikalischen Integrität der Daten und der rein technischen Verfügbarkeit von Infrastrukturen aufgrund der Komplexität der Technologie und der integrierten Netzwerke neue Risiken, die zunehmend an Bedeutung gewinnen (Stichwort »Kritische Infrastrukturen«). Nicht nur, dass der Schutz der Privatsphäre und die Vertraulichkeit und Integrität sämtlicher Kommunikation zunehmend an Bedeutung gewinnt, darüber hinaus wird Datensicherheit zu einem integralen Baustein in einem ganzheitlichen, auf mehrseitige Sicherheit basierenden Datenschutzkonzept (Müller/Pfitzmann 1997: 11f.; Ulrich 1999: 14)[6].

Zum zweiten setzt die im wörtlichen Sinne globale Dimension der IuK-Netzwerke nationalen oder regionalen Regelungen enge Grenzen. Insbesondere die Reichweite des klassischen Ansatzes eines normenorientierten Datenschutzes, dessen Rechtsgeltung öffentlich kontrolliert und gewährleistet wird, endet im Gegensatz zu den Datenströmen spätestens an den jeweiligen Landesgrenzen. Die mit der Umsetzung der Datenschutzrichtlinie erfolgte Harmonisierung des europäischen Datenschutzrechtes, mit der weit über die bisherigen Regelungen hinaus ein einheitlicher Rechtsrahmen sichergestellt

werden soll, vermag diesen Missstand lediglich zu lindern, beseitigen kann sie ihn nicht (vgl. Simitis 1998: 183 f.; DuD 8/2000). Denn in globalen Zusammenhängen sind selbst regional einheitliche Regelungen letztlich partikulare Regime-Inseln, deren begrenzte Ausdehnung zugleich mit der Reichweite einer legitimierten – dennoch mehr oder weniger effektiven – Rechtsdurchsetzung zusammenfällt. Internationale oder gar globale Vereinbarungen und Verträge sind jedoch aufgrund der divergierenden Datenschutztraditionen und Rechtsphilosophien nur schwer zu erzielen, wie nicht zuletzt die Verhandlungen zu den »Safe-Harbour-Principles« zwischen den USA und der EU zeigten.[7] Zudem bleibt zumindest zu fragen, ob multilaterale Abkommen ein akzeptables Schutzniveau zu erzielen vermögen und flexibel an die Dynamik der technischen Entwicklung anzupassen sind. Dies gilt um so mehr in Anbetracht der notgedrungen vorherrschenden Praxis, in derartigen Verhandlungen lediglich den »kleinsten gemeinsamen Nenner« bestimmen und festschreiben zu können.

Diese Situation verändert die Rahmenbedingungen für einen angemessenen und effektiven Datenschutz – die Rede ist von einem Neuen Datenschutz oder von Datenschutzgesetzen der dritten Generation (vgl. Bäumler 1998 und Bäumler/v. Mutius 1999, Tauss/Özdemir 2000). Zum klassischen Schutz der individuellen Privatsphäre im Sinne der Verwirklichung der informationellen Selbstbestimmung treten untrennbar sowohl die notwendige Berücksichtigung der kommunikativen Autonomie aller an der elektronischen Kommunikation Beteiligten als auch die notwendige Gewährleistung einer hinreichenden technischen Datensicherheit als Grundvoraussetzung hinzu, als conditio sine qua non (Tauss/Özdemir 2000: 143; Ulrich 1999: 14; DuD 5/2000, Bizer 1999: 45).

Nicht nur die nachhaltige Zweckbindung für die Erhebung und Verarbeitung personenbezogener Daten und die Vertraulichkeit individueller Kommunikation gilt es sicherzustellen, auch die sichere und vertrauliche Kommunikation von Unternehmen, Organisationen und Verwaltungsbehörden sowie die Sicherheit ihrer sensiblen gespeicherten Daten sind in einem ganzheitlichen Datenschutzkonzept zu berücksichtigen. Die erfolgreiche Erfüllung aller Aufgaben hängt dabei zunehmend von der Realisierung der vier wichtigsten informationstechnischen Schutzziele Vertraulichkeit, Integrität, Verfügbarkeit und Zurechenbarkeit ab, d.h. der technologisch auszuschließenden unbefugten Kenntnisnahme Dritter sowie unbefugter Veränderung der Daten, der bedarfsnahen Zugänglichkeit relevanter Informationen und der im – autorisierten – Bedarfsfall möglichen Identifikation der kommunizierenden Nutzer (vgl. Rannenberg/Pfitzmann/Müller 1997: 22 f.).[8] Gerade die erfolgreiche Bearbeitung dieser komplexen Aufgabenstellung wird durch die vereinfachte, dezentrale und globale Vernetzung der Datenverarbeitungsprozesse strukturell erschwert.

Zeitgleich lokalisieren zahlreiche Studien und Prognosen mit dem notwendigen Vertrauen und mit der hinreichenden Akzeptanz bei den potentiellen Nutzern die entscheidenden kritischen Variablen für die künftige gesellschaft-

liche Bedeutung der neuen IuK-Möglichkeiten, gerade in den Bereichen E-Government, E-Democracy oder auch E-Commerce (vgl. Booz Allen Hamilton 2000). Die gesellschaftspolitisch prekäre digitale Spaltung der Gesellschaft in Nutzer und Nichtnutzer und die spürbare Zurückhaltung der Nutzer, auch komplexe und hochsensible Transaktionen im Netz durchzuführen, ist (auch) eine Folge des Misstrauens in die Sicherheit und Vertraulichkeit der neuen IuK-Möglichkeiten. Erst wenn die Bürgerinnen und Bürger, die Unternehmen und auch die Verwaltungsbehörden davon überzeugt sind, dass ihre sensiblen Daten und ihre vertrauliche Kommunikation zuverlässig, unverändert und innerhalb ihrer Kontrollparameter übermittelt oder verarbeitet werden, erst dann werden sich die fraglos bestehenden Informations-, Transparenz-, Rationalisierungs- und Interaktionspotentiale der neuen IuK-Möglichkeiten realisieren lassen.

Der Staat ist daher aus seiner allgemeinen Schutz- und Gewährleistungsverpflichtung keineswegs zu entlassen. Vielmehr ist – analog zu anderen Politikfeldern – auch auf dem zunehmend akuten Gebiet des Datenschutzes von der partikularen und ineffektiven Detailregulierung mit großer Tiefe umzustellen auf die Schaffung variabler Rahmenbedingungen für einen effektiven Selbstschutz der individuellen Nutzer und einen marktregulierten Wettbewerb um das höchste systemische und/oder technische Datenschutzniveau. Gemeinsam mit der international harmonisierten Normierung von Datenschutzzielen bilden diese Aspekte eines »Neuen Datenschutzes« (vgl. Tauss/Özdemir 2000: 143 f.; DuD 5/2000) komplementäre Antwortstrategien auf die zwei Herausforderungen der neuen Rahmenbedingungen, der Dezentralisierung und Verknüpfung der Erhebung, der Speicherung, der Übermittlung sowie der Verarbeitung sensibler Daten und der länderübergreifenden, sprich globalen Dimension der Netzwerke. Der individuelle Selbstdatenschutz, der Systemdatenschutz und der technisch implementierte Datenschutz bedingen sich gegenseitig und ergänzen das bestehende normative Instrumentarium auf Selbstregulierung abhebender Mechanismen.[9] Sie besitzen dabei unserer Meinung nach das größte Potential, einen nachhaltigen und effektiven Datenschutz mit einer hinreichenden Datensicherheit zu verbinden.

2. Modernisierung des Datenschutzrechtes – eine Zwischenbilanz

Die SPD-geführte Bundesregierung und die Koalitionsfraktionen haben die immensen Herausforderungen, mit denen sich das Datenschutzrecht in der Wissens- und Informationsgesellschaft konfrontiert sieht, erkannt. Sie sind angetreten mit dem Ziel, die demokratischen Beteiligungsrechte der Bürgerinnen und Bürger zu stärken. In der Koalitionsvereinbarung heißt es: »Effektiver Datenschutz im öffentlichen und im privaten Bereich gehört zu den unverzichtbaren Voraussetzungen für eine demokratische und verantwortbare Informationsgesellschaft. Die notwendige Anpassung des deutschen Datenschutzrechts an die Richtlinie der Europäischen Union soll kurzfristig umge-

setzt werden. Durch ein Informationsfreiheitsgesetz wollen wir unter Berücksichtigung des Datenschutzes den Bürgerinnen und Bürgern Informationszugangsrechte verschaffen.«[10]

In einem ersten Schritt hat die SPD-geführte Bundesregierung unmittelbar nach ihrem Amtsantritt in einem gemeinsamen Moratorium des Bundesinnenministeriums und des Bundeswirtschaftsministeriums die jahrelange Debatte um eine Regulierung kryptographischer Verfahren beendet und angesichts der Bedeutung dieses wichtigen Selbstschutzinstrumentes auf eine gesetzliche Regelung verzichtet (Statt dessen hat das Bundeswirtschafts-ministerium die Verfügbarkeit und Weiterentwicklung kryptographischer Verfahren – quasi als staatliche Dienstleistung – maßgeblich gefördert und forciert).

Bundesregierung und Koalitionsfraktionen haben sich auf eine umfassende Modernisierung des Datenschutzrechtes in einem zweistufigen Verfahren verständigt. In einem ersten Schritt wurden in dieser Legislaturperiode die Vorgaben der EG-Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr in deutsches Recht umgesetzt. Durch die Umsetzung der EG-Datenschutz-Richtlinie wird europaweit ein einheitliches Datenschutzniveau geschaffen und werden einheitliche Maßstäbe für die Erhebung und Verarbeitung von Daten in der Europäischen Union festgelegt. Die zentralen Ziele der EG-Datenschutzrichtlinie lauten zusammengefasst: Transparenz der Datenverarbeitung und Akzeptanz der Verbraucher und Nutzer. Mit dieser ersten Novellierung des Bundesdatenschutzgesetzes (BDSG) wurden zugleich erste Bausteine der Modernisierung des Datenschutzrechtes aufgenommen, beispielsweise die Prinzipien der Datenvermeidung und der Datensparsamkeit und das Datenschutzaudit. In einem zweiten Schritt sollte nun – unmittelbar an die Umsetzung der EG-Datenschutzrichtlinie anschließend – das gesamte Datenschutzrecht mit dem Ziel einer umfassenden Modernisierung auf den Prüfstand gestellt werden. Hierzu hat das Bundesministerium des Innern ein Gutachten in Auftrag gegeben, welches den Reformbedarf und die Reichweite aufzeigen und Grundlinien zur »Modernisierung des Datenschutzrechtes« erarbeiten sollte. Im Herbst 2001 wurde dieses Gutachten der Öffentlichkeit vorgestellt (Rossnagel/Pfitzmann/Garstka 2001).

Die schrecklichen Ereignisse des 11. September 2001 in New York und Washington haben nicht nur die politische Agenda grundlegend verschoben, sondern auch die (sicherheits-)politische Debatte insgesamt: Galt angesichts der eingangs beschriebenen Herausforderungen in globalen Kommunikationsnetzen bis dahin die Feststellung, dass an die Stelle staatlicher Regulierung zunehmend die Anleitung und Hilfe zur Selbsthilfe der Nutzer treten müsse und dass das Kontrollmoment des Staates – im Sinne des Cybercontrol – hinter den Schutzmoment der Nutzer und der sensiblen Infrastrukturen – im Sinne der Cyberprotection – zurücktreten müssen, so hat der 11. September 2001 diese ungeschriebenen Regeln einer effektiven Netz- und Datenschutzpolitik grundlegend verändert. Bereits früh wurde von

Netzaktivisten vorhergesagt, dass eine massive Abkehr von diesen gewonnenen Überzeugungen und eine Umkehr des Verhältnisses von Cybercontrol und Cyberprotection bevorsteht. Die Entwicklung in fast allen westlichen Staaten hat diese Befürchtungen mittlerweile mehr als bestätigt. Der spezifische Kontext internationaler paketvermittelter Kommunikation ist in Gefahr, aus dem Blick zu geraten und unter dem wiedererstarkten Primat eines klassisch interpretierten (nationalen) Sicherheitsverständnisses zu verschwinden.

Obwohl sich die beschriebenen Rahmenbedingungen nicht wesentlich geändert haben, folgen die gegenwärtigen sicherheitspolitischen Maßnahmen infolge des Terroranschlages vor allem wieder dem Regelungsmodus »law and order« – wenn auch mit gewissen Einschränkungen. Rechtsdurchsetzungs- und Strafermittlungsprobleme ergeben sich nun aus Sicht der Sicherheitsbehören wieder eher aus Rechtslücken sowie überzogenen datenschutzrechtlichen Bedenken, einem gefährlichen Laisser-faire und mangelnder finanzieller, technischer wie personeller Ausstattung der Behörden, als aus der technologischen Dynamik und globalen Vernetzung der neuen IuK-Möglichkeiten. Die Ambivalenzen und mit ihnen die Warnungen vor einer Überregulierung oder einer überzogenen Kontrolle der Bürger erscheinen – vorerst – nachrangig. Der Staat, so die Argumentation weiter, sei in seiner ureigensten Aufgabe als Garant der öffentlichen Sicherheit herausgefordert und müsse regieren. Das »Wer, Was und Wie« der Sicherheitsfrage lässt sich wieder eindeutig beantworten: Allein der Staat sorgt für eine umfassende Sicherheit für alle, bei der die Ermittlungs- und Rechtsdurchsetzungsperspektive im Vordergrund steht und durchgreifende Regulierung als einziges Mittel erscheint. Die wichtige Wechselbeziehung von Cybercontrol auf der einen und Cyberprotection auf der anderen Seite gerät aus dem Blick. Es setzt sich in der politischen Debatte wieder zunehmend die Überzeugung durch, dass beide Aspekte unvereinbar sind und dass der Kontrolle der Vorzug vor dem Schutz gegeben werden muss.

Das gemeinsame Ziel einer in diesem Sinne erhöhten Sicherheit wird derzeit zur Legitimation für zahlreiche Maßnahmen zur Erweiterung der Überwachungs- und Kontrollmöglichkeiten herangezogen, wofür die Debatten um die Telekommunikations-Überwachungsverordnung oder den Einsatz des sogenannten IMSI-Catchers beispielhaft angeführt werden können. Aber nur in Ausnahmefällen stehen Wirksamkeit, Angemessenheit und auch Nebeneffekte dieser Aktivitäten auf der Tagesordnung.

Immerhin sollte, und dies ist ein positiver Aspekt, darauf hingewiesen werden, dass auch dass sogenannte Sicherheitspaket II nicht die jüngsten Entwicklungen in der Form der Gesetzgebung vollständig zurückdrehen konnte: Mit der auf Initiative der Koalitionsfraktionen erfolgten grundsätzlichen Befristung der Maßnahmen und der Kopplung einer eventuellen Verlängerung an eine positive Evaluierung sind zwei zentrale Momente der neuen Formen moderner Gesetzgebung auch unter den derzeitigen schwierigen Rahmenbedingungen realisiert worden.

Natürlich gehört zu einer modernen Gesetzgebung mehr als Befristung und

Evaluierung, und genau hier wird die zweite Stufe zur Modernisierung des Datenschutzrechtes ansetzen. So ist es geradezu eine Voraussetzung für die erfolgreiche Modernisierung des Datenschutzrechtes, dass die wichtige Wechselbeziehung zwischen Cybercontrol und Cyberprotection wieder thematisiert und vor allem die teilweise schwerwiegenden Nebenfolgen einer Verengung der Perspektive auf den Kontrollgedanken wieder in das Blickfeld der politischen Debatte gerückt werden.

3. Umsetzung der zweiten Stufe der Modernisierung des Datenschutzrechtes

Die positiven Erwartungen an das Datenschutzrecht und die Unzulänglichkeit der bisherigen Regelungen sollen mit der Umsetzung der zweiten Stufe ein modernes Datenschutzrecht aufgegriffen bzw. beseitigt werden. Dieses wird nicht nur einfacher und verständlicher sein, sondern darüber hinaus auch hinsichtlich der neuen Formen der Datenverarbeitung risikoadäquat. Um das erste Ziel zu erreichen, müssen die Selbstbestimmung der betroffenen Person gestärkt und die Selbstregulierung und Selbstkontrolle der Datenverarbeiter ermöglicht und verbessert werden. Um das zweite Ziel zu erreichen, müssen vor allem Konzepte des Selbstdatenschutzes und des Systemdatenschutzes umgesetzt werden.

Das nun vorliegende Gutachten markiert wichtige Eckpunkte für die Umsetzung der zweiten Stufe der Modernisierung des Datenschutzrechtes. Kurz gefasst lauten die Kernaussagen des Gutachtens[11] wie folgt:

1. Ein modernes Datenschutzrecht sollte auf einem allgemeinen Gesetz gründen, das bereichsspezifischen Regelungen vorgeht. Dieses sollte grundsätzliche und präzise Regelungen der Verarbeitung personenbezogener Daten und vermeidet möglichst offene Abwägungsklauseln enthalten.
2. Das Gesetz soll darüber hinaus auch allgemeine Regelungen zur Technikgestaltung, zur Datensicherung, zur Datenschutzorganisation, zur Datenschutzkontrolle und zur Selbstregulierung enthalten. Wird die Vorrangregelung im Verhältnis zwischen BDSG und bereichsspezifischen Regelungen umgedreht, können die bisherige Normenflut und Rechtszersplitterung verringert und Widersprüche vermieden werden. Spezialregelungen in bereichsspezifischen Gesetzen sollten nur Ausnahmen von den allgemeinen Regelungen enthalten und nur für bestimmte riskante Datenverarbeitungen die Anforderungen verschärfen oder bei unterdurchschnittlich riskanten Datenverarbeitungen Erleichterungen bieten. Auch könnten Ausnahmen vorgesehen werden, wenn Aufgaben im Allgemeininteresse ansonsten nicht erfüllt werden können.
3. Die allgemeinen Datenschutzgrundsätze sollten gleichermaßen für den öffentlichen und für den nichtöffentlichen Bereich gelten. In beiden Bereichen ist – risiko- und nicht bereichsabhängig – das gleiche Datenschutzniveau zu gewährleisten. Unterschiede sind insoweit zu berück-

sichtigen, als im nichtöffentlichen Bereich die Regelungsadressaten Grundrechtsträger sind und im öffentlichen Bereich Allgemeininteressen verfolgt werden müssen.

4. Wenn das Datenschutzrecht entlastet und die Regelung des Datenverarbeitungsverhältnisses stärker seinen beiden Parteien überlassen werden soll, muss die Transparenz der Datenverarbeitung gegenüber der betroffenen Person erhöht werden. Zielsetzung eines modernen Datenschutzrechts muss es sein, ausreichende Informationen über die Erhebung personenbezogener Daten, über die Umstände und Verfahren ihrer Verarbeitung und die Zwecke ihrer Nutzung für die betroffenen Personen und die Kontrollstellen sicherzustellen. Wer geschäftsmäßig personenbezogene Daten automatisiert verarbeitet, sollte verpflichtet sein, die Struktur der Datenverarbeitung in verständlicher Form zu veröffentlichen, soweit dies ohne Offenlegung von schützenswerten Geheimnissen möglich ist. Mit angemessenem Aufwand muss überdies durchschaubar sein, was das System einschließlich aller Betriebs- und Anwendungssoftware genau tut. Im Interesse konsistenter Regelungen müssen die datenschutzrechtlichen Informationspflichten mit den für Anbieter und Unternehmen geltenden Transparenzregeln beispielweise aus dem Recht des Fernabsatzes harmonisiert werden.
5. Soweit die Datenverarbeitung Interessen der betroffenen Person beeinträchtigen könnte, soll die Entscheidung über diese vorrangig der Selbstbestimmung der betroffenen Person überlassen werden. Im Einzelfall muss die Datenverarbeitung grundsätzlich durch Einwilligung oder Einwilligungssurrogate wie Vertrag und vertragsähnliches Vertrauensverhältnis oder Antrag gegenüber einer Behörde erlaubt werden können. Die Einwilligung ist der genuine Ausdruck des Rechts auf informationelle Selbstbestimmung. Da aber zwischen den betroffenen Personen und den verantwortlichen Stellen in der Regel ein erhebliches Machtgefälle besteht, muss die Selbstbestimmung gestärkt werden. Ziel eines modernen Datenschutzrechts muss es daher sein, einerseits die Zulässigkeit der Datenverarbeitung im vertretbaren Umfang der individuellen Selbstbestimmung zu überlassen, andererseits aber deren Freiwilligkeit durch Rahmenregelungen abzusichern.
6. Grundsätzlich sollte im nichtöffentlichen Bereich eine »Opt-in-Lösung« gewählt werden: Die Datenverarbeitung setzt die vorherige Einwilligung der betroffenen Person voraus. Allerdings muss eine Datenverarbeitung auch ohne Einwilligung der betroffenen Person möglich sein. Zur Umschreibung dieser Ausnahmefälle ist der bisher die Datenverarbeitung steuernde Begriff des »berechtigten Interesses« zu weit. Ausnahmen sollten nur erlaubt sein, wenn dies zum Schutz oder zur Verfolgung eigener Rechte oder Rechte Dritter notwendig ist, oder wenn es erforderlich ist, um eine Gefahr für Leben, Gesundheit oder sonstige bedeutende Rechtsgüter der betroffenen Person zu beseitigen und die betroffene Person ihre Zustimmung nicht geben kann, oder wenn die

Datenverarbeitung erforderlich ist, um Verpflichtungen zu erfüllen, die durch Rechtsvorschriften der verantwortlichen Stelle auferlegt wurden.

7. Im öffentlichen Bereich sollte die Datenverarbeitung zulässig sein, wenn sie »zur Erfüllung einer gesetzlich zugewiesenen und in der Zuständigkeit der öffentlichen Stelle liegenden bestimmten Aufgabe erforderlich« ist. Soweit es allerdings um Verarbeitungszwecke und -formen geht, die gegen den Willen der betroffenen Person durchgesetzt werden müssen und deren Interessen stark beeinträchtigen können, sollen bereichsspezifische Regelungen die Zwecke und Formen risikoadäquat regeln. Die Einwilligung kann im öffentlichen Bereich die Datenverarbeitung im Wesentlichen nur im nicht gesetzlich gebundenen Bereich legitimieren.
8. Insgesamt sind den Prinzipien der Datenvermeidung und Datensparsamkeit eine grundlegende Bedeutung einzuräumen. Soweit für die Zwecke der Datenverarbeitung ein Personenbezug nicht erforderlich ist, muss dieser von Anfang an vermieden oder nachträglich durch Löschung der Daten, ihre Anonymisierung oder Pseudonymisierung beseitigt werden. Darüber hinaus sind die verantwortlichen Stellen zu verpflichten, soweit dies technisch möglich und verhältnismäßig ist, ihre Datenverarbeitungsverfahren so zu gestalten, dass sie möglichst keinen Personenbezug und auch keine Personenbeziehbarkeit aufweisen. Dieses Ziel kann durch Anonymität oder Pseudonymität der betroffenen Person erreicht werden. Anonymität und anonymitätsnahen Arten von Pseudonymen sollte grundsätzlich Vorrang gegeben werden. Die vorgenannten Grundsätze der Transparenz und der Vermeidung des Personenbezugs können nur durch die betroffenen Personen selbst durchgesetzt werden (Selbstdatenschutz). Sie müssen in die Lage versetzt werden, die Nutzung von technischen und organisatorischen Schutzinstrumenten selbst zu bestimmen. Dies sind Instrumente für Inhaltsschutz (Konzelation, Steganographie), Anonymität, Pseudonymität und Identitätsmanagement. Programme, die Schlüssel, Identitäten und Pseudonyme verwalten und den Nutzer bei der Verwendung von Selbstschutztechniken unterstützen, müssen gefördert werden. Eine Bildungsoffensive zum Umgang mit Instrumenten des Selbstdatenschutzes wäre zu erwägen.
9. Darüber hinaus müssen die Grundsätze der Datenverarbeitung organisatorisch sichergestellt werden. Viele bereits bestehende organisatorische Verpflichtungen der verantwortlichen Stellen sollten zu einem integrierten Datenschutzmanagementsystem zusammengefasst und fortentwickelt werden, um Verantwortlichkeit sicherzustellen, das Datenschutzbewusstsein zu stärken und eine datenschutzfreundliche Betriebsorganisation zu erreichen. Die Bestellung eines Datenschutzbeauftragten, die Erarbeitung eines Plans der Datenschutzorganisation und die Erstellung eines Datenschutz- und Datensicherungskonzepts sind die wesentlichen Bestandteile.

10. Zur Stärkung der Akzeptanz des Datenschutzes und um eine ständige Fortentwicklung entsprechend den sich verändernden und zunehmenden Risiken zu ermöglichen, muss ein modernes Datenschutzrecht auch Anreize für einen effektiven und sich fortentwickelnden Schutz bieten. Daher wird den verantwortlichen Stellen die Möglichkeit geboten, mit ihren Anstrengungen zur Implementierung eines effektiven Datenschutzes zu werben. Hierzu gehören insbesondere die vertrauenswürdige Auditierung von Datenschutzmanagementsystemen. Verantwortliche Stellen, die am Datenschutzaudit teilnehmen, sollten von öffentlichen Stellen bevorzugt berücksichtigt werden, wenn es um Aufträge zur Verarbeitung personenbezogener Daten geht.
11. Insgesamt muss der zu entwickelnde neue Datenschutz künftig durch, nicht gegen Technik erreicht werden. Datenschutzrecht muss versuchen, die Entwicklung von Verfahren und die Gestaltung von Hard- und Software am Ziel des Datenschutzes auszurichten und die Diffusion und Nutzung datenschutzgerechter oder -fördernder Technik zu fördern. Datenschutz sollte so weit wie möglich in Produkte, Dienste und Verfahren integriert sein. Adressaten des Datenschutzrechts können daher nicht mehr nur die für die Datenverarbeitung verantwortlichen Stellen sein. Das Datenschutzrecht muss bereits bei der Entwicklung der Technik Einfluss auf deren Gestaltung nehmen. Es muss datenschutzgerechte Technik fordern und fördern. Zu diesem Zweck sollten zumindest drei Regelungen vorgesehen werden. Die Hersteller sollten verpflichtet werden, für die Gestaltung ihrer Produkte zumindest die Erfüllung einiger zentraler Produktanforderungen zu überprüfen. Wer datenschutzgerechte Produkte herstellt, sollte die Möglichkeit erhalten, diese zertifizieren zu lassen und mit dem Zertifikat werben zu können. Schließlich sollten die verantwortlichen Stellen aufgefordert werden, datenschutzgerechte Produkte zu verwenden. Zumindest für öffentliche Stellen sollte dies zu einer gesetzlichen Pflicht erhoben werden.
12. Eine weitaus größere Bedeutung wird für einen Neuen Datenschutz der gesellschaftlichen Selbstregulierung zukommen, beispielsweise durch Konkretisierungen der gesetzlichen Grundsätze durch branchen- oder unternehmensspezifische Selbstverpflichtungen. Um in dieser ein faires Verfahren, einen angemessenen Interessenausgleich, die Berücksichtigung von Gemeinwohlinteressen und eine gewisse demokratische Legitimation zu gewährleisten, muss der Gesetzgeber auch für diese Regelsetzung einen gesetzlichen Rahmen vorgeben, um den Mindeststandard zum Schutz der Betroffenen zu gewährleisten und die Selbstregulierung zu entlasten. Selbstregulierung ermöglicht es der Wirtschaft, relativ schnell passgerechte branchen- oder unternehmensbezogene verbindliche Regelungen zu entwickeln, die die schnelle Entwicklung der Technik, die Komplexität ihrer Systeme und die Vielfalt ihrer Anwendungen berücksichtigen. Der entscheidende Anreiz für Branchen, Verbände oder Unternehmen, eigene, durch Kontrollstellen anerkannte

Verhaltensregeln zu erstellen, besteht in der Möglichkeit, die zu konkretisierenden Gesetzesvorgaben selbstständig und auch für die Kontrollstellen verbindlich auszugestalten.

13. Schließlich müssen mit dem neuen Datenschutzrecht auch die Betroffenenrechte weiter gestärkt werden. Sie bieten eine wesentliche Stütze für einen effektiven Datenschutz nur, wenn sie von den Betroffenen auch tatsächlich wahrgenommen werden und wahrgenommen werden können. Die betroffenen Personen müssen ihre Rechte frei und unbehindert sowie unentgeltlich ausüben können, ohne Zwang, dies zu tun oder nicht zu tun. Betroffenenrechte sollten wenn möglich nur im allgemeinen Datenschutzgesetz geregelt und möglichst knapp und einfach formuliert werden, damit auch die Betroffenen selbst sie verstehen. Sie sind ausdrücklich für unabdingbar zu erklären und dürfen nicht durch Rechtsgeschäft ausgeschlossen werden können. Die Unterscheidung zwischen öffentlichen und nichtöffentlichen Stellen ist auch bezüglich der Betroffenenrechte aufzugeben. Im Rahmen der Online-Kommunikation sollten die betroffenen Personen ihre Rechte auch telekommunikativ wahrnehmen können. Die betroffene Person sollte bereits vor der Datenerhebung über ihre Rechte informiert werden. Die Informations- und Unterrichtungspflichten sind daher entsprechend auszuweiten. Die Auskunft sollte umfassend erfolgen und sich je nach Anforderung der betroffenen Person auf alle Aspekte der Datenverarbeitung erstrecken. Insbesondere gehören hierzu Angaben zu den gespeicherten Daten selbst, zu deren Herkunft, zu den Empfängern der Daten und Teilnehmern eines automatisierten Abrufverfahrens, zum Zweck der Datenverarbeitung, zum Auftragnehmer bei Datenverarbeitung im Auftrag und zum Dienstleister bei Out-sourcing, wie auch Angaben über die erfolgte Berichtigung, Löschung oder Sperrung von Daten, über den Aufbau, die Struktur und den Ablauf der automatisierten Datenverarbeitung, insbesondere über Profilbildungen und deren Struktur. Ausnahmen von der Auskunftspflicht sollten im Unterschied zur heutigen Regelung auf wenige unabdingbare Fallkonstellationen reduziert werden.
14. Entscheidender Bedeutung kommt natürlich auch in Zukunft der Datenschutzkontrolle zu. Die Datenschutzkontrolle sollte für den öffentlichen und nicht öffentlichen Bereich einschließlich der Telekommunikation, Mediendienste und Rundfunkanstalten zusammengeführt werden. Hierfür bieten sich der Bundes- und die Landesbeauftragten an. Sie müssen zu Kompetenzzentren für Datenschutz und Datensicherheit entwickelt werden, die Kontroll- und Beratungsaufgaben aus einer Hand anbieten. Eine solche Vereinheitlichung der Kontrollstellen entspricht der Europäischen Datenschutzrichtlinie und führt zu wünschenswerten Synergieeffekten. Überdies erleichtert eine Vereinheitlichung es den Betroffenen, ihre Anrufungsrechte wahrzunehmen. Im Sinn einer völligen Unabhängigkeit der Kontrollstellen nach Art. 28 DSRL sollte die

Rechtsaufsicht über die Kontrollstellen sowohl für den öffentlichen wie auch für den nichtöffentlichen Bereich neu überdacht werden. Rechtsaufsicht ist immer mit einer Einflussnahme auf die Amtsführung der beaufsichtigten Stelle verbunden. Die Einführung der Initiativkontrolle auch im nichtöffentlichen Bereich führt überdies zu einem weitergehenden Eingriff in die Unternehmensrechte und legt eine Kontrolle über diese durch unabhängige, nicht in die Ministerialverwaltung eingebundene und von ihr kontrollierte Stellen nahe. Die notwendige demokratische Legitimation der Kontrollstellen erfolgt – wie auch heute schon – durch die Wahl der Amtsinhaber durch die Parlamente und ihre Berichtspflicht gegenüber diesen. Zur Klarstellung der Unabhängigkeit wäre eine Einrichtung des Bundesbeauftragten als oberste Bundesbehörde oder aber die Anbindung des Bundesbeauftragten für den Datenschutz an den Deutschen Bundestag – ähnlich der Stellung der Wehrbeauftragten – wünschenswert.

15. Auch die Stellung der betrieblichen und behördlichen Datenschutzbeauftragten muss gestärkt werden. Ihre Weisungsfreiheit und Unabhängigkeit sollte durch einen verstärkten Kündigungsschutz unterstützt werden, der sich an dem für Mitglieder der Mitarbeitervertretung orientiert. Lediglich natürliche Personen sollten als Datenschutzbeauftragte bestellt werden können. Externe Datenschutzbeauftragte sollten nur noch für einen Mindestzeitrahmen von fünf Jahren bestellt werden dürfen, um eine Umgehung des Kündigungsschutzes zu verhindern. Die Anforderungen an Fachkunde und Qualifikation sowie die sachliche und personelle Ausstattung der Beauftragten sollten näher beschrieben werden. Das Verhältnis zwischen Datenschutzbeauftragtem und Mitarbeitervertretung muss geklärt werden. Ein neues BDSG sollte auch die Funktion eines Konzerndatenschutzbeauftragten aufnehmen. Dies würde zu wünschenswerten Synergieeffekten führen und die Rolle des Datenschutzes im gesamten Konzernverbund stärken. Einem vom deutschen Datenschutzrecht sanktionierten Konzerndatenschutzbeauftragten wird es darüber hinaus in weltweit tätigen Konzernen leichter fallen, Datenschutzgrundsätze im gesamten Konzern durchzusetzen.

Die Koalitionsfraktionen beraten derzeit in ihren Arbeitsgruppen einen Antrag, der diese zentralen Eckpunkte für einen Neuen Datenschutz aufgreift und die Ankündigung der Bundesregierung unterstützt, dass sie unter Einbeziehung von Wissenschaft und Praxis Gesetzentwürfe zu einem Arbeitnehmerdatenschutzgesetz sowie zu einem neuen Bundesdatenschutzgesetz vorlegen will. Die Koalitionsfraktionen geben mit diesem Antrag ihrer Erwartung Ausdruck, dass die Bundesregierung diese Gesetzentwürfe rechtzeitig in das parlamentarische Verfahren einbringen wird, damit diese bis Mitte der 15. Legislaturperiode beraten und verabschiedet werden können.

Diese Erwartung ist von der Gewissheit bestimmt, dass eine Fortschreibung des nationalen Grundrechtsschutzes der überragenden Bedeutung der Entwicklung einer zivilen Informationsgesellschaft freier Bürger entsprechen

würde. Wesentliche Unterstützung könnte die Modernisierung des Datenschutzrechtes zudem dadurch bekommen, wenn flankierend die informationelle und kommunikative Selbstbestimmung als Grundrecht der Informationsgesellschaft in das Grundgesetz aufgenommen würde.

4. Fazit

Das Grundrecht auf informationelle Selbstbestimmung soll zu einem Kommunikationsgrundrecht weiterentwickelt werden, das als Querschnittsgrundrecht den kommunikativen Gehalt aller Grundrechte zum Ausdruck bringt. Aus diesem Grund sollten auch Datenschutz und Informationsfreiheit als Kehrseiten derselben Medaille angesehen werden, die zwar immer wieder auch in einem Spannungsverhältnis zueinander stehen, jedoch zugleich Funktionsbedingungen eines demokratischen Gemeinwesens und notwendige Bestandteile einer freiheitlichen Kommunikationsordnung sind. Denn noch immer gilt: Will die Gesellschaft beim Übergang zur Wissens- und Informationsgesellschaft am Ziel eines freiheitlich-demokratischen Gemeinwesens festhalten und will sie auch die wirtschaftlichen und arbeitsmarktpolitischen Potenziale nicht gefährden, kommt sie nicht umhin, auch in einer vernetzten und digitalisierten Welt das Grundrecht auf informationelle und kommunikative Selbstbestimmung zu bewahren – und das wird nur durch eine umfassende Modernisierung des bestehenden Datenschutzrechtes zu erreichen sein. Ganz im Sinne von Alfred Büllesbach wird dem neuen Datenschutz zugleich eine grundlegend neue Bedeutung als Wettbewerbs- und Standortvorteil zukommen, die es auch im Hinblick auf den europäischen und internationalen Kontext und im Interesse des Datenschutzes – zu nutzen gilt.

1 Jörg Tauss ist Mitglied des Deutschen Bundestages, Vorsitzender des Unterausschusses Neue Medien beim Bundestagsausschuss für Kultur und Medien und bildungs- und forschungspolitischer Sprecher sowie Beauftragter für Neue Medien und zur Reform des Datenschutzrechtes der SPD-Bundestagsfraktion. Dieser Beitrag entstand in Zusammenarbeit mit Johannes Kollbeck und Nermin Fazlic.

2 Die Arbeitsgruppe bestand neben Alfred Büllesbach aus dem damaligen Bundesbeauftragten für den Datenschutz, Hanspeter Bull, dem damaligen Datenschutzbeauftragten der Freien Hansestadt Hamburg, Claus Henning Schapper, dem Mitarbeiter der SPD-Fraktion Jürgen Klie sowie dem Obmann der SPD-Fraktion, Gerd Wartenberg, MdB.

3 Das Eckwertepapier ist unter der Adresse www.tauss.de abrufbar.

4 Vgl. Roßnagel/Pfitzmann/Garstka (2001):

5 An dieser Stelle gilt es nochmals, Herrn Professor Alfred Büllesbach und allen anderen Mitwirkenden im Arbeitskreis »Datenschutz« der SPD-Bundestagsfraktion und im Begleitausschuss der Koalitionsfraktionen »Modernisierung des Datenschutzes« herzlich für die hervorragende Unterstützung zu danken.

6 Vgl. Enquete-Kommission 1998 und DuD 5/2000. Zur mehrseitigen Sicherheit vgl. Müller/Pfitzmann 1997: 11 f.

7 Die Prinzipien dieses »sicheren Hafens« für den transatlantischen Austausch sensibler Daten sind auf dem DuD-Datenschutzserver abrufbar (www.dud.de, Link Datenschutzrecht, Internationales Recht), siehe auch http://www.datenschutz-berlin.de/doc/eu/index.htm# save_harbour.

8 Das vierte Schutzziel der Zurechenbarkeit von Netzaktivitäten steht selbstverständlich in einem

Spannungsverhältnis zu dem datenschutzrechtlichen Grundsatz, insbesondere auch eine anonyme Nutzung der IuK-Netzwerke zu ermöglichen (vgl. Roßnagel/Scholz 2000: 721 f.). Hier bietet die Pseudonymisierung der Nutzung für bestimmte Transaktionsklassen einen möglichen Kompromiss, vermag allerdings nicht die Spannung aufzuheben (a.a.O.).

9 Vgl. zu Selbstregulierung Bäumler 1998 und Heil 2001 sowie zur Implementierung technikrechtlicher Instrumente Bizer 1998.

10 »Aufbruch und Erneuerung – Deutschlands Weg ins 21. Jahrhundert«. Koalitionsvereinbarung zwischen der Sozialdemokratischen Partei Deutschlands und Bündnis 90/Die Grünen vom 20. 10. 1998.

11 Die folgenden Aussagen basieren im Wesentlichen auf den Ergebnissen des Gutachtens »Modernisierung des Datenschutzrechts«, welches von Alexander Roßnagel, Andreas Pfitzmann und Hansjürgen Garstka im Auftrag des Bundesministeriums des Innern im Herbst 2001 vorgelegt wurde. Siehe auch die zehn Schwerpunkte der Modernisierung des Datenschutzrechts, die vor dem Deutschen Bundestag am 6. 4. 2002 zu Protokoll gegeben habe, Deutscher Bundestag, BT-Prot. 14/165, 16180 (B) f.

Literatur

Bäumler, Helmut (Hrsg.) (1998): Der neue Datenschutz. Datenschutz in der Informationsgesellschaft von morgen. Neuwied/Kriftel/Berlin.

Bäumler, Helmut/von Mutius, Albert (1999): Datenschutzgesetze der dritten Generation. Texte und Materialen zur Modernisierung des Datenschutzrechts. Neuwied/Kriftel.

Bizer, Johann (1998): Technikfolgenabschätzung und Technikgestaltung im Datenschutzrecht. In: Bäumler, Helmut (Hrsg.): 1998, S. 45 – 64.

Bizer, Johann (1999): Datenschutz durch Technikgestaltung. In: Bäumler, H./ v. Mutius, A. (Hrsg.) 1999, S. 28 – 59.

Bizer, Johann (2001): Ziele und Elemente der Modernisierung des Datenschutzrechts. In: DuD 5/2001, S. 274 – 277.

Büllesbach, Alfred (1997): Datenschutz bei Informations- und Kommunikationsdiensten. Gutachten im Auftrag der Friedrich-Ebert-Stiftung. Bonn.

Büllesbach, Alfred/Garstka, Hansjürgen (1997): Systemdatenschutz und persönliche Verantwortung. In: Müller, Günter/Pfitzmann, Andreas (Hrsg.) (1997): Mehrseitige Sicherheit in der Kommunikationstechnik. Bonn u. a. 1997, S. 383 – 398.

Büllesbach, Alfred (Hrsg.) (1997): Datenschutz im Telekommunikationsrecht. Deregulierung und Datensicherheit in Europa. Köln.

Büllesbach, Alfred/Höss-Low. Petra (2001): Vertragslösung, Safe Harbor oder Privacy Code of Conduct. In: DuD 3/2001: S. 135 – 138.

Booz, Allen & Hamilton (2000): Digital Spaltung. Studie für die Initiative D 21. Berlin 2000.

DuD, Themenhefte der Fachzeitschrift Datenschutz und Datensicherheit:

DuD 5/2000: Neues Datenschutzrecht.

DuD 7/2000: Standards der Datensicherheit.

DuD 8/2000: Datenschutz international.

Enquete-Kommission (1998): »Zukunft der Medien in Wirtschaft und Gesellschaft – Deutschlands Weg in die Informationsgesellschaft«. Vierter Zwischenbericht: Sicherheit und Schutz im Netz. BT-Drs. 13/11002, Bonn 1998.

Heil, Helmut (2001): Datenschutz durch Selbstregulierung – Der europäische Ansatz. In: DuD 3/2001: S. 129 – 134.

Huhn, Michaela/Pfitzmann, Andreas (1998): Verschlüsselungstechniken für das Netz. In: Leggewie, Claus/Maar, Christa (Hrsg.): Internet und Politik. Köln 1998, S. 438 – 455.

Müller, Günter/Pfitzmann, Andreas (Hrsg.) (1997): Mehrseitige Kommunikation – Vertrauen in Technik durch Technik. In: Müller, Günter/Pfitzmann, Andreas (Hrsg.) (1997): Mehrseitige Sicherheit in der Kommunikationstechnik. Bonn u.a. 1997, S. 11 – 19.

Rannenberg, Kai/Pfitzmann, Andreas/Müller, Günter (1997): Sicherheit, insbesondere mehrseitige Sicherheit. In: Müller, Günter/Pfitzmann, Andreas (Hrsg.) (1997): Mehrseitige Sicherheit in der Kommunikationstech-nik. Bonn u.a. 1997, S. 21 – 30.

Roßnagel, Alexander (1997): Rechtliche Regelungen als Voraussetzung für Technikgestaltung. In: Müller, Günter/Pfitzmann, Andreas (Hrsg.): Mehrseitige Sicherheit in der Kommunikationstechnik. Bonn u.a. 1997, S. 361 – 382.

Roßnagel, Alexander/Scholz, Philip (2000): Datenschutz durch Anonymität und Pseudonymität. In: MMR 12/2000, S. 721 – 731.

Roßnagel, Alexander/Pfitzmann, Andreas/Garstka, Hansjürgen (2001): Modernisierung des Datenschutzrechtes. Gutachten im Auftrag des Bundesministeriums des Innern. Berlin.

Simitis, Spiros (1998): Das Netzwerk der Netzwerke: Ein Markt jenseits aller Kontrollen? In: Leggewie, Claus/Maar, Christa (Hrsg.): Internet und Politik. Köln 1998, S. 183 – 193.

Simitis, Spiros (2001): Auf dem Weg zu einem neuen Datenschutzkonzept, DuD 12/2001, 714 ff.

Tauss, Jörg/Özdemir, Cem (2000): Umfassende Modernisierung des Datenschutzrechtes in zwei Stufen. In: Recht der Datenverarbeitung, RDV 4/2000, S. 143 – 146.

Ulrich, Otto (1999): »Protection Profiles« – ein industriepolitischer Ansatz zur Förderung des »neuen Datenschutzes«. In: Europäische Akademie, Graue Reihe Bd. 17. Bonn 1999.