Bettina Sokol (Hrsg.)

20 Jahre Datenschutz
-
Individualismus oder Gemeinschaftssinn?

Düsseldorf 1998

Herausgeberin:

Die Landesbeauftragte
für den Datenschutz
Nordrhein-Westfalen
Bettina Sokol
Reichsstraße 43

40217 Düsseldorf

Tel.: 0211/38424-0
Fax: 0211/3842410
E-mail: datenschutz@mail.lfd.nrw.de
mailbox@mail.lfd.nrw.de

Deutsche Vereinigung
für Datenschutz e.V.
Bonner Talweg 33-35

53113 Bonn

Tel.: 0228/222498
E-mail: dvd@bg.bib.de

ISSN: 0179-2431
Druck: Neusser Druckerei und Verlag GmbH
Düsseldorf 1998

Vorwort

Die 20jährige Existenz des Bundesdatenschutzgesetzes haben die Deutsche Vereinigung für Datenschutz e.V. und ich als Landesdatenschutzbeauftragte Nordrhein-Westfalens zum Anlaß genommen, am 1. November 1997 eine Tagung unter dem Titel "20 Jahre Datenschutz - Individualismus oder Gemeinschaftssinn?" - zu veranstalten. Die dort am Vormittag gehaltenen Plenarvorträge und nachmittäglichen Arbeitsgruppenreferate werden mit diesem Dokumentationsband einer interessierten Öffentlichkeit zugänglich gemacht. Denn, daß der Wunsch nach produktivem Streit, den ich am Ende der Veranstaltungseröffnung ausgesprochen habe, in Erfüllung gegangen ist, habe ich der positiven Resonanz entnehmen können, die die Veranstaltung gefunden hat. Als Service für die Leserinnen und Leser schließt sich der Eröffnung noch ein Überblick über die nachfolgenden Beiträge an. Die Beiträge sind teilweise überarbeitet und mit Fußnoten angereichert worden, teilweise wurde aber auch bewußt der Charakter des gesprochenen Wortes so weit wie möglich beibehalten.

Nicht nur allen Vortragenden und Referierenden möchte ich an dieser Stelle nochmals herzlich danken, sondern auch der Westfälischen Wilhelms-Universität Münster, namentlich dem Institut für Informations-, Telekommunikations- und Medienrecht der Professoren Dr. Thomas Hoeren und Dr. Bernd Holznagel, LL.M., die freundlicherweise die örtliche Tagungsleitung in den Räumen der Universität übernommen haben. Stellvertretend für die Mitarbeiterinnen und Mitarbeiter des Instituts sei hier Herrn Berthold Hildering für seinen Einsatz gedankt.

Nicht unerwähnt lassen möchte ich auch die freundliche Unterstützung, die uns die Daimler-Benz AG und die debis-Systemhaus GmbH gewährt haben. Auch dafür vielen Dank. Nicht zuletzt gilt mein besonderer Dank Kordula Attermeyer-Steinkühler und Andrea Duifhuis aus meiner Dienststelle, die mit hohem Engagement die Durchführung der Veranstaltung erst ermöglicht haben. Dank gebührt auch Holger Bongers, Ute Grevels, Günter Heinen, Elke Lewitzki, Ursula Spicker und Michael Wilms, ohne deren schreibtechnische und organisatorische Hilfe der vorliegende Dokumentationsband nicht entstanden wäre.

Düsseldorf, März 1998 Bettina Sokol

Inhaltsverzeichnis

Eröffnung

Bettina Sokol

Sehr geehrte Damen und Herren, es freut mich, Sie hier und heute ganz herzlich zu unserer Veranstaltung: „20 Jahre Datenschutz - Individualismus oder Gemeinschaftssinn?“ begrüßen zu können, mit der wir zurückschauen, aber auch einen Blick nach vorne wagen möchten. 20 Jahre Datenschutz sind nicht nur 20 Jahre Bundesdatenschutzgesetz, sondern 20 Jahre einer lebhaften Diskussion und heftiger - teils kritischer - Auseinandersetzungen um Sinn und Funktion des Datenschutzes.

Die Anfangszeit des Datenschutzes war davon geprägt, daß die Datenverarbeitung auf wenigen großen Rechnern stattfand. Schon der in den siebziger Jahren gebräuchliche Begriff "Rechenzentrum" charakterisierte zutreffend die zentralen Großanlagen, deren Funktionsweise nur einigen Eingeweihten bekannt war, deren Kapazität und Tempo der Datenverarbeitung aber einem durchschnittlichen, heutigen PC in aller Regel weit unterlegen waren. Der staatliche Verwaltungsapparat - der Orwell'sche „Große Bruder“ - wurde zudem als Hauptbedrohung für die informationelle Selbstbestimmung angesehen. Es galt, Entwicklungen zu vermeiden, die zu einer immer umfassenderen, lückenlosen Registrierung des einzelnen und der einzelnen hätten führen können, letztlich zur gläsernen Bürgerin oder zum gläsernen Bürger in einer dann in ihrer Funktionsfähigkeit geschwächten Demokratie.

Die konzeptionelle Antwort des Datenschutzrechts bestand im Verbot der Verarbeitung personenbezogener Daten mit dem Vorbehalt einer Erlaubnis für gesetzlich zugelassene oder für frei vereinbarte Zwecke. Mit anderen Worten: Die Verarbeitung personenbezogener Daten bedurfte und bedarf einer gesetzlichen Grundlage, die selber den Verwendungszweck der Daten hinreichend genau bestimmt. In der damaligen Zeit war außerdem die Verantwortlichkeit für die Datenverarbeitung, also die datenverarbeitende Stel-

le, relativ einfach exakt bestimmbar und auf die Einhaltung der datenschutzrechtlichen Vorschriften kontrollierbar.

Den heutigen Ausgangsbedingungen der entstehenden Informations- oder auch Wissensgesellschaft wird dieses Konzept in weiten Teilen nicht mehr gerecht. In der vernetzten Gesellschaft findet Datenverarbeitung erstens mit einer Vielzahl von Beteiligten statt. Datenverarbeitende Stellen sind nicht mehr nur zentrale staatliche Institutionen, sondern potentiell alle Netzbürgerinnen und Netzbürger. Zweitens werden personenbezogene Daten nicht mehr nur bewußt und gezielt erhoben, sondern ergeben sich darüber hinaus beiläufig als Nebeneffekt der Nutzung von Informations- und Kommunikationsdiensten. Bereits die ganz normale Nutzung des Netzes führt dazu, daß in vielfältiger Weise personenbezogene Daten anfallen. Drittens resultiert aus all dem eine Art „Neue Unübersichtlichkeit“ für die Betroffenen. Ob es angesichts der Internationalisierung der Datenflüsse, der wachsenden Datenbestände in privater Hand und angesichts der sicherlich zunehmenden staatlichen Begehrlichkeiten, sich auch dieser privaten Bestände gegebenenfalls bedienen zu können, im Einzelfall noch überblickbar ist, was mit den Daten geschieht, scheint mehr als zweifelhaft zu sein.

Kommunikation und Wissen werden die zentralen Begriffe der Informationsgesellschaft sein. Ob der Datenschutz seinen Platz darin finden wird, hängt nicht zuletzt auch davon ab, daß er sich einer Modernisierung unterzieht, die den neuen Anforderungen adäquat Rechnung trägt. Der Schutz des Rechts auf informationelle Selbstbestimmung ist in der Informationsgesellschaft objektiv dringlicher denn je. Soll der Datenschutz nicht zu einer normativen Fiktion werden, müssen etliche Fragen geklärt werden.

Seit der Volkszählungsentscheidung des Bundesverfassungsgerichts sind viele bereichspezifische Regelungen zum Datenschutz getroffen worden. Diese Regelungen haben in etlichen Bereichen erst die Datenverarbeitung erlaubt, indem sie deren Erforderlichkeit für vielfältige Zwecke konkretisiert und die näheren Verarbeitungsmodalitäten festgeschrieben haben. Dabei wurde allerdings häufig nur das gesetzlich nachvollzogen und legitimiert, was bis dahin Verwaltungspraxis ohne rechtliche Grundlage war. In der Sache selbst wurde dem Datenschutz mit der Nachlieferung der gesetzlichen Erlaubnis oft genug ein Bärendienst erwiesen. Wie können wir künftig eine solche Verrechtlichungsfalle vermeiden?

Hinzukommt: Welche Anforderungen sind heute an die Regelungstiefe bereichspezifischer Datenschutzvorschriften zu stellen? Sicherlich muß der Verwendungszweck der zu verarbeitenden Daten präzise festgelegt werden. Weiter muß den Betroffenen auch mit hinreichender Bestimmtheit erkennbar sein, wer was wann bei welcher Gelegenheit und wie lange über sie weiß. Manche der Bestimmungen, die wir haben, lösen diesen Anspruch aber nicht ein. Sie sind kaum verständlich formuliert. Sie arbeiten mit Querverweisen und Bezugnahmen, die ihren Inhalt manchmal nicht nur einschränkend relativieren, sondern nahezu in sein Gegenteil verkehren.

Wir werden auch künftig in bestimmten Bereichen nicht ohne spezifische Regelungen zum Datenschutz auskommen können. Ebensowenig werden wir auf das Datenschutzrecht insgesamt verzichten können. Es bedarf vielmehr einer Umstrukturierung, die in einigen Punkten auf Verschlankung setzen kann, in anderen jedoch sogar Erweiterungen verlangen muß. Dies gilt beispielsweise für die Rechte der Betroffenen. Gerade angesichts der technologischen Entwicklung, die die komplexer werdenden Verarbeitungsmöglichkeiten einer immer einfacheren Handhabung zugänglich macht, brauchen die Betroffenen Rechte, die ihnen Transparenz, Entscheidungsfreiheit und Handlungsoptionen eröffnen.

Das Recht muß sich jedoch der Grenzen seiner Steuerungsfähigkeit bewußt sein. Es muß neben einem hoheitlichen Ordnungsrahmen auch Anstöße dafür liefern, daß Gefährdungen für den Datenschutz gar nicht erst entstehen. Als Beispiele seien hier nur das neue Teledienstedatenschutzgesetz und der Mediendienstestaatsvertrag genannt. Übereinstimmend normieren beide Regelungswerke beispielsweise, daß sich die Gestaltung und Auswahl technischer Einrichtungen an dem Ziel auszurichten hat, keine oder so wenige personenbezogene Daten wie möglich zu erheben, zu verarbeiten und zu nutzen. Der Grundsatz der Datenvermeidung, der damit zum Ausdruck gebracht wird, ist zwar nicht neu, aber neu ist der Ort, an dem er zu beachten ist, nämlich schon auf der Ebene der technischen Voraussetzungen für die Kommunikation.

Das Recht selbst kann mit seinen Anforderungen die Entwicklung und den Einsatz datenschutzfreundlicher Technologien fördern und verlangen. Datenschutz durch Technik greift nicht erst, wenn das Recht an seine Durchsetzungsgrenzen stößt. Aber für diese Fälle, an deren Auftreten wir uns in der vernetzten Welt sicherlich werden gewöhnen müssen, ist die Befähigung der Menschen unverzichtbar, sich selbst vor Datenschutzverletzungen

schützen zu können. Dabei gilt es allerdings zu vermeiden, daß ein Teil der Bevölkerung auf der Strecke bleibt und sich nur noch die Spezialistinnen und Spezialisten unter den Computerfreaks ein angemessenes Datenschutzniveau organisieren können.

Meine Damen und Herren, zu all diesen Fragen wünsche ich uns einen Tag des produktiven Streits!

Zu den einzelnen Beiträgen:

Die Vorgeschichte des Datenschutzes, seine Geburtsfehler und seine weitere - in drei Phasen unterteilte - Existenz untersucht *Lutterbeck* in seinem Beitrag unter Berücksichtigung der technischen, politischen und rechtlichen Entwicklungen. Vor dem veränderten politischen Hintergrund und der modernen technischen Infrastruktur sieht er die Steuerungskraft und Durchsetzbarkeit des Rechts schwinden. Kritisch beleuchtet er nochmals die Volkszählungsentscheidung des Bundesverfassungsgerichts von 1983. Bereichspezifische Regelungen wie auch die Eingriffsdogmatik selbst seien unter den heutigen Rahmenbedingungen fragwürdig bis obsolet geworden. Lutterbeck fordert, die Staatsfixiertheit des Datenschutzes aufzugeben und empfiehlt den Datenschützern, wieder genauer zuzuhören, Fehler zuzugeben sowie wieder Neugierde zu entwickeln.

Das Internet sowie die multimedialen Informations- und Kommunikationsdienste bezeichnet *Pitschas* als technische Zauberformeln der Zukunft, die ihren Beitrag zur Entgrenzung unseres Verständnisses von Raum, Zeit und Privatheit leisten werden. In der Kommunikationsverdichtung sieht er einen Freiheitsgewinn, der zu einem Wandel des staatlichen Selbstverständnisses führen werde. Zu den staatlichen Kernaufgaben werde künftig auch die Informationsversorgung der Gesellschaft zählen. Seine Informationsfunktion habe der Staat mit der Schaffung einer informationsrechtlichen Infrastruktur und einem veränderten Datenschutzrecht zu erfüllen. Dafür bedürfe es des Konzepts einer dimensionalen, selbstregulativen und zugleich rahmensetzenden Informations- bzw. Wissensordnung. Die Wirklichkeit werde verfehlt mit einem Verständnis des Rechts auf informationelle Selbstbestimmung als Eigentumsgrundrecht, in dessen Freiheitsbereich mit jedweder Ausübung staatlicher Informationskompetenz potentiell eingegriffen werde. Unter den Bedingungen der Informationsgesellschaft sei eine Neuinterpretation gefordert, die von der abwehrrechtlichen Perspektive zur teilhaberecht-

lichen Betrachtung zu wechseln habe. Notwendig sei die Entwicklung eines verfassungsrechtlichen Strukturkonzepts der informationellen Selbststeuerung in Verbindung mit der Informationsfreiheit und dem Recht des einzelnen auf Information, dem eine staatliche Informationspflicht entspreche. Der erforderliche Datenverkehrsschutz müsse gleichwohl einheitlich für den öffentlichen wie für den privaten Sektor eine interessengesteuerte Objektstellung der Bürger zu verhindern wissen.

Am Beispiel der individuellen Einwilligung in die Verarbeitung personenbezogener Daten, die in der Praxis zunehmend als Hebel für die Einschränkung gesetzlicher Schutzstandards genutzt werde, hinterfragt *Walz* das Konzept des „Selbstdatenschutzes". Für erforderlich hält er eine Diskussion über die Grenzen der Individualautonomie im Datenschutzrecht. Wo die freie Ausübung des Rechts auf informationelle Selbstbestimmung aufhöre und die staatliche Interventionspflicht zugunsten der Schwächeren beginne, müsse in der Informationsgesellschaft mit ihren vielfältigen interaktiven elektronischen Verkehrsformen neu definiert werden. Die Umsetzung der Europäischen Datenschutzrichtlinie in bundesdeutsches Recht sieht Walz als Chance für eine Modernisierung des Datenschutzes, mit der sowohl auf neue Technikrisiken reagiert als auch über Alternativen zu unserem bisherigen Datenschutzsystem nachgedacht und die individuelle Rechtsposition der von Datenverarbeitung Betroffenen gestärkt werden könnte. Er stellt ein Wissensdefizit hinsichtlich der Qualität und der Funktionsfähigkeit bundesdeutscher Datenschutzgesetze sowie -instanzen fest und fordert insoweit eine selbstkritische Evaluation. Die Auflösung der Grenzen zwischen öffentlichem und privatem Recht konstatiert er ebenso wie die Notwendigkeit des Einsatzes datenschutzfreundlicher Technik. Sowohl grenzüberschreitende als auch nationale Regulierung behielten jedoch ihren jeweiligen Stellenwert, da technischer Datenschutz zwar helfen könne, Grundrechtsschutz durchzusetzen, ihn aber nicht ersetzen könne.

Die Europäische Datenschutzrichtlinie und ihre notwendige Umsetzung in bundesdeutsches Recht ist Gegenstand der Beiträge von *Garstka* und *Büllesbach*. Büllesbach benennt insoweit die Unterschiede zwischen der Richtlinie und dem bisherigen Bundesdatenschutzgesetz und fordert die möglichst einheitliche Umsetzung der Richtlinie in allen Mitgliedstaaten. Garstka kritisiert die bisher vom Bundesinnenministerium vorgelegten Entwürfe für die Novellierung des Bundesdatenschutzgesetzes als defizitär, da sie nicht nur die Chance einer Fortentwicklung des Datenschutzrechts verpaßten, sondern sogar zwingende Änderungen unterließen. Die Auswirkun-

gen der Richtlinie auf das bundesdeutsche Recht zeigt er anhand verschiedener Begriffsbestimmungen sowie der materiellen Anforderungen der Richtlinie, insbesondere im Hinblick auf die Rechte der Betroffenen und die Datenschutzkontrolle.

Rieß und *Müller-Maguhn* setzen sich mit der Bedeutung und den Folgen der Globalisierung für den Datenschutz auseinander. Rieß verlangt ein mehrseitiges multinationales Datenschutz- und Sicherheitskonzept, das sowohl im Bereich multinationaler Unternehmen als auch auf der Ebene multinationaler zwischenstaatlicher Vereinbarungen und auf der Ebene von Nichtregierungsorganisationen zu etablieren sei. Die immer wieder zur Diskussion stehenden Absichten zur Reglementierung der Kryptographie seien ein untauglicher Versuch, das nationalstaatliche Gewaltmonopol im Netz herzustellen, zumal schon die Überwachungsmöglichkeiten für Telekommunikationsnetze überzogen seien. Müller-Maguhn skizziert die veränderten Ausgangsbedingungen eines Lebens in der Informationsgesellschaft und beansprucht auch für die Netzwelt ein Recht auf Teilhabe, vor allem aber auf Privatsphäre. Vor dem Hintergrund des globalen Netzes benennt er die Gemeinsamkeiten und die Unterschiede der in verschiedenen Ländern jeweils vorherrschenden Bewertungen gleicher Sachverhalte. Schließlich schlägt er die Funktion eines „Transparenzbeauftragten“ und die Verwendung von Warnhinweisen vor.

Bizer und *Pfitzmann* befassen sich mit dem Verhältnis von Technik und Recht. Die klassischen rechtlichen Steuerungsinstrumente sieht Bizer angesichts der technischen Entwicklung nicht mehr als ausreichend an. Demgegenüber plädiert er unter anderem für Verschlüsselung, für Möglichkeiten des anonymen und pseudonymen Handelns sowie für eine datenminimierende Systemgestaltung als Elemente eines neuen Datenschutzrechts, das Technik gestalten und Selbstschutzkonzepte motivieren und flankieren könne. Mehrseitige Sicherheit und Selbstschutz sind auch aus der technischen Perspektive Pfitzmanns zentrale Begrifflichkeiten, um Datenmißbrauch möglichst zu verhindern und Pseudokonflikte zu vermeiden. Gleichwohl könne auch eine im Sinne des Datenschutzes optimal gestaltete Technik das Recht letztlich nicht überflüssig machen.

20 Jahre Dauerkonflikt: Die Novellierung des Bundesdatenschutzgesetzes

Bernd Lutterbeck

1. Ein Blick nach vorn ...

„Ich erinnere mich an ein verwirrendes Detail, das eine Internet-Sachverständige in dem Hearing zu dieser Sache geäußert hat: Diese Frau war irgendwann in einem MUD (Multi User Dungeon, ein Online-Fantasiespiel). Irgend so ein Missetäter ließ seinen virtuellen Hund auf die Frau los, weil sie angeblich in seine Domain eingebrochen war. Glücklicherweise waren die anderen MUD - Bewohner bereit, sie zu retten, indem sie vehement gegen die Attacke des virtuellen Biestes protestierten."

Die Richterin *Loretta Preska* erinnert sich dieser Äußerung in der ersten Fußnote ihres Urteils, das über die Verfassungsmäßigkeit eines New Yorker Gesetzes zur Regelung von Schmuddelinhalten im Internet zu entscheiden hatte. Sie resümiert in dieser Entscheidung vom 20. Juni 1997 auch die Essenz dieser Geschichte:

„Ich war erleichtert, daß diese Geschichte ein gutes Ende hatte. Aber ich muß gestehen, diese kleine Geschichte hat mit das Fenster zu einer mir bis dahin völlig verschlossenen Welt geöffnet."[1]

[1] District Court for the Southern District of New-York in der Sache American Library Association e.a. v. Pataki v. 20.06.1997 <http://www.ftc.org/court/nycdadec.html, besichtigt am 30.06.1997>.

Die Richterin *Loretta Preska* gibt zu, daß sie sich noch wundern kann. Sie wundert sich über die neuartigen sozialen Beziehungen, die durch den Gebrauch einer neuen Technik entstehen. Natürlich interessiert sie als Juristin der Regelungsgehalt der neuen Situation. Ihr Urteil gibt ihr die Chance, diesen auszudrücken.

Um nichts anderes geht es auch im deutschen Datenschutz: Neue Technik - neue soziale Sachverhalte - neue Regelungen, wo immer sie geboten sind. Zumindest in Festvorträgen wird man sich über diese Gleichung schnell verständigen können. Aber es ist in Deutschland schwer vorstellbar, daß eine ernst zu nehmende Persönlichkeit sich öffentlich wundert - sie wäre denn Bundespräsident. Ich vermute, daß Richterin *Preska* ihren *Aristoteles* sehr wohl gelesen hat, der im ersten Buch der Metaphysik schreibt: *„...Verwunderung (...) ist der Anfang des Philosophierens. ... Wer sich über eine Sache fragt und verwundert, der glaubt sie nicht zu kennen.“*[2] Wer nicht fragt und sich nicht mehr wundert, erhält auch keine Antwort. Ich fürchte, dies ist die Zustandsbeschreibung des Datenschutzes und mit ihm vieler Datenschützer im Herbst 1997. 20 Jahre Dauerkonflikt mit Sicherheitsbehörden, mit Sozialleistungsträgern, unwilligen Kommunalverwaltungen und wem auch immer, 20 Jahre Kampf um einen besseren Datenschutz haben dem Datenschutz und mit ihm vielen Datenschützern den letzten Tropfen Blut aus den Adern gesogen. Ich will im folgenden prüfen, ob Wiederbelebungsversuche Aussicht auf Erfolg haben.

2. Und ein Blick zurück

2.1 Die Vorgeschichte

Man kann natürlich den Datenschutz und damit seine Geschichte mit dem Erlaß des Bundesdatenschutzgesetzes vor 20 Jahren beginnen lassen. Bei einer solchen Betrachtung rücken naturgemäß das Gesetz selber und die stetigen Bemühungen, es zu verändern, in den Vordergrund. Diese Sicht betont die politische Auseinandersetzung und die instrumentelle Seite des Themas.

[2] Aristoteles, Metaphysik. Buch I, Kap. 2 (c), in: Philosophische Schriften, Bd. 5. Hamburg 1995.

Man kann aber, was ich vorschlage, sehr viel früher anfangen. Denn alle wesentlichen technischen Paradigmen, auf die der Datenschutzgedanke aufgesetzt wurde, die meisten, häufig zähneknirschenden politischen Zugeständnisse und alle intellektuellen Konzepte stammen aus der Zeit vor Erlaß des Bundesdatenschutzgesetzes. Diese Sicht betont die intellektuelle Seite des Themas und interessiert sich für den gesellschaftlichen Prozeß, der neue Techniken möglich und neue Regularien erforderlich macht. Sie fragt nach den Paradigmen und Konzepten des Datenschutzes.

Das technisch-, organisatorisch-, politische Paradigma des Datenschutzes ist auch in heutigen Publikationen gelegentlich noch präsent: Eine kurze, aber mächtige Diskussion in den USA um Datensammlungen über Vietnamkriegsgegner und Vorhaben der Administration, zentrale Datensammlungen in Washington D.C. aufzubauen, führte Mitte der sechziger Jahre zum Stopp entsprechender Pläne. Der Ausgang dieser Diskussion war in Deutschland durchaus bekannt, als in der Presse um 1968 eine Debatte um die entsprechenden zentralistischen Pläne der Regierung *Kiesinger* entbrannte.[3] Auch diese Diskussion war kurz und heftig. Ihren Abschluß fand sie mit dem hessischen Datenschutzgesetz von 1970. Schon die Besonderheit dieses Anfangs ist heute überwiegend in Vergessenheit geraten: Datenverarbeitung und Datenschutz wurden durchaus als Einheit gesehen - als Seiten eines einheitlich verstandenen technischen Fortschritts, den man gewünscht und nach Kräften gefördert hat.

Die frühen Datenschützer waren begeisterte Förderer der Informationstechnik. Die damals bekannte Parole „Hessen vorn!“ war Ausdruck dieser in keiner Hinsicht technikfeindlichen Gesinnung: Hessen wollte führend in der Datenverarbeitung und im Datenschutz zugleich sein. Die frühen, vor allem akademischen Datenschützer, wollten da nicht nachstehen. Wenn man ihnen böse will, könnte man diese Personen als Technokraten bezeichnen, keineswegs aber als Technikfeinde.

Das *intellektuelle Paradigma* ist wohl völlig in Vergessenheit geraten und bestenfalls noch wenigen, zumeist älteren Personen bekannt. Der Anfang ist Mitte der sechziger Jahre von einer Gruppe zumeist evangelischer Theologen bzw. theologisch interessierter Juristen an der Universität München gelegt worden. Ihre Wortführer waren *Siegfried Grundmann* und zu allererst

[3] Grundlegend Kamlah: Right to Privacy. Das Allgemeine Persönlichkeitsrecht in amerikanischer Sicht unter Berücksichtigung neuer technologischer Entwicklungen, Köln 1969.

der heutige Bundespräsident *Roman Herzog*. Der schon früh brillante *Roman Herzog* hat das unabänderliche Credo dieser Gruppe in einem fulminanten Einleitungskapitel zur ersten Auflage des *Evangelischen Staatslexikons* niedergeschrieben: *„Der Mensch des Technischen Zeitalters in Recht und Theologie“*.

Wer dieses umfangreiche Kapitel heute liest, ist überrascht über die Sensibilität in technischen und naturwissenschaftlichen Sachverhalten und die Gewißheit der handelnden Personen, Zeugen einer neuen Epoche zu sein. Vor allem fällt ihm die Wucht der philosophischen Aussage auf, wenn *Herzog* etwa schreibt:

„Die Entwicklung, die der Mensch in den letzten Jahren genommen hat, und mehr noch die Entwicklung, die sich für die nächsten zehn oder fünfzehn Jahre andeutet, ist so revolutionär, daß keine Wissenschaft, die sich mit dem Menschen und seinen Institutionen befaßt, einen Augenblick mit dem Versuch ihrer Deutung und Bewältigung zögern darf.“[4]

Nur wenige Jahre später war es *Wilhelm Steinmüller*, einem jungen Habilitanden dieses Kreises, gelungen, diese Philosophie in einem gesellschaftlichen Anwendungsbereich praktisch umzusetzen. Zusammen mit mir und *Christoph Mallmann* legte er dem Bundesinnenministerium 1971 ein Gutachten mit dem beziehungsreichen Titel „Grundlagen des Datenschutzes“ vor.[5] Mit diesem Gutachten ist die intellektuelle Vorgeschichte des Datenschutzes im wesentlichen beendet. [6]

[4] Herzog: Der Mensch des technischen Zeitalters in Recht und Theologie. Vorwort zur 1. Aufl. des Ev. Staatslexikons, Stuttgart 1966, S. XXI ff.

[5] Steinmüller/Lutterbeck/Mallmann: Gutachten im Auftrag des Bundesministers des Innern, BT-DRs. VI/3826 v. 07.09.1972. Dem Gutachten ist ein „Probelauf“ vorangegangen, in dem wir die Figur der informationellen Selbstbestimmung erstmals der Öffentlichkeit vorgestellt haben, vgl. Mallmann: Das Problem der Privatsphäre innerhalb des Datenschutzes, in Siemens A.G. (Hrsg.), Datenschutz - Datensicherung. München: Siemens A.G. 1971, S. 19 ff.

[6] Podlech hat unsere Formulierungen dann später in eine juristisch widerspruchsfreie Textversion übersetzt, vgl. Podlech, AK GG, 1984, Art. 2 Abs. 1 Rdnr. 45.

2.2 In der Blüte der Jahre

Anfang der siebziger Jahre konnte der deutsche Datenschutz so etwas wie ein Exportschlager der Bundesrepublik werden: Die Parole „Hessen vorn!“ war ansteckend nicht nur für die restliche Republik. Sie stand für Modernität, Reformwillen und die Bereitschaft, Computer einzusetzen, wo immer das möglich war. Nicht zu unterschätzen auch, daß die Bundesrepublik durch unser Gutachten über ein intellektuelles Konzept verfügte, mit dem man die sperrige neue Materie Datenschutz rechtlich einfangen konnte.

2.2.1 Geburtsfehler

Trotzdem hat es in Bonn einen nicht enden wollenden Kampf um das Datenschutzgesetz gegeben. Dieser lange Kampf verweist auf einen Geburtsfehler des bundesdeutschen Datenschutzes, der auch heute noch nicht behoben ist: Die Ressortzuständigkeit für den Datenschutz liegt beim Bund und in den Bundesländern beim Innenministerium. Diese Zuständigkeitsverteilung hat für den Datenschutz zumindest drei problematische Konsequenzen:

1. Die Innenminister sind auch zuständig für Polizei, Verfassungsschutz und Geheimdienste. Die Geschichte des Datenschutzes zumindest im Bund kann man lesen als ein stetiges miteinander Verwachsen und Verwuchern von Datenschutz und Innerer Sicherheit. Es ist diesem Verständnis geschuldet, wenn eine BDSG-Novelle in einem Artikelgesetz mit einigen Gesetzen zur Inneren Sicherheit erlassen wird. Angesichts der Macht, die das klassische Ressort Innenminister nach wie vor im Konzert der Bürokratien hat, gibt es kaum eine öffentliche Stelle des Bundes, die unbefangen mit dem Thema Datenschutz umgehen kann. So steht häufig die Innere Sicherheit auf der Tagesordnung, auch wenn sie gar nicht berührt ist.

2. Auch die Datenverarbeitung selber ressortiert bei den Innenministern, wo sie bei Zugrundelegung von Wirtschaftlichkeits- und Effizienzgesichtspunkten nichts zu suchen hat. Es ist hoch unwahrscheinlich, daß ein Innenministerium, das als Verfassungsministerium aus guten Gründen einen gewissen Konservatismus an den Tag legen muß, als Ministerium, das die Entwicklung der Informationstechnik mindestens in der Öffentlichen Verwaltung voranzutreiben hat, eine besondere Dynamik

an den Tag legen wird. Es fehlen die fachlichen Kompetenzen, der wirtschaftliche Sachverstand und das Verständnis für neue technische Entwicklungen. Belege für die mangelnde Dynamik dieses Ressorts lassen sich reichlich finden. Man schaue sich nur an, wie das Ministerium selbst und der Bundesdatenschutzbeauftragte als Teil dieses Ressorts im Netz präsent ist.

So ist der alte innere Zusammenhang zwischen Datenschutz und technischer Entwicklung schon früh zerrissen worden. Innere Sicherheit und ein veraltetes Verständnis von Verwaltung haben die Oberhand bekommen über den Wunsch, ja die Notwendigkeit, die Verwaltungen nicht nur des Bundes mit Hilfe der Informationstechnik zu modernisieren und als Ausdruck der Modernität auch den Datenschutz voranzutreiben.

Der Preis für dieses konzeptionelle Gemenge aus Bewahrung der Verfassung, Datenschutz, Datenverarbeitung, Verwaltungsreform und Innerer Sicherheit ist hoch: Neueste Statistiken der OECD belegen einen Modernitätsrückstand der, wenn auch nicht aller deutschen Verwaltungen gegenüber etlichen anderen Industriestaaten.[7] Daß der vormalige Exportschlager Datenschutz nunmehr zum Ladenhüter geworden ist, ist ein eher nebensächlicher Effekt dieser bedrückenden Zahlen.

3. Mit der Ressortzuständigkeit war ein weiterer Effekt vorgegeben, der praktisch wahrscheinlich bedeutsamer war und ist als die meisten konzeptionellen Kontroversen. Mit dieser Zuständigkeit war einer überwiegend juristischen Betrachtung des Datenschutzes das Tor geöffnet. Andere Sichtweisen aus Ökonomie und Informatik haben es bis heute schwer gehört zu werden - trotz anders lautender Rhetorik.

   Auch dieser Kampf um eine eher juristische oder eher technisch-politische Sicht war bereits 1977 vorläufig entschieden. Bei der Besetzung des ersten Bundesdatenschutzbeauftragten wurde nicht der Techniker und Politiker ausgewählt. Die Wahl fiel auf den Verfassungsjuristen.

[7] Auf diesen Tatbestand hat vor längerem Naschold: Modernisierung des Staates. Zur Ordnungs- und Innovationspolitk des öffentlichen Sektors. Berlin 1993, aufmerksam gemacht, sowie mein Beitrag: Funktionswandel des Staates, in: Büllesbach (Hrsg.): Staat im Wandel, Köln 1995, S. 7 ff.

	Die Vorphase des Datenschutzes beginnt:
07.10.1970	• Datenschutzgesetz von Hessen
15.07.1971	• Datenschutzgutachten von Steinmüller, Lutterbeck und Mallman
	Die erste Phase des Datenschutzes beginnt:
27.01.1977	• Das BDSG erblickt die Welt
1978	• Der Bundesdatenschutzbeauftragte nimmt seine Arbeit auf
1980-1990	• Länderdatenschutzgesetze, diverse bereichspezifische Datenschutzgesetze
	Die zweite Phase des Datenschutzes beginnt:
15.12.1983	• Volkszählungsurteil des Bundesverfassungsgerichts
20.12.1990	• Erste BDSG-Novelle im Gesetz zur Fortentwicklung des Datenschutzes und der Datenverarbeitung
	Die dritte (europäische) Phase des Datenschutzes beginnt:
24.10.1995	• Datenschutzrichtlinie der EU
24.10.1998	• Umsetzungsfrist für die EU-Richtlinie endet
01.01.1999	• Datenschutz im Amsterdamer Vertrag (Art. 286 EGV)
	Die vierte Phase des Datenschutzes hat begonnen:
schleichend, vielleicht beginnend etwa 1984	„Just in dem Augenblick, in dem die Anerkennung ihren Höhepunkt erreicht, steuert der Datenschutz auf seine tiefste Krise zu.“ (S. Simitis am 3. September 1984 im Hessischen Landtag)
	• Der Datenschutz wird bürokratisch

Tabelle 1: Entwicklungsstufen des Datenschutzes

2.2.2 Drei Phasen

Ein übergreifender technisch-organisatorischer Gesichtspunkt, drei innenpolitische Gesichtspunkte unterschiedlicher Reichweite und ein intellektuelles Moment waren also kennzeichnend für das Datenschutzkonzept der *ersten Phase*:

Eine Orientierung am zentralistischen Modell von Staatsführung und EDV-Einsatz, eine Vermischung des Datenschutzanliegens mit spezifischen innenpolitischen Maßgaben, wie sie der Kultur des Bundesinnenministeriums

entsprechen und ein eigentümliches intellektuelles Konzept, ohne das man auch heute den praktisch geltenden Datenschutz nicht verstehen kann. Kern dieses Konzeptes, das bekanntlich u.a. die Erfindung des informationellen Selbstbestimmungsrechts enthielt, war, aus der Rückschau von 25 Jahren betrachtet, seine theologische Wucht, weniger seine juristischen Erfindungen. Übertragen gesprochen war Gottes Zorn so mächtig, daß sich bis heute nur zaghafter intellektueller Widerstand gerührt hat.

Die Stunde des Sieges im Jahre 1977 war also auch eine Stunde der Niederlage. Diese historischen Umstände sollte man kennen, wenn man zu einer erneuten Runde im Kampf um den besseren Datenschutz antritt.

Trotz dieses eher nüchternen Befundes nenne ich diese Phase „*in der Blüte der Jahre*“. In der Datenschutzpraxis der folgenden Jahre ist es nämlich immer weiter aufwärts gegangen. Tüchtige, motivierte und hoch qualifizierte Mitarbeiter in den neu entstehenden Behörden mit dem Schub einer wohlwollenden veröffentlichten Meinung im Rücken konnten das neue Anliegen Datenschutz einer durchaus interessierten Öffentlichkeit bekannt machen. Gesetz für Gesetz wuchs das Selbstbewußtsein, um 1983 einen nie mehr erlangten Höhepunkt zu erreichen. Es schien so, als sei das Wohl der Republik vom Datenschutz abhängig. Das Volk hatte sich erhoben und gegen den Staat gemotzt und dabei vor Gericht Recht behalten, was so gar nicht deutscher Tradition und der Tradition deutscher Verfassungsjuristen entspricht. Nur sehr kluge Beobachter konnten im Urteil des Bundesverfassungsgerichts den Keim einer verheerenden Niederlage des Datenschutzes entdecken, von der er sich bis heute nicht erholt hat. Bevor ich diese Sicht näher behandle, möchte ich wenigstens kurz auf weitere Phasen des Datenschutzes eingehen.

In der *zweiten Phase* macht es sich der Datenschutz zur Aufgabe, das Volkzählungsurteil rechtlich umzusetzen. Zahlreiche Gesetze in allen Bereichen sind die Folge. Es kommt auch, nach wiederum quälenden Jahren des politischen Ringens, eine Datenschutznovelle zustande. Unter Fachleuten bleibt strittig, inwieweit dieses neue BDSG eine wirkliche Verbesserung darstellt.

In der *dritten Phase* wird der Datenschutz europäisch. Man könnte diese Phase mit guten Gründen mit der Kommissions-Drucksache von 1990 anfangen lassen.[8] Ich starte sie mit dem finalen Akt, insofern bleibt der über-

[8] KOM (90) 314 endg. v. 13.09.1990.

wiegend dezionistische Charakter dieser historischen *Tabelle* (Tabelle 1) gewahrt. Ich schließe sie ab mit dem 01.01.1999, wenn der Amsterdamer Vertrag die bisher geltenden Datenschutz-Rechtsakte für die Gemeinschaftsorgane in Kraft setzt.

Die entscheidenden Bewährungsproben müssen die deutschen Interessengruppen erst noch bestehen. *Simitis* hat die bevorstehenden Aufgaben schon so formuliert: Wie verhindert man, daß ein deutscher Betrachter beim Anblick von Art. 7 der Datenschutz - Richtlinie sofort an sein geliebtes Verbot mit Erlaubnisvorbehalt und ein Franzose bei Art. 8 sofort an seine Vorschriften über sensitive Daten denkt?[9] Wie vermeidet man also, daß auf dem Umweg der Interpretation supranationale Vorschriften wieder nationalisiert werden? Wie auch immer - die Regionalisierung und Internationalisierung des Datenschutzes stehen ins Haus.

3. Das Volkszählungsurteil - ein Pyrrhussieg für den Datenschutz?

Ein gutes halbes Jahr nach dem Volkszählungsurteil[10] konnte man über Für und Wider des Richterspruchs schon einigermaßen plausible Vermutungen anstellen. *Rupert Scholz* und *Rainer Pitschas* haben das getan - in einer Monographie, die, wenn ich das so sagen darf, wider den herrschenden Zeitgeist gebürstet war.[11] Heute wird man dieses Buch gelassener lesen müssen, denn auch der vermeintliche intellektuelle Antipode des von *Scholz* und *Pitschas* vertretenen Ansatzes, *Spiros Simitis*, zeigt sich schon 1984 auf der ganzen Höhe seiner intellektuellen Brillanz: Eminent klug, nachdenklich und zugleich rätselhaft.

3.1 Simitis Analyse

Am 3. September 1984 spricht *der Hessische Datenschutzbeauftragte Spiros Simitis* auf einem Symposium der Hessischen Landesregierung zum

[9] Simitis, NJW 1997, 282 f.
[10] BVerfGE 65, 1 ff.
[11] Scholz/Pitschas: Informationelle Selbstbestimmung und staatliche Informationsverantwortung. Berlin 1984.

Thema „Informationsgesellschaft oder Überwachungsstaat“.[12] Trotz der veränderten politischen Zeitläufe war es noch immer Hessen, das eingedenk seiner alten Parole „Hessen vorn“ dem Rest der Republik den Weg des Fortschritts weisen wollte. Man glaubte damals zu wissen, daß die gesellschaftliche Stimmung, die das Urteil trug oder doch nur zu ihm geführt hat, für einen von der Gesellschaft gewünschten Aufbruch steht - wohin auch immer. Entsprechend hochkarätig besetzt war das Symposium, das im Plenarsaal des hessischen Landtags stattfand.

Der hessische Datenschutzbeauftragte Spiros Simitis wartete in seiner Einführungsrede mit einer Zustandsbeschreibung des Datenschutzes auf, die etliche seiner Zuhörer stark verwirrt hat. Man kann das noch heute in den Protokollen der Veranstaltung nachlesen. Zu dieser Verwirrung trug ein einziger Satz bei:

„So paradox es freilich klingt: Just in dem Augenblick, in dem die Anerkennung ihren Höhepunkt erreicht, steuert der Datenschutz auf seine tiefste Krise zu.“ (S. 29)

In drei Punkten und drei Überschriften bringt *Simitis* diese Krise zum Ausdruck:

1. Die poröse rechtliche Infrastruktur
2. Der veränderte politische Kontext
3. Die modifizierte technische Infrastruktur

Unter der ersten Überschrift spricht Simitis davon, daß *„die Realität der Datenverarbeitung (..) durch eine mindestens genauso konsequente Domestizierung des Datenschutzes gekennzeichnet (sei)“*. Es sei ein „Konstruktionsfehler“, daß die Datenschutzgesetze als Auffanggesetze konzipiert seien (S. 31). Die zweite Überschrift ist auch heute noch gut geeignet für einen analytischen Bezugsrahmen: *„... Datenschutz zielt auf einen kalkulierten Informationsverzicht ... um der Demokratie willen.“* Schon seit der zweiten Hälfte der siebziger Jahre habe sich der ökonomische Kontext für dieses Konzept geändert, eine wirtschaftlich kritische Situation habe sich auf die Politik auswirken müssen. *„Den verknappten Ressourcen entspricht eine*

[12] Simitis: Reicht unser Datenschutzrecht angesichts der technischen Revolution? - Strategien zur Wahrung der Freiheitsrechte, in: Staatskanzlei von Hessen (Hrsg.): Informationsgesellschaft oder Überwachungsstaat. Protokoll des Symposiums der Hessischen Landesregierung. Wiesbaden 1984, S. 27 ff.

verschärfte Kontrolle der Einnahmen und Ausgaben sowie der Versuch, das staatliche Leistungssystem zu rationalisieren.“ (S. 33) Man reibt sich verdutzt die Augen: War nicht in der zweiten Hälfte der siebziger Jahre das Jahrhundertgesetz BDSG überhaupt erst in Kraft getreten? Man darf also gespannt sein, wie der Autor solche Irritationen beantwortet.

Auch in seiner dritten Überschrift beweist der Datenschutzbeauftragte seine konzeptionelle Weitsicht: Natürlich orientieren sich die Datenschutzgesetze *„an der Vorstellung einer durch die automatische Verarbeitung ausgelösten und nicht mehr revidierbaren Zentralisierung der Information“*. (S. 38) Kurz und bündig heißt es bei ihm:

„Kurzum, die Prämisse der Datenschutzgesetze ist auf den Kopf gestellt: Nicht die Zentralisierung, sondern die Dezentralisierung beherrscht das Feld.“ (S. 38) Natürlich läßt diese Analyse nur einen einzigen Schluß zu: *„Der Datenschutz ist an den Grenzen seiner Funktionsfähigkeit angelangt. Dem Gesetzgeber bleibt ... keine andere Wahl: Will er sich wirklich an die verfassungsrechtlichen Vorgaben halten, dann muß er sich für ein neues Datenschutzkonzept entscheiden.“* (S. 40)

3.2 Hassemers Analyse

Ich habe diese eine Stimme herausgegriffen, weil sie gut dokumentiert ist und wirklich klug zusammenfaßt, was man schon 1984 hätte wissen können. Vor allem aber auch deshalb, weil man an den späteren Tätigkeitsberichten des *Hessischen Datenschutzbeauftragten* ziemlich gut nachvollziehen kann, wie der Nachfolger im Amt mit dieser Analyse umgeht. Ich zitiere aus den Berichten für 1993 bis zur Abschiedsrede von *Winfried Hassemer* am 30. Mai 1996:[13]

„Das Jahr 1993 war in Staat und Gesellschaft der Bundesrepublik von Sorgen geprägt. Diese Sorgen haben auch den Datenschutz erreicht und beeinträchtigt. Auf zwei Feldern konnte man spüren, daß sich das Klima geändert hat: in der Wirtschaft und bei der inneren Sicherheit (...)

[13] Alle folgenden Zitate über den Server des Hessischen Datenschutzbeauftragten <http://www.hessen.de/hdsb, besichtigt am 15.10.1997>.

Die wirtschaftlichen Probleme und die Angst vor dem Verbrechen bewirken für den Datenschutz am Ende dasselbe: Sie erhöhen die Kontrollbedürfnisse des Staates (...)

Der Datenschutz nimmt an den langfristigen Entwicklungen in Staat und Gesellschaft teil. Er kann sie hier und da beeinflussen, er kann sie aber nicht umdrehen. Daß wir auf absehbare Zeit mit wirtschaftlichen Schwierigkeiten und in Verbrechensfurcht leben müssen, führt zu Einschränkungen bei der Gewährleistung der informationellen Selbstbestimmung der Bürger. Die Datenschützer können das beklagen und monieren, sie können es aber, wie sich zeigt, nicht verhindern.“ Der für späteres wichtige Satz lautet: *„Darauf müssen sie sich theoretisch und pragmatisch einstellen.“*

In seinem *Bericht für 1994*, weist der Beauftragte auf die Bedeutung des Datenschutzes für die Menschen, die Alltagspraxis hin und schreibt: *„Auch sonst scheinen mir Kampf und Werben um gesetzliche Einrichtungen des Datenschutzes nicht mehr im Zentrum der Aufmerksamkeit stehen zu müssen.“*

Schließlich heißt es in seinem Bericht für 1995: *„Für die Zukunft steht ein neues Datenschutzkonzept zur Debatte. Vor allem die Entwicklungen der modernen Informations- und Kommunikationstechnologie haben die ursprünglichen Erwartungen des Gesetzgebers widerlegt, Datenschutz sei im wesentlichen die Kontrolle eines zentralen Rechners in öffentlicher Hand. Statt dessen gibt es viele kleine Rechner, untereinander vernetzt und vor allem in privater Hand.“*

Und in seiner Abschlußrede vom 30. Mai 1996 formuliert *Hassemer*: *„Wir brauchen ein neues Konzept des Datenschutzes. Dazu zwei Vorstellungen: Wir dürfen die Augen nicht davor verschließen, daß die Zeiten der Vorstellungen aus den siebziger Jahren vorbei sind (...). Die Vorstellung, daß wir einen Leviathan haben, einen zentralen Staat, welcher die Daten aller Bürger verarbeitet und deshalb auch so kontrolliert werden muß, ist nicht falsch (...). Aber sie ist nicht mehr die einzig richtige. Mittlerweile gibt es Datenverarbeitung von höchster Bedrohlichkeit (...) auch in privaten Händen (...).*

Als zweiten Punkt spricht *Hassemer* die zentralen, primären Probleme der Gesellschaft an: *„Verteilungsgerechtigkeit, Armut und gesellschaftlicher*

Reichtum". Wenn diese in den Hintergrund getreten sind, würden die tertiären und quartären Probleme wichtiger. Zu diesen tertiären Problemen zähle der Datenschutz.

3.3 Vergleich der Analysen

Vergleichen wir *Hassemers* Ausführungen mit dem Analyseraster und der Schlußfolgerung von *Simitis*:

1. Die *poröse rechtliche Infrastruktur* 1994 scheint sich dieser Punkt erledigt zu haben. Fast flächendeckende bereichspezifische Datenschutzgesetze machen neue Gesetze im großen und ganzen nicht mehr nötig. Alltagsarbeit ist angesagt.

2. Der *veränderte politische Kontext*. Hier schließen die Analysen beider Beauftragter nahtlos aneinander, mit einer etwas anderen Tendenz bei *Hassemer*. Die wirklich drängenden Probleme der Gesellschaft führen zunächst dazu, dem Datenschutz einen Platz in der zweiten Reihe zuzuweisen. Beide erkennen natürlich gleichermaßen, daß eine dramatisch veränderte gesellschaftliche Situation ein bestimmtes Konzept von Datenschutz obsolet machen kann.

3. Die *modifizierte technische Infrastruktur*. Natürlich hat kaum jemand geahnt, welche Dynamik sich durch die Vernetzung entwickelt hat. Davon abgesehen aber gleichen sich die Analysen aus dem Jahr 1984 und 1996.

Auch die Folgerungen, die die Beauftragten im Jahr 1984 und 12 Jahre später ziehen, sind fast bis aufs Wort identisch: Wir brauchen ein neues Konzept des Datenschutzes, schreiben sie beide. Faßt man die Analysen diverser Texte aus 12 Jahren zusammen, so weiß man, worauf aus der Sicht *hessischer Datenschutzbeauftragter* eine Antwort gefunden werden muß:

1. Die *ökonomische Situation* hat sich entscheidend geändert. Verteilungsgerechtigkeit und Armut sind die drängenden Fragen.

2. Die *technische Situation* hat sich, wie manche behaupten, sogar revolutionär verändert. Die verteilte und weltweit vernetzte Datenverarbeitung ist etwas anderes als die zentrale Datenverarbeitung.

3. Die *politische Situation*, die für den Datenschutz Modell gestanden hat, hat sich geradezu umgekehrt: Der Leviathan ist abhanden gekommen. War es in der Anfangszeit die Sorge vor dem zentralistischen Polizeistaat, versucht man heute den Staat als Bündnispartner gegen private Mächte zu gewinnen. Im engeren Bereich der Inneren Sicherheit geht es längst nicht mehr um die Abwesenheit von Polizei, sondern um deren Anwesenheit.

Man fragt sich natürlich, warum diese Autoren trotz ihres analytischen Weitblicks gleichsam stereotyp bei der Forderung nach einem neuen Datenschutzkonzept geblieben sind.

Simitis hatte unter der Überschrift „Die poröse rechtliche Infrastruktur“ vor allem bereichspezifische Gesetze gefordert. Schon für 1994 kann sein Nachfolger Entwarnung geben: Rechtsprogramm im wesentlichen erledigt, Datenschutz ist eine Sache der Praxis - nicht mehr und nicht weniger. Trotzdem zugleich und immer wieder die Forderung nach dem neuen Konzept. Dadurch machen die Beauftragten auf einen Widerspruch aufmerksam, den sie aber nicht offenlegen können oder wollen.

Ich behaupte, daß dieser Widerspruch im Volkszählungsurteil selbst angelegt ist: Die historische Leistung der Richter bestand darin, ein überkommenes Hauptfreiheitsrecht in einen Informationstatbestand umzudeuten und dadurch die informationelle Struktur moderner, technikgestützter Interessenkonflikte hervorzuheben.

Die Figur des informationellen Selbstbestimmungsrechts setzt auf der Einsicht in einen tiefgreifenden Wandel der überkommenen, im wesentlichen zu Beginn des 19. Jahrhunderts entstandenen Wissensordnung auf. Wenn heute mit unterschiedlicher Begründung entweder die juristische Figur selbst oder nur ihre praktische Umsetzung in diversen bereichspezifischen Gesetzen als dysfunktional bezeichnet wird, dann vor allem deshalb, weil das Gericht eine voraussehbare Fehlentwicklung nicht bedacht hat.

Die deutsche Rechtsordnung und mit ihr die in der Rechtswissenschaft und Rechtspraxis herrschende Meinung mußte auf den neuen informationellen Typus mit den überkommenen juristischen Instrumenten antworten, vor allem der Eingriffsdogmatik des öffentlichen Rechts, die sich in den Kämpfen zwischen Krone und Bürgertum im letzten Jahrhundert herausgebildet hat. Die in diesem Modell vorausgesetzte Arbeitsteilung zwischen dem Staat und seinen Institutionen, den Bürgern mit ihren Rechten und den im Rahmen der gemischten Wirtschaftsverfassung selbständig agierenden Marktkräften ist aber gerade durch den Kern der neuen Wissensordnung - die Technisierung des Wissens selbst in einem kognitiv-technischem Komplex - fragwürdig bis obsolet geworden.

Überspitzt könnte man also sagen, daß eine Figur des ausgehenden 20. Jahrhunderts - informationelle Selbstbestimmung - mit Instrumenten des 19. Jahrhunderts - bereichspezifische Gesetze - behandelt wurde.

Das Urteil hat also auch Fehlentwicklungen begünstigt oder gar hervorgerufen. Ich betone auch: Es liegt nun nicht auf der Hand, wie man diesen Befund in etwas münden läßt, was theoretisch und praktisch gleichermaßen überzeugt. Ich werde im nächsten Punkt einige konzeptionelle Überlegungen vorstellen, die langfristig weiterhelfen könnten. Eine wichtige Tugend scheint mir dabei vorgegeben:

Die Staatsfixiertheit des Datenschutzes mit seiner Konzentration auf Gesetze, rechtliche Regelungen und das Verhältnis Staat - Bürger muß aufgegeben werden.

Natürlich kann man das Orakel, mit dem sich *Simitis* 1984 an eine überwiegend staunende Öffentlichkeit gewandt hat, in verschiedene Richtungen deuten. Ich habe versucht, eine Denkrichtung herauszuarbeiten, die schon 1984 die problematischen Aspekte des Volkszählungsurteils hervorgekehrt hat. *Simitis* hat sie sicher nicht in seinen Einzelheiten gesehen, in seiner Praxis als Datenschutzbeauftragter hat er sogar häufig das Gegenteil getan. Aber - das macht die Güte eines Orakels aus - in seinen Überschriften, in seinem analytischen Bezugsrahmen ist das Scheitern des damals und heute geltenden Datenschutzkonzeptes bereits angelegt.

4. Regelungstypen und Problemverschiebungen

4.1 Die Datenschutzbeauftragten im Netz

Am 30. September 1997 habe ich die Webseiten der deutschen Datenschutzbeauftragten besucht. Neun Landesdatenschutzbeauftragte habe ich im Netz gefunden. Fünf Beauftragte strukturieren ihr Angebot mit nur geringen Abweichungen mit einem einfachen Informationsangebot (Adressen, Gesetze, Tätigkeitsberichte, Pressemitteilungen) wie der Hessische Beauftragte.[14] Ganz einfach macht es sich der Rheinland-Pfälzer Beauftragte. Er linkt zur Datenschutzseite der Berliner Humboldt-Universität zurück, über den ich seine Adresse erst gefunden habe.[15] Er gibt auch auf seiner Seite bekannt, daß E-Mail-Anfragen nicht beantwortet werden. Geradezu sprachlos macht die Seite, mit der der Thüringer Beauftragte auf sich aufmerksam macht. Die Seite ist zudem nicht verlinkt. Gewissermaßen außer Konkurrenz läuft der Berliner Beauftragte. Er bietet mit Abstand das breiteste und formal und inhaltlich am besten gestaltete Angebot aller Beauftragten.

Zusammengefaßt ergibt dies folgende Zahlen:
- 6 Beauftragte bieten ein teils karges, teils reichhaltiges Angebot,
- 2 Beauftragte bieten Seiten an, die Stoff für eine Satire bieten,
- 1 Beauftragter aus Schleswig-Holstein sei vorübergehend entschuldigt, weil er seine Seite neu aufbaut,
- 7 Landesdatenschutzbeauftragte sind überhaupt nicht im Netz präsent,
- 1 Bundesdatenschutzbeauftragter ist nicht im Internet.

Das ergibt summa summarum:
- 6 Treffer bei 17 möglichen.

Diese geringe Trefferzahl läßt verschiedene Schlüsse zu: Entweder handelt es sich bei der Präsenz im Netz um etwas Unwichtiges. Dann könnte die bessere Einsicht die Mehrzahl der Beauftragten zum Verzicht auf eher unnütze Arbeit geführt haben. Oder es handelt sich um etwas Wichtiges. Dann spricht eine Vermutung dafür, daß die Datenschutzbeauftragten in ihrer Mehrzahl den Anschluß an eine technische Entwicklung verloren haben.

[14] Bayern, Brandenburg, Hamburg, Saarland.
[15] Die Humboldt-Universität betreut die Web-Angebote der deutschen Rechtsfakultäten zum Thema Datenschutz, <http://www.rewi.hu-berlin.de/datenschutz, alle Verweise besichtigt am 15.10.1997>.

Auf dem Umweg der Klärung dieser Fragen könnte man Hinweise auf den Zustand des Datenschutzes überhaupt erhalten.

4.2 Ist das Internet wichtig?

Durchaus gewichtige Stimmen in den Industriestaaten sprechen dem Internet eine herausragende Bedeutung zu, manche wie *Präsident Clinton* sprechen gar von der Internet-Revolution.[16] Denn das Internet verändert die Art und Weise, wie wir Produkte und Dienstleistungen produzieren, fundamental. Ich bezweifele, ob es unter Ökonomen und ökonomisch bewanderten Politikern irgendwo in der Welt eine Stimme gibt, die das anders sieht. Gestritten wird unter Ökonomen lediglich darüber, wann und in welchen Sektoren die ökonomischen Effekte eintreten und wer von ihnen profitiert.

Rechtspolitisch und juristisch haben sich in den letzten Jahren zwei Auffassungen herausgebildet: Die *erste Auffassung* findet sich gern unter dem Motto „Das Internet ist kein rechtsfreier Raum" zusammen. Sie wird vertreten von Ministern der Bundesregierung,[17] dem wohl überwiegenden Teil der deutschen Rechtswissenschaft,[18] aber auch den Datenschutzbeauftragten. Der *Bundesdatenschutzbeauftragte* führt dazu in seinem 576 Seiten starken Bericht für 1995 und 1996 aus, er habe *„Löcher"* im *„Leitplankensystem an der Datenautobahn"* entdeckt und weiß zu berichten: *„Zur Zeit ist die Unsicherheit der Bürger gegenüber den neuen Informationstechnologien immer noch groß. Berichte über die „anarchischen" Zustände haben viele abgeschreckt."* [19]

Später verspricht der Datenschutzbeauftragte Abhilfe: *„Verkehrsregeln auf der Datenautobahn"* müssen her: *„Der bisher in den Datennetzen praktizierte Verhaltenskodex - die Netiquette - reicht heute als Regelungselement*

[16] The White House: A Framework for Global Electronic Commerce v. 01.07.1997 <http://www.whitehouse.gov/WH/Commerce/read.html, besichtigt am 05.08.1997>.
[17] Der Server des BMBF hält eine Presseerklärung bereit: „Rüttgers: Das Internet ist kein rechtsfreier Raum <http://www.bmbf.de/ archive/presse/presse96/pm092696.htm, besichtigt am 03.07.1997>.
[18] In neuesten Publikationen scheint sich die ehedem sehr starre Position der deutschen Juristen zu entkrampfen. Man vgl. z.B. Sieber: Kontrollmöglichkeiten zur Verhinderung rechtswidriger Inhalte in Computernetzen, CR 1997, 581 ff.; 653 ff. und Mayer, Recht und Cyberspace, in: Humboldt Forum Recht Nr. 3/1997 <http://www.rewi.hu-berlin.de/3-1997/ Drucktext. html, besichtigt am 09.11.1997>. Auch diese Stimmen scheuen jedoch die Konsequenzen, die amerikanische Autoren ziehen.
[19] BfD, 16. Tätigkeitsbericht, 1997, S. 30.

nicht mehr aus. Erpressungsversuche von Firmen im Cyberspace, das Sammeln von Daten über die Netzaktivitäten eines Nutzers und das Anbieten von Nutzerprofilen, das Anbieten von Kinderpornographie und das Auftauchen extremistischer Gewaltpropaganda machen deutlich, daß die Selbstregulierungskräfte der Netzgemeinde nicht mehr genügen." (S. 148)

Ähnlich äußert sich das „Budapest-Berlin-Memorandum der Internationalen Arbeitsgruppe für Datenschutz in der Telekommunikation am 19. November 1996.[20]

Für diese wohl in erster Linie metaphorische Sicht, die mal von der Datenautobahn, mal von der „weltweiten Megamaschine Internet"[21] spricht, ist das Netz eine technische Entität, in dem man mit Hilfe alter oder auch neuer Regeln für Ordnung zu sorgen hat. Wie selbstverständlich nimmt man an, daß der Datenschutz, mithin die Beauftragten, zu den benötigten Ordnungskräften gehört. So heißt es im Budapest-Berlin-Memorandum: *„Das Recht jedes Einzelnen, die Datenautobahn zu benutzen, ohne überwacht zu werden, sollte garantiert werden. Andererseits muß es im Hinblick auf die Nutzung personenbezogener Daten auf der Datenautobahn (...) („Leitplanken") geben."*[22]

Die *zweite Auffassung* betont die Eigenständigkeit des durch das Internet geschaffenen Raumes gegenüber der sonstigen, auch durch die Rechtsordnung gebildeten Welt. Ich scheue mich zur Kennzeichnung dieser Gegebenheit das Gegensatzpaar real-virtuell zu verwenden, weil die Beziehungen, die im Netz eingegangen werden, ja ihrerseits höchst real sind. Diese Auffassung wird vertreten von dem überwiegenden Teil der Bürgerrechtsbewegungen, die sich im Netz äußern, einem großen Teil der amerikanischen Rechtswissenschaft und ihnen folgend dem *Supreme Court der Vereinigten Staaten* und einer Reihe von amerikanischen Instanzgerichten.[23] In Deutschland hat diese Auffassung außerhalb des Netzes nur wenige Anhänger.

---

[20] Abgedruckt DuD 3/1997, 154 ff.
[21] TB des Berliner DSB 1996, 1997, S. 16 f.
[22] DuD 3/1997, 156 (unter 3).
[23] Aus der umfangreichen Literatur, die im Netz vor allem auch über die Online-Zeitschriften sehr gut zu verfolgen ist, vgl. nur Johnson/Post, Law and Borders. The Rise of Law in Cyberspace. <http://www.cli.org/X0025_LBFIN.html, besichtigt am 08.09.1997; Lessing: Reading the Constitution in Cyberspace. In: Cyberspace Law Papers Iss. 4, March 1997 <http://www.ssrn.com/cyberlaw/lawpapers.html, besichtigt am 08.09.1997>.

Der *Supreme Court* hat diese Auffassung so auf den Begriff gebracht: *„Das Internet ist ein einzigartiges und völlig neuartiges Medium für weltweite Kommunikation.“* (Übersetzung von mir) Das Internet sei nicht vergleichbar mit den alten Medien - Briefpost, Buch, Presse, Telefon und Fax, Foto, Film, Tonträger, Funk und Fernsehen.[24] Das Gericht lehnt es also ab, das Internet im Wege der Analogie zu bewerten und sagt damit, daß die alten Rechtsinstrumente für das neue Medium Internet überwiegend untauglich sind. Das Internet sei nichts anderes als freie Rede, die sich wie auf einem Marktplatz entfalten könne und müsse.

Ein technisches, ein rechtliches und ein politisches Argument sprechen dafür, diese Auffassung auch in Deutschland zu übernehmen:

Das technische Argument:

Das Internet ist von niemandem geplant worden. Keine hierarchische Instanz hat dafür oder dagegen gestimmt. Eine Vielzahl von Entscheidungen über Protokolle, Backbone-Netze und welche Sachverhalte auch immer hat zu der heutigen Struktur geführt. Anarchie hat dort nie geherrscht. Anarchie war es höchstens aus der Sicht von jemand, der Gestaltung nur aus der Sicht einer hierarchischen Instanz oder im Falle des Rechts aus der Sicht des Staates denken kann.

Es ist deshalb nachgerade abwegig, wenn es im Budapest-Berlin-Memorandum heißt: *„Das Internet kann als erste Stufe der sich entwickelnden Globalen Informations-Infrastruktur bezeichnet werden.“*[25] Auch die Datenautobahn, die der Bundesdatenschutzbeauftragte so forsch regulieren will, hat es nie gegeben und wird es nie geben. Das Internet ist in der Vergangenheit nicht von Regierungen geplant worden. Es wird auch in der Zukunft nicht von Regierungen geplant.

[24] Entscheidung in der Sache J. Reno v. American Civil Liberties Union e.a. v. 26.06.1997. <http://supct.law.cornell.edu/supct/html/96-511.ZO.html, besichtigt am 26.06.1997>. Inzwischen wird die Entscheidung auch in Deutschland gerne zitiert. Dabei wird zumeist übersehen, daß die tatsächlichen Feststellungen vom Gericht der Vorinstanz übernommen wurden. Die Instanzrichter haben nachgerade ein Lehrbuch des Internet´s für Juristen geschrieben. Man vgl. deshalb District Court for the Eastern District of Pennsilvania v. 11.06.1996, im Netz unter <http://aclu.org/court/cdadec.html, besichtigt am 30.07.1997>.

[25] DuD 3/1997, 154.

Das rechtliche Argument:

Das Gericht ist in eine naheliegende Falle nicht getappt. Würde man nämlich dem Satz „Das Internet ist kein rechtsfreier Raum“ zustimmen, müßte man die vorfindliche Rechtsordnung in den neuen Raum gleichsam hinüberklappen. Würde man das tun, würde das Recht wesentliche Effekte wieder zunichte machen, bzw. kaum jemand würde sich um das Recht kümmern, weil es überwiegend im Netz nicht durchsetzbar ist. Häufig sind auch rechtliche Regelungen gar nicht erforderlich, weil es wie im vom *Supreme Court* entschiedenen Fall technische Lösungen zur Lösung unerwünschter gesellschaftlicher Effekte gab.

Den Bürger, der nach der Behauptung des Bundesdatenschutzbeauftragten geschützt werden müsse, weil er Angst vor den „anarchischen Zuständen“ im Netz hat, gibt es nicht. Seriöse Meinungsumfragen aus 1997 weisen ihn und fast gleichwertig auch weibliche Nutzer als wohl informiert aus. Datenschutz steht nicht im Zentrum der Befürchtungen der Bürger, die im Netz arbeiten. An vorderster Stelle steht die Angst vor Zensur - in den USA nicht anders als in Europa.[26]

Das Urteil des *Supreme Courts* zwingt dazu, Teile von Welt noch einmal neu zu denken. Es enthält also eine Absage an die Bequemlichkeit - der Machthaber genauso wie der Bürger. Die Clinton-Administration hat auf diese Einsicht sehr schnell reagiert. Am 1. Juli 1997 stellte sie den Rahmen-

[26] Es gibt inzwischen zahlreiche Staistiken über die tatsächliche Nutzung von Internetdiensten und die Einstellung der Nutzer. Die vermutlich seriöseste Untersuchung erfolgt zweimal jährlich im Auftrag des W3-Konsortiums durch die Georgia Tech University. Bei der Befragung vom Mai 1997 sind 20.000 Nutzer in den USA, in geringerem Umfang auch in Europa, befragt worden. Die Ergebnisse stehen Online zur Verfügung unter <http://www.gvu.gatech.edu/user_surveys, besichtigt am 17.06.1997>.
„What do Netizens feel is the most important issue facing the Internet?“ hieß eine der Fragen vom Mai. „Censorship“ stand in den USA (34%) und in Europa (32%) mit Abstand an erster Stelle. „Privacy“ bekam in den USA den zweiten Rang, während die Europäer „Navigationsprobleme“ an die zweite Stelle gesetzt haben (17,4%). „Privacy“ hatte bei den Europäern einen deutlich geringeren Stellenwert (17,3%). Die Ergebnisse einer Befragung unter angeblich 16.403 deutschen WWW-Nutzern findet sich unter <http://www.w3b.de/>. Im 8. GVU-Report vom Dezember 1997 haben sich die Gewichte verschoben </survey-1997-10>: Privacy steht augenblicklich an erster Strelle der Besorgnisse der Amerikaner (30,49%), gefolgt von der Angst vor Zensur (24,18%). in Europa überwiegt noch die Angst vor Zensur, während die W3B-Umfrage für Deutschland Datenschutz deutlich an die erste Stelle der Besorgnisse setzt (35,8%, Zensur 6%).
Diese Zahlen beweisen sicher noch nichts. Sie sollten aber zur Vorsicht mahnen und eine öffentliche Instanz wie den BfD zu größerer Sorgfalt bei seinen Argumenten anspornen.

plan für „Electronic Commerce“ vor, der 5 Prinzipien aufstellt. Im vierten Prinzip von Electronic Commerce heißt es:

„Die Regierungen sollten die einzigartige Qualität des Internet anerkennen. Der explosive Erfolg des Internet hängt wesentlich zusammen mit seiner dezentralen Natur und der Tradition von „Bottom-up-Governance“. Demgemäß paßt wahrscheinlich für das Internet der Rahmen nicht, der in den letzten 60 Jahren für Telekommunikation, Radio und Fernsehen gebaut wurde.“ [27]

Das politische Argument

Die digitale Ökonomie stützt sich auf das Internet und das Internet stützt die digitale Ökonomie. Zahllose Akteure gestalten und entfalten dieses Gebilde in Myriaden von Einzelentscheidungen. Das Gebilde ist indifferent gegenüber der Geographie, der Zeit und gegenüber Grenzen,[28] und widersetzt sich den klassischen Instrumenten der politischen Steuerung. Der *Supreme Court* erkennt dieses Faktum an und ordnet es zugleich, indem es das Internet als normatives Gebilde erfaßt und begründet. Manche werden einwenden, da habe ein Gericht aus seiner Kultur heraus geurteilt. Mein Gegenargument lautet: Was hindert uns in dieser grenzenlosen Ökonomie, in der wir tagtäglich Waren aus allen Kontinenten kaufen, die Weisheit eines amerikanischen Urteils anzunehmen? Unsere Rechtsordnung meines Wissens nach nicht.

Der veränderte weltweite politische Kontext zwingt vor allem dazu, das Geschehen in der Welt unter Markt- und Wettbewerbsgesichtspunkten zu durchdenken, neu zu durchdenken. Manch einem wird schon beim Gedanken an eine solche Sicht ein Schauer über den Rücken laufen. Diese Personen sollten sich aber klar machen, daß wir seit langem schon unter einem solchen Gesichtspunkt regiert werden. Die Europäische Union ist bekanntlich in ihrer ersten Säule als Wettbewerbsgemeinschaft konzipiert, die erst durch den Amsterdamer Vertrag eine Art bürgerrechtlichen Überbau erhalten hat. Unter der Überschrift „Regieren ohne Regierung“ diskutiert man in

[27] Fußn. 167.
[28] Ruggiero: Charting the Trade of the Future. Towards a Borderless Economy. Rede vor der International Industrial Conference am 29.09.1997 in San Franzisko.
<http://www.wto.org/wto/new/press77.htm, besichtigt am 30.09.1997>. R. ist Präsident der WTO.

der europäischen Integrationsforschung seit längerem, durch welche Art von Verhalten Regieren bewirkt wird, nachdem es jedenfalls überwiegend nicht das Recht ist.[29]

4.2 Regulierungstypen

Die folgenden Überlegungen möchten eine solche Debatte anstoßen. Sie versuchen, technische, politische und rechtliche Argumente einem einheitlichen Rahmen zuzuordnen. Die Einzelheiten dieses Ansatzes sind noch im Fluß und entstammen einer laufenden Forschungsarbeit mit meinem Kollegen Kei Ishii, die Ende 1997 abgeschlossen sein soll.[30] Einen Überblick gibt die *Tabelle 2*, deren Ausgangspunkt eine empirische Fragestellung ist: Welche Typen von Regelungen werden von welchem Akteur gesetzt? Welche Typen von wesentlichen Problemen lassen sich aggregieren? Welche Typen verschieben sich und welche bleiben gleich? Relativ einfach dürften sich Antworten für die *Vertikale* in der Tabelle finden lassen.

Es ist eine vergleichsweise triviale Einsicht, daß neben dem klassischen Gesetz eine Reihe von andersartigen Regelungen Geltung beanspruchen. So waren im Datenschutz ursprünglich nur Gesetze vorhanden. Inzwischen gibt es zusätzlich Technologien, technische Produkte, diverse Regularien, die unter der Ebene von Gesetzen, Verhalten zu steuern vorgeben. Auch wenn sich einzelne dieser Konzepte zunehmender Beliebtheit erfreuen, wie etwa datenschutzfreundliche Technik[31] - Privacy Enhanced Technologies (PET) -, so ist doch über den Wirkungsmechanismus, vor allem über den jeweiligen Interessenhintergrund wissenschaftlich nur wenig gearbeitet worden. Die entsprechende Diskussion findet fast ausschließlich in den USA statt. Gelegentliche deutsche Ansätze sind sehr abstrakt und empirisch wenig gehaltvoll.[32]

---

[29] Eine hervorragende Übersicht über den Stand der Diskussion geben Jachtenfuchs/ Kohler-Koch, Regieren in dynamischen Mehrebenensystemen, in: dies. (Hrsg.), Europäische Integration. Opladen 1996, S. 15 ff. sowie Bulmer: The Governance of the European Union, Journal of Public Policy 4 (1995), S. 351 ff.

[30] Kei Ishii hat seine Vorstellungen in einem Vortrag, der auch die folgende Tabelle entnommen ist, näher ausgeführt: Netlaw & Netiquette, im Netz unter <http://ig.cs.tu-berlin.de/ki/003>

[31] Siehe dazu AK Technik der DSB, Datenschutzfreundliche Technologien, DuD 12/1997, 709 ff.; Entschließung der DSB, 54. Konferenz 1997, DuD 12/1997, 735.

[32] In den USA beteiligen sich vor allem auch solche Autoren an der Diskussion, die aus dem Urheberrecht kommen. Man vgl. Gillet/Kapor: The Self-Governing Internet. Coordination by design. Massachusetts Institute of Technology 1996 <http://ccs.mit.edu/CCWP197.html, besichtigt am 09.09.1997>; Littmann: Reforming Information Law in Copyrights Image.

In Deutschland viel zu wenig bekannt und diskutiert ist die Rubrik *Marktmechanismen* und der Aspekt der *Quersubventionierung*. Klassisch ist hierfür die Guilette-Strategie. Man verschenkt Rasierapparate, um Klingen zu verkaufen. Ähnlich könnte man beispielsweise mit dem Urheberrecht im Internet verfahren. Weil das Urheberrecht gar nicht oder nur beim größtem Kontrollaufwand durchzusetzen ist, verzichtet der Urheber auf seine Rechte und sucht Wege der Quersubventionierung. Bekanntes Beispiel ist die Firmenstrategie der Firma *Netscape*: Sie verschenkt den Browser, um mit Server-Software Geschäfte zu machen. Der Urheber verzichtet also auf den ökonomischen Ertrag seiner Urheberrechte, um so geschäftlich erfolgreich zu sein. Es ist eine Frage des terminologischen Geschmacks, ob man den Kern des verbliebenen Rechts noch Urheberrecht nennen sollte.

Sehr viel schwieriger sind die Typenprobleme, die sich auf der *Horizontalen* stellen. Ich gehe davon aus, daß diese Tabelle einige wesentliche Problemtypen des Internet identifiziert. Nach der Analyse einiger amerikanischer Gerichtsentscheidungen vermute ich, daß Datenschutz in den wesentlichen Problemtypen eine lediglich dienende Rolle spielt:

<http://www.msen.com//~litman/dayton.hztm, besichtigt am 19.02.1997>; Swire: Markets, Self-Regulation and Government Enforcement in the Protection of Personal Information <http://www.acs.ohio-state.edu/units/law/swire1/cyber.htm, besichtigt am 16.08.1997>; Varian. Economic Issues Facing the Internet. Paper v. 15.09.1996 <ftp://alfred.sims.berkeleey.edu/pub/Papers//econ-issues-internet.html, besichtigt am 10.08.1997>. Aus der deutschen Diskussion vgl. die Ergebnisse des Diskursprojektes der Deutschen Gesellschaft für Rechts- und Verwaltungsinformatik in Lutterbeck/Wilhelm: Rechtsgüterschutz in der Informationsgesellschaft. Bericht 1993/5 des Fachbereichs Informatik der TU Berlin 1993.

Regulierungs-typen / Gesellsch./ Rechtl. Problem	**Nationale Gesetze (incl. Supra-, internationale)**		**Markt-Mechanismen**	**Selbstregulierung**		**Technologien**	
	Rechtsvorschrif-ten	Case Law		Industrie/Stände	Andere	Methoden	Product
Datenschutz	Datenschutz-Richtlinie der Europäischen Union (1995) BDSG (Änderung zum Okt. 1999)	Volkszählungs-urteil (1983, BverfG)		Ethische Leitlinien der Gesellschaft für Informatik (1993) Platform for Privacy Preferences (P3) (des W3C)	`Netiquette`	Kryptograhie Open Profiling Standard (OPS)	Pretty Good Privacy
Urheberrecht	Nationale Copy-right-Gesetze Berner, Paris Konventionen WIPO-Übereink.	Feist v. Rual Telephone (1990, U.S. Su-preme Court)	Crossubsidiza-tion of intellec-tual property creation, for example via advertising			Digital Zertifi-cate Stega-nographie	
Domainnamen	Trademark laws			gTLD-MoU (global Top Leval Domain Memoran-dium of Understand-ing)			Alternic name.space
Zensur/ Freie Meinung-säuß./ Inhaltkontrolle	Communications Decency Act	ACLU v. Reno (1997 U.S. Supreme Court)		Freiwillige Selbst-kontrolle Multimediadienste (1997)		PICS (Platform for Internet Content Selection)	

Tabelle 2: Die „Types of Regulations“ © Kei Ishii & Lutterbeck; Stand 26.11.1997

Wollte man das Urheberrecht im Netz wirklich mit den klassischen staatlichen Instrumentarien durchsetzen, kommt man ohne einen staatlichen Kontrollapparat oder Urheberrechts-Management-Systeme nicht aus. Zählt man es zu seinen Rechten, anonym lesen zu dürfen, müßte das Urheberrechtsmanagement ohne personenbezogene Daten auskommen - was heute überwiegend noch nicht garantiert ist.[33] Das Hauptinteresse ist ein Interesse an Information. Datenschutz hat eine dienende, untergeordnete Funktion.

Der *Supreme Court* hatte in dem erwähnten Fall über die Gefahren einer Zensur im Internet zu entscheiden. Ein entsprechendes Gesetz hätte nur Sinn gemacht, wenn Alter und Identität potentieller Empfänger anstößigen Materials offenbart worden wären.[34] Schutz vor Zensur ist das Hauptinteresse. Datenschutz hat eine dienende, untergeordnete Funktion. Bei aller Ungenauigkeit dieser Analyse läßt sich eine Hypothese aufstellen:

Als Solitär, der einsam in der Landschaft steht, macht Datenschutz jedenfalls für das Internet keinen Sinn. Die Konflikte verlangen Abwägungen, z. B. zwischen Urheberrecht und Datenschutz, für die in den herkömmlichen Datenschutzkonzepten kein Raum ist.

In seiner Abschiedsrede spricht *Winfried Hassemer* von den primären Problemen einer Gesellschaft einerseits, von den tertiären oder quartären Problemen andererseits. Die *sekundären* Probleme übergeht er schamhaft. Ich bin davon überzeugt, daß die hier behandelten Typenprobleme der Horizontalen und Vertikalen, vor allem ihr Zusammenwirken auf ein mächtiges gesellschaftliches Problem verweisen. Ich bin gerne bereit, diese Probleme in den Bereich des Uneigentlichen, des Sekundären zu verweisen, wenn sie denn gelöst werden. Man wird abwarten müssen, welcher Platz dann noch für *Hassemers* tertiäre und quartäre Probleme offengehalten werden muß.

[33] Cohen: A Right to Read Anonymously: A Closer Look at „Copyright Management“ in Cyberspace, Cyberspace Law Papers, Iss. 7, August 12, 1997
<http://www.ssrn.com/cyberlaw/lawpaper.html, besichtigt am 05.09.1997>.

[34] Vgl. hierzu American Civil Liberties Union (ed): Fahrenheit 451.2: Is Cyberspace Burning? <http://www.aclu.org/issues/cyber/burning.html>; Lessing: Tyrrany in Cyberspace: The CDA was bad - but PICS may be worse, Cyber-Rights Iss. 5.07, July 1997 <http://wired.com/wired/5.07/cyber_rights.html, besichtigt am 16.08.1997>.

5. „Noch ist nichts verloren“

Drei unerbetene Ratschläge an die Datenschutzbeauftragten

Vielleicht habe ich in guter Absicht überzeichnet. Auch bei erneutem Nachdenken halte ich den Kern meiner Erwägungen für bedenkenswert:

Der deutsche Datenschutz, mit ihm ein Großteil der Datenschützer, hat den Anschluß an die technische und gesellschaftliche Entwicklung verloren.

Der deutsche Datenschutz hat es versäumt, konzeptionell über das Volkszählungsurteil hinaus zu denken. Deshalb kommt Datenschutz bei den Wünschen und Interessen der Bevölkerung nur noch als marginales Problem vor, und kaum einer außerhalb der kleinen Szene der Datenschützer glaubt noch daran, daß ausgerechnet der Datenschutz Motor für eine fortschrittliche Entwicklung der Informationsgesellschaft sein wird. Vor gut 20 Jahren war man Avantgarde. Heute ist man Beamter.

Dabei stehen die Chancen gut, verlorenes Terrain wieder gut zu machen: Durch den Vertrag von Amsterdam hat die Europäische Union eine Art grundrechtlichen Überbau erhalten, der ausfüllungsbedürftig ist.

Zu denken ist dabei gar nicht so sehr an den Datenschutz im engeren Sinne, sondern vielmehr an das Transparenzgebot des Art. 255 (ex 191a) EG-Vertrag. Damit wird das Freedom of Information-Prinzip geltendes europäisches Recht.

Endlich hat also der Datenschutz ein zwingendes rechtliches Argument zur Seite, konzeptionell eine Richtung anzusteuern, wie sie etwa in einigen modernen Datenschutzgesetzen von Quebec und Ungarn schon realisiert wurden: Datenschutz im engeren Sinne und Freedom of Information gehören zusammen.

Die europäische Integration könnte mit anderen Worten den lahm gewordenen Gaul wieder flott machen.

Die Tatsache, daß unter anderem die Bundesregierung in einer Erklärung zur Schlußakte hinhaltenden Widerstand gegen die Geltung des Transparenzprinzips angekündigt hat, läßt ahnen, welche Widerstände auf der Seite

des Bundes zu erwarten wären. Einen Vorgeschmack auf diese Diskussion in den Ländern gibt auch das Brandenburger Parlament, in dem gegenwärtig ein Gesetzentwurf zur Aktenöffentlichkeit behandelt wird.[35] Es wird vielleicht noch schwieriger werden als damals, als ein Datenschutzgesetz gegen die Interessen fast aller durchgesetzt werden mußte.

Bevor man vor dieser Kärneraufgabe zurückzuckt, seien die Alternativen nochmals zugespitzt genannt, die auf den deutschen Datenschutz zukommen: Der eine Weg weist in Richtung Bürokratie, die sich dann auch nicht scheut, Leitplanken für nicht existente Autobahnen anzuschaffen. Der andere Weg ist höchst unsicher: Es ist nicht einmal klar, ob es Datenschutzbeauftragte heutigen Typs künftig noch geben wird. Als früherer Mitarbeiter eines Datenschutzbeauftragten, der z. B. die erste Kontrolle durchgeführt hat, die je in Deutschland veranstaltet wurde, erlaube ich mir drei Ratschläge, wie man die Wegstrecke bewältigen könnte:

1. Datenschützer sollten wieder genauer zuhören.

Nicht jeder, der sich skeptisch zum heutigen Datenschutz äußert, ist auch sein Gegner. Man lese die Kontroverse zwischen Nitsch und Dronsch, die 1995 und 1996 in der Zeitschrift für Rechtspolitik zum Thema Datenschutz und Informationsgesellschaft stattgefunden hat. Zwei Autoren watschen sich bzw. den Datenschutz ab, statt Antworten auf die doch unbestrittenen konzeptionellen Probleme zu geben.[36]

[35] Gesetzentwurf der Landesregierung für ein Akteneinsichtsrechtsgesetz (AERG), LT-Drs. 2/4417 v. 05.09.1997; in Brandenburg ist ein solches Gesetz aufgrund der Landesverfassung erforderlich. Dazu Bleyl, DuD 1/1998. Die Chancen, daß ein entsprechendes Gesetz in Kraft tritt, sind daher groß. Demgegenüber dürften entsprechende Entwürfe in Berlin und dem Bund wenig Aussicht auf Erfolg haben, vgl. Gesetzentwurf zur Förderung der Informationsfreiheit im Land Berlin, LT-Drs. 13/1623 v. Mai 1997 und Entwurf eines Gesetzes zur Gewährleistung des freien Zugangs zu Informationen, BT-Drs. 13/8432 v. 22.07.1997; als vorläufig letztes Land der EU hat das Vereinigte Königreich begonnen, das FOI-Prinzip zu implementieren, vgl. White Paper „Your Right to Know. The Government's Proposals for a freedom of Information Act" v. 12.12.1997 <http://www.national-publishing.co.uk/ document/caboff/foi/contents.htm, besichtigt am 14.12.1997>.

[36] Vgl. Nitsch, ZRP 1995, 361 ff. und die Antwort von Dronsch, ZRP 1996, 206 ff.

2. Datenschützer sollten Fehler zugeben können.

Ich hatte *Roman Herzog* als einen der geistigen Großväter des modernen Datenschutzes vorgestellt. Ist eine solche Person glaubwürdig, wenn sie heute als Bundespräsident in der bekannten Adlon - Rede folgendes Beispiel für lähmende Rituale bringt: *„Wir streiten uns um die unwichtigen Dinge, um den wichtigen nicht ins Auge sehen zu müssen. Erinnert man sich heute noch an den Streit über die Volkszählung, der vor ein paar Jahren die ganze Nation in Wallung brachte?“*[37]

Ich gehe davon aus, daß *Herzog* seine Vergangenheit als Richter und Rechtswissenschaftler bei diesen Sätzen nicht ganz vergessen hat. Sollte man diese Sätze übergehen, weil sie aus dem politischen Interesse gefallen sind, das man gerade nicht teilt? Was hätte es für Konsequenzen, wenn Datenschützer sich eine solche Sicht zu eigen machten? Würde man sich etwas vergeben, wenn man gesellschaftspolitisch und auch juristisch nochmals über die Volkszählung nachdenkt?

3. Datenschützer sollten wieder neugierig sein.

Natürlich habe ich die Richterin *Loretta Preska* eingangs nicht umsonst hervorgehoben. Sie hat mir gewiß imponiert, in Wahrheit brauche ich sie vor allem für meinen Schlußakkord. Wer nicht neugierig ist, dem ist das Neue stets das Alte. Ich finde den Gedanken unerträglich, daß um uns herum eine friedliche Revolution im Gange ist und der Datenschutz in der staubigen Ecke steht.

[37]Herzog, Aufbruch ins 21. Jahrhundert. Rede des Bundespräsidenten in Berlin, in Bulletin des Presse- und Informationsamtes der Bundesregierung Nr. 33 v. 30.04.1997, S. 353 ff.

Bedeutungswandel des Datenschutzes im Übergang von der Industrie- zur Informationsgesellschaft

Rainer Pitschas

Ein altchinesischer Fluch geht dahin, einem anderen zu wünschen, „in interessanten Zeiten leben zu müssen“. Das bedeutet für den Betroffenen nichts anderes, als sich in der nächsten Zeit gefahrvollen und wechselnden Herausforderungen an die Sicherung der eigenen Existenz gegenübergestellt zu sehen.

Pars pro toto gilt dies auch für das Leben in der Informationsgesellschaft. In ihr sieht sich die informationelle Selbstbestimmung des Bürgers von neuem herausgefordert. Deshalb wird verstärkt der „Modernisierung und europäische(n) Harmonisierung des Datenschutzrechts“ das Wort geredet.[1] Fraglich scheint aber, ob dies der richtige Weg für die sich entfaltende Informationsgesellschaft sein kann. Denn deren Grundtypus wird durch den Umstand gekennzeichnet, daß in ihr ein explosionsartiges und technologisch ermöglichtes Wachstum der Kommunikationsmöglichkeiten und -bedürfnisse der Bürger und Institutionen festzustellen ist. Die Gründe hierfür sind vielgestaltig. Der Begriff der „Informationsgesellschaft“ steht jedenfalls für einen gesamtgesellschaftlichen und -staatlichen *Rationalisierungsprozeß weltweiter Natur* im Umgang mit Informationen. An ihm ist das Entstehen globaler Märkte ebenso maßgeblich beteiligt, wie die Entwicklung der technischen Zivilisation, die Individualisierung von Lebenslagen, der gesellschaftliche Wertewandel und die funktionale Differenzierung

[1] Dammann/Simitis, EG-Datenschutzrichtlinie. Kommentar, Baden-Baden 1997, S. 59.

der bürgerlichen Gesellschaft. Meine daran anschließende *These* ist, daß dieser Rationalisierungsvorgang künftig nach einer neuen Balance zwischen freiem Datenverkehr, staatlichem Datenschutzrecht und gesellschaftlichem Selbstschutz verlangt. Wir stehen vor einem *Paradigmawandel des Datenschutzrechts.*

I. Entwicklungslinien der „Informationsgesellschaft" und der Wandel der Staatsfunktionen

1. Evolution der informatisierten Gesellschaft

a) In der gegenwärtigen gesellschaftlichen Entwicklung, die wesentlich durch den wissenschaftlich-technischen Fortschritt geprägt ist, erweist sich gerade „Information" als der entscheidende Rohstoff für die Produktion von Wissen und als Treibstoff der Veränderung der Wissensordnung. Denn „Information" ist an sich belanglos; erst ihre Aggregation mit weiteren Informationen zu „Wissen" und dessen Verbindung mit Lernvorgängen, in denen Wissensnetze aufgebaut, umgeordnet oder erweitert werden, bildet den eigentlichen Kern der zivilisatorischen Evolution in der sog. Informationsgesellschaft. Zu recht ist deshalb darauf hingewiesen worden, daß der wachsende Verbund von Informationen aller Art und ohne Rücksicht auf Gewicht oder Wahrheit des Informationsgehalts zu einer neuen Informationsqualität, zur „Wissensverarbeitung" führt.[2] In deren Verlauf treten neue Denk- und Darstellungsformen eines datenerzeugenden und -nachfragenden Erkenntnisstils aufgrund beliebig möglicher Verknüpfungen durch den Einsatz von Informations- und Kommunikationstechnik (IuK-Technik) auf. Chipkarten und Internet verändern so unser Leben.

   Dadurch wandelt sich zugleich die *Rationalitätsstruktur* in der Gesellschaft: Eine datenzentrierte, auf den grenzüberschreitenden bzw. internationalen wissenschaftlich-technischen Diskurs und die Sofort-Kommunikation im ökonomischen Sektor festgelegte Problembe-

[2] Ladeur, Das Umweltrecht der Wissensgesellschaft, 1995; Spinner, Die Wissensordnung, Opladen 1994, S. 24 ff.

wältigung tritt in den Vordergrund. Formen virtueller Vergemeinschaftung werden erkennbar, in deren Folge es zu einer neuen Qualität der Informationsverarbeitung kommt. Der Einfluß von Telearbeit und Teleshopping, von Informations- und Kommunikationsdiensten aller Art entgrenzt zudem unser Verständnis von Raum, Zeit und Privatheit: Ehen werden im Fernsehen geschlossen, Liebesnächte in Talk-Shows abgehandelt. Was ist noch wirklich private Sphäre?

Es liegt nahe, diese Vorgänge als „Publifizierung" des Individuums und „Informatisierung" der Gesellschaft zu bezeichnen. In deren Folge prägt einerseits der Zusammenhang von marktwirtschaftlicher Produktivität, Globalisierung und Information die Informationsnotwendigkeiten in den Nationalstaaten bzw. deren kommunikativen Bedarf in supranationalen Gemeinschaften. Auf der anderen Seite avanciert die ruhelos innovative Informations- und Kommunikationstechnik (IuK-Technik) in ihrer Verknüpfung mit den „neuen Medien" zu einer Schlüsseltechnologie des gesellschaftlichen Fortschritts bzw. zur „Durchbruchstechnologie". Sie ermöglicht eine qualitativ und quantitativ entwickelte Informationsverarbeitung sowie eine intensivere Proliferation personenbezogener Daten.[3]

b) Wendet man dabei den Blick auf die Zunahme der Intensität und die Reichweite grenzüberschreitender Austausch- und Interaktionsbeziehungen - seien es informationswirtschaftliche Transaktionen, informationelle Austauschprozesse oder der grenzüberschreitende Austausch von Umweltinformationen -, so offenbart sich, daß Kommunikation für die wirtschaftliche und soziale Integration trans-, supra- und international unerläßlich ist. Dies gilt für die Entwicklung der Weltwirtschaft und globaler Märkte ebenso wie für das Funktionieren des Binnenmarktes in der Europäischen Union (EU) i. S. des Art. 7a EGV. Länder und Unternehmen erlangen etwa durch einen freien Datenverkehr weit umfassenderen Zugang zum Kapital als je zuvor. So findet beispielsweise China ebenso leicht Käufer in aller Welt für seine Anleihen wie Schweden. Dabei ist Transparenz unabdingbar. Wenn Unternehmen

[3] Steinmüller, Informationstechnologie und Gesellschaft, Darmstadt 1993, S. 307 ff.

und Staaten die Ziele der Aktionäre und Anleiheinhaber identifizieren und zeigen, wie sie erreicht werden, steigen ihre Chancen, weltweit das Vertrauen der Investoren zu gewinnen.

In diesem Prozeß werden Gewinner sofort sichtbar. Nicht anders ergeht es den Verlierern: Die Aktionäre von Microsoft und Intel können bestätigen, daß in den letzten sieben Jahren Vermögen in einem zuvor nicht dagewesenem Umfang geschaffen wurde. Bei Apple und Digital Equipement hingegen, einst Unternehmen mit Produkten höchster Qualität und größter Anhängerschaft, bewirkten inkonsistente Leistungen und willkürliche Kommunikation einen unbarmherzigen Wertverfall an den Aktienbörsen. Auch diese stehen selbst in einem weltweiten Informationszusammenhang. Zur höchst wichtigen Frage wird: Wie präsentiere ich einer jeweils als entscheidend erachteten Öffentlichkeit die Daten über die eigene Leistung und wie finde ich diejenigen Informationen, die für die Leistungserzeugung notwendig sind.

Diese Aufgabe ist risikoreich. Sie erfaßt Wirtschafts- und Sozialpartner gemeinsam und verträgt kaum Informationsschranken. Mehr noch: Zwischen *allen* am wirtschaftlichen und sozialen Leben Beteiligten führt die angestrebte sozio-ökonomische Kohärenz zur fortschreitenden Zunahme bereichsüberschreitender Ströme personenbezogener Daten im öffentlichen wie im privaten Sektor.

Einbezogen darin sind Staaten und deren Regierungen. Schnelle Reaktionen auf die wirtschaftlichen und sozialen Entwicklungen im Zuge einer stetigen Interaktion offenbaren dabei einen inneren Zusammenhang von Kommunikation, weltweiten Märkten und sozialer Demokratie: Die Vereinigten Staaten von Amerika, die noch vor 15 Jahren nicht daran dachten, ihr Haushaltsdefizit zu reduzieren oder Unternehmen zu ermutigen, die Wertsteigerungsprozesse stärker zu berücksichtigen, unterstützen nun im Zeichen eines „New Public Management“ kreative Anpassungsprozesse an den Markt - freilich auch damit einhergehende Konkurse und Massenentlassungen. Doch sonnen sich heute die USA im Ruhm niedriger Arbeitslosigkeit, niedriger Inflation und niedriger Zinsen. Frankreich dagegen, das die rohen Kräfte des freien Marktes nur widerwillig akzeptiert und sich bisweilen dagegen wehrt, hatte weniger

Glück: Das Ergebnis ist - wie in zahlreichen anderen europäischen Industriestaaten - eine deutlich zu hohe Arbeitslosigkeit.

c) Was folgt daraus für unser Thema? In einer *ersten Schicht* der Erkenntnis ergibt sich, daß ungehinderte Kommunikation sowie der freie Verkehr personenbezogener Daten für das Entstehen globaler Märkte und den effektiven Wettbewerb ebenso unerläßlich scheinen, wie diese im Zustand eines freien Handels den Wohlstand fördern und den umfassenden Informationsaustausch ermöglichen. Grenzenlose Kommunikation, freier Datenverkehr, offene Märkte und Demokratie sind auf diese Weise untrennbar miteinander verbunden.[4] Darüber hinaus und *zweitens* offenbart sich, daß im Informationszeitalter eine hohe Produktivität der Marktwirtschaft vor allem durch kreative Kommunikation und effiziente Informationsflüsse sicherzustellen ist. Die Gestaltung und Beherrschung von Informationsflüssen ist das Thema der Zukunft, nicht jedoch deren Unterbindung bzw. inflexible Kanalisierung durch weitere „Verrechtlichung" der Informationserhebung und -verarbeitung. Der „freie Datenverkehr" darf deshalb nur sehr bedingt aus Gründen des Datenschutzes beschränkt werden. Er ist vielmehr zukünftig mit dessen Hilfe zu fördern.

   Schließlich und *drittens* verblüfft die Geschwindigkeit, mit der Informationen zu denen gelangen, die am meisten zu gewinnen oder zu verlieren haben, sowie die Geschwindigkeit der (globalen) Reaktion auf jüngste Bekanntmachungen. Der Mikroprozessor bewirkt, was die Ultraschallgeschwindigkeit im Flugverkehr noch lange nicht erreicht hat. Jedes Ereignis zeitigt heute sofort Konsequenzen. Die Globalisierung erzeugt Informationen; deren freier Fluß ermöglicht die Globalisierung. Märkte werden auf diese Weise „informatisiert"; für Informationen entstehen „Märkte".

d) Besondere Erwähnung verdienen im Zusammenhang dieser Entwicklung das *Internet* sowie die multimedialen Informations- und Kommunikationsdienste als technische Zauberformeln der Zukunft. In

[4] Skeptisch Raulet, Neue Medien - Neue Öffentlichkeit?, in: Hoffmann-Riem/Vesting (Hrsg.), Perspektiven der Informationsgesellschaft, Baden-Baden 1995, S. 31 (44).

vielen Bereichen der globalen Marktwirtschaft wirkt sich das Internet bereits aus: Aktienmarktdaten, wie etwa die letzten Verkaufskurse, sind jedem, der über einen Internet-Zugang verfügt, ohne weiteres und meist kostenlos ebenso zugänglich wie zahllose andere Erkenntnisse. *Daten in Echtzeit* sind damit eines der Ergebnisse, die wir der Entwicklung der IuK-Technik verdanken. Ihr Fortschritt ermöglicht die Herausgabe von qualifizierten Informationen für wissenschaftliche, professionelle, soziale und betriebliche Werke und Informatiker sowie die Anwendung neuer Technologien als Instrument, um Effizienz und Effektivität der Kundenbeziehungen zu erhöhen. Zugleich bietet die datenschutzfreundliche Technikentwicklung dem Nutzer die Chance, selbst darüber zu entscheiden, welche seiner Daten er offenbaren und welche er geheimhalten will. Es ist keine Utopie, daß deshalb jeder Netzbürger sein eigener Datenschutzbeauftragter werden könnte.[5]

Freilich steht die IuK-Technik heute nicht mehr nur für sich im Wandel der Wissensordnung. Schon längst sind andere Techniken und Medien zur Informationserhebung, -verarbeitung und -verwendung hinzugetreten. Die Zusammenführung der dazugehörigen einzelnen Technologien und Anwendungen - informationstechnisch: Personalcomputer; kommunikationstechnisch: Telefon, Fax, Mobilfunk, e-mail; unterhaltungselektronisch: Rundfunk, Fernsehen, Video - kulminiert in der Bezeichnung „*Muldimedia*“. Wir verstehen darunter den Oberbegriff für neuartige Produkte und Dienste, denen die interaktive Verwendung von Medienformen auf der Basis der digitalen Technik zur gleichzeitigen Übertragung von Daten, Sprache und Bewegtbild gemeinsame Merkmale sind. Hinzu kommt die Fähigkeit der genannten Produkte und Dienste zur interaktiven Nutzung bzw. Integration sowie die Vernetzung als Möglichkeit des Zugangs zu allen weltweit gespeicherten Informationen. Insgesamt haben wir es mit einer sich experimentiell verändernden Welt der Datenverarbeitung, der digitalen Telekommunikation und der integrierten Medien zu tun.[6]

---

[5] In diesen Zusammenhängen zuletzt Simitis, Internet oder der entzauberte Mythos vom „freien Markt der Meinungen“, in: Freundesgabe für F. Kübler, 1997, S. 285 ff.

[6] Hochstein, NJW 1997, 2977 ff.; Salmony, Multimedia und Elektronische Medien: von der CD-Rom bis zum interaktiven Fernsehen, in: Müller/Kohl/Strauß (Hrsg.), Zukunftsperspektiven der digitalen Vernetzung, Heidelberg 1996, S. 307 ff.

Auf diese Weise entstehen *multimediale Kommunikationsnetze*, die uns in der modernen Zivilisation und vor allem zum ökonomischen Nutzen informationell und materiell miteinander verbinden. In bezug auf ihre Nutzung und Wirkung läßt sich die Reichweite, lassen sich die Grenzen des Datenschutzes vor allem im Privatsektor nicht mehr mit den bislang üblichen Mitteln bestimmen. Waren-, Arbeits- und Kapitalmärkte mutieren statt dessen zu *Informationsmärkten*, die den Datenverkehr als Gesamtheit von Kommunikationschancen den Prinzipien von Angebot und Nachfrage anstelle hoheitlicher Regulierung unterstellen wollen. Nicht zuletzt zeigt sich hier die Problematik eines überkommenen Datenschutzkonzepts, das sich auf den *Staat* als Informationspartner des Bürgers und den Einsatz seiner Machtmittel zu ihrem (Daten-)Schutz konzentriert hat. Demgegenüber tut nunmehr die Selbstorganisation dieses Schutzes not.

2. Freiheitsgewinn durch Kommunikationsverdichtung

Die mittlerweile auf diesem Fundament erreichte *Informationsvielfalt, -offenheit und Kommunikationsverdichtung* hat eine lange Geschichte. Sie beginnt mit der Installation des Telefonnetzes gegen Ende des vorigen Jahrhunderts und setzt sich fort mit der Ablösung der Kommunikationsnetze von den Verkehrsnetzen. Nicht mehr länger sind seither Information und Kommunikation an Boten, an die Kutsche oder an die Eisenbahn bzw. an die Nutzung der Flugzeuge gebunden. Vielmehr sind in den elektronischen Kommunikationsnetzen, die sich von den Verkehrsnetzen abgelöst haben, die Kommunikationschancen vom Faktor Zeit in der Raumüberwindung nahezu unabhängig geworden.

a) Die Konsequenz dessen ist, bezogen auf die Organisation des modernen Staates, eine wachsende *politische Dezentralisierung*. In einem Kommunikationsnetz sind nämlich alle Teilnehmer mit allen anderen Teilnehmern direkt umwegfrei verbunden. Die Zentralität des Kommunikationssystems verliert sich; mit der Ablösung der Kommunikation von raumgebundenen Verkehrsträgern nimmt die Dichte der Beziehungen, die Menschen und Institutionen zentralitätsfrei miteinander verbinden, sprunghaft zu. Damit läßt sich festhalten: In der Informationsgesellschaft kommt es nicht nur zu einem Wandel der Kommunikations-

geschwindigkeit, sondern auch zu verstärkter politischer Dezentralisierung („Regionalisierung“).

b) Auf deren Grundlage bewirken das Informationswachstum und die Kommunikationsverdichtung in den informationstechnisch hochintegrierten Gesellschaften zunehmende *Individualisierungsprozesse* unter gleichzeitiger Steigerung der Freiheitschancen und informationellen Selbstverantwortung für den einzelnen Bürger. Denn der technische Fortschritt erschwert den Aufbau und den Bestand totalitärer (staatlicher) Informationsmonopole. Aus diesem Grund konnte die noch im vorigen Jahrzehnt weltweit befürwortete Reform der Weltinformationsordnung i. S. einer partiellen Abschottung bestimmter Weltregionen von Informationen nicht gelingen. In der globalisierten Wissensgesellschaft überleben zudem nationale und supranationale Volkswirtschaften nur, wenn deren Trägern (Wissenschaftlern, Ingenieuren, Managern u. a. m.) der freie Zugang zu Quellen des Wissens gestattet ist. Der technische und wissenschaftliche Fortschritt erhöht zugleich als Medium der Beschleunigung die Diffusion von Informationen.

   Zu dem skizzierten *Freiheitsgewinn* rechnet ferner die Individualisierung der globalen Informationsgesellschaft i. S. einer wachsenden *personalen Nachfrage nach Informationen.* Diese richtet sich gegen den Staat, um die eigene Verantwortung situationsgerecht betätigen zu können, aber sie ist auch an die Informationsmärkte als Selbsteröffnung von Datenverkehr adressiert. Die Entwicklung der Informationsdienste und des „electronic commerce“ spiegelt diese *informationelle Selbststeuerung durch Informationsteilhabe* wider. Auch die Mikroelektronik trägt ihren Teil dazu bei. Denn die Möglichkeit, Informationen interaktiv auszutauschen und damit personale Kommunikation zu bewirken, nimmt mit dem Ausbau der IuK-Technik und der Entwicklung multimedialer Produkte und Dienste sprunghaft zu.

3. Einordnung in den Wandel der Staatsfunktionen

Der Drang zum selbstregulierten Datenverkehr in der globalisierten Informationsgesellschaft, die Zunahme an Individualität durch Information und Wissen sowie die Möglichkeit der politischen Dezentralisierung sind mäch-

tige Quellen des Freiheitsgewinns; sie führen aber auch zu gravierenden Veränderungen im *staatlichen Selbstverständnis*. Die Handlungsebene des Staates unterliegt dem Zwang zu struktureller Umgestaltung, zur Revision der Verwaltungsverfahren und zum Einbezug individuell-kognitiver wie motivationaler Verhaltensprozesse in die Entscheidungsbildung der Institutionen. Dies gilt sowohl für die Exekutive wie für die Legislative und ebenso für die Rechtsprechung. Informierte Bürger wollen auf allen Ebenen mitentscheiden; sie erwarten größere Felder informationell-gesellschaftlicher Selbststeuerung.

a) Mit dieser Konsequenz fügt sich der skizzierte Informatisierungsprozeß in den derzeitigen *Wandel der Staatsfunktionen* ein. Diesen kennzeichnet zum einen die wachsende *Subjektivierung der Institutionen*, zum anderen die *Verantwortungsdistanzierung* des spätmodernen Staates („schlanker Staat“).[7] Letztere meint die Rücknahme der staatlichen Aufgaben- und Verfahrensverantwortung unter gleichzeitiger Zuweisung zahlreicher Staatsaufgaben in die gesellschaftliche Zuständigkeit. Es kommt zu grundlegenden Veränderungen im Verhältnis von Staat und Gesellschaft durch eine neue Zuordnung von privater und öffentlicher Verantwortung („Verantwortungsteilung“). Unter dem Gesichtspunkt der Informationsgenerierung und -verteilung ist die signifikante Konsequenz dieser Entwicklung die „Privatisierung“ der Information auf seiten der Amtswalter und die „Vergesellschaftung“ hoheitlich erlangter Daten, wie etwa das Umweltinformationsrecht zeigt.[8]

b) Die Rückwirkungen dessen auf das Gefüge gewaltenbalancierter Informationsverantwortungen im Staat, auf das Gegenseitigkeitsverhältnis von Verwaltung und Verwaltungsgerichtsbarkeit ebenso wie auf das Beziehungsgeflecht zwischen dieser, der autonomen Verwaltung und der Gesetzgebungsfunktion lassen sich ferner als ein *Rationalisierungsprozeß der Staatsfunktionen* begreifen. Deren Veränderung bedeutet einerseits „Rationalisierung“, nämlich bewußte Anpassung ihrer

[7] Näher dazu Pitschas, Organisationsrecht als Steuerungsressource, in: Schmidt-Aßmann/Hoffmann-Riem (Hrsg.), Verwaltungsorganisationsrecht als Steuerungsressource, Baden-Baden 1997, S. 151 (158, 182 ff.).
[8] Meyer-Rutz, Das neue Umweltinformationsgesetz, Köln 1995.

Leistung bzw. Leistungsfähigkeit an gewandelte politische Ziele und Inhalte bzw. an gewandelte gesellschaftliche Kontextbedingungen wie jene des Übergangs zur Informationsgesellschaft.[9] Dieser Prozeß wird andererseits von einer internen Re-Strukturierung der Staatsfunktionen je für sich und im Verhältnis dieser zueinander begleitet. Ausdruck hierfür sind z. B. die gegenwärtige Verwaltungsmodernisierung, die „Ökonomisierung" der Justiz oder auch der Funktionswandel des Gesetzes.

Informationell bedeutet dies zunächst, daß nunmehr der Staat die Bürger verstärkt und anders informieren muß, damit diese die ihnen prinzipiell zugewachsene Eigenverantwortung auch tatsächlich wahrnehmen können. Die Diskussion hierüber verläuft sich allerdings im Widersinn einer Argumentation über den „präzeptoralen Staat".[10] Sie konzentriert sich zudem und irrigerweise auf das Problem der sog. Informationseingriffe, statt zu einer Weiterentwicklung des Grundrechtsverständnisses über die traditionelle Eingriffsabwehr hinaus zu finden.[11]

Weitere Konsequenzen aus den Informatisierungs- und Subjektivierungsphänomenen liegen sodann in der Veränderung der internen Organisation und Abläufe in den jeweiligen Staatsfunktionen, z. B. in der öffentlichen Verwaltung. So wird bereits jetzt das Internet zum Motor der Verwaltungsmodernisierung; die schon bestehenden Bürgerinformationssysteme erhalten eine neue Reichweite.[12] Auch Demokratie und Bürgerbeteiligung erhalten neue Impulse. Die Entwicklung mag, wie Projekte in den USA - z. B. die „electronic townmeetings" - zeigen, zur Vision einer „virtuellen Demokratie" führen. Mit anderen Worten erzeugt die informatisierte Gesellschaft neue Diskussions- und Entscheidungsformen im Rahmen der repräsentativen sowie unmittelbaren De-

[9] Siehe mit Bezug auf die IuK-Technik Pitschas, Verwaltung und Verwaltungsgerichtsbarkeit im staatlichen Modernisierungsprozeß, in: Blümel/Pitschas (Hrsg.), Verwaltungsverfahren und Verwaltungsprozeß im Wandel der Staatsfunktionen, Berlin 1997, S. 27 (49 f., 63). Reinermann, Verwaltungsinformatik und Verwaltungsreform, in: Informatik in Recht und Verwaltung, Heidelberg 1997, S. 80 (84 f.).

[10] Di Fabio, JZ 1993, 689 ff.

[11] Zur Kritik auch Albers, Zur Neukonzeption des grundrechtlichen „Daten"schutzes, in: Haratsch/Kugelmann/ Repkewitz (Hrsg.), Herausforderungen an das Recht der Informationsgesellschaft, Stuttgart u. a. 1996, S. 113 (123).

[12] Lenk/Brüggemeier/Hehmann/Willms; Bürgerinformationssysteme, Opladen 1990.

mokratie. Bürgernähe durch „elektronische Demokratie“ ist keine Zukunftsvision mehr.[13] Dagegen ist dem Verständnis behördlicher Kooperation und des Miteinanders von Staat und Gesellschaft als „informationelle Gewaltenteilung“ der Abschied zu geben.

4. Die „Informationsfunktion“ des kommunikativen Staates

Die Evolution der Informationsgesellschaft wirkt somit auf die politische Entwicklung und rechtliche Grundordnung des modernen Staates ein, die seine kompetenz- und funktionenteilige Organisation ausprägt. Im Grundsatz der Gewaltenteilung fand der moderne Verfassungsstaat hierfür und bislang das ihm angemessene Leitbild. Es ermöglichte ihm die notwendige Ausdifferenzierung und Zuordnung staatlicher Regelungs- sowie Entscheidungsfunktionen einschließlich der Verfahren von Gesetzgebung, Exekutive und Rechtsprechung. Weil und soweit der Grundsatz der Gewaltenteilung deren widerspruchsfreies Ineinandergreifen gewährleisten will, ist er zugleich als *Prinzip der Funktionengliederung* zu verstehen.

Die skizzierten dynamischen Entwicklungsperspektiven der Informationsgesellschaft erweitern das überkommene Funktionenschema. Sie fügen dem eine weitere Funktion, nämlich die *Informationsfunktion des Staates* hinzu. Diesen trifft eine zunehmende Verantwortung für die Informationsausstattung und innere Re-Orientierung der gesellschaftlichen Interaktions-, Kommunikations-, Unterrichtungs- und Entscheidungsprozesse. Dabei tritt der verantwortungsdistanzierte Staat nicht mehr nur und nicht einmal vorwiegend als Entscheidungsträger in unterschiedlichen Gewalten- bzw. Funktionenkonstellationen auf. Vielmehr und einerseits bietet er dem Bürger und den gesellschaftlichen Institutionen für deren Entscheidungen durch seine Informationen eine Orientierungshilfe und Handlungsentwürfe zur Auswahl in Situationen der Ungewißheit, die sich in der „Risikogesellschaft“ häufen.[14] Umgekehrt wird auch der Bürger im kommunikativen

[13] Zittel, Über die Demokratie in der vernetzten Gesellschaft. Das Internet als Medium politischer Kommunikation, in: Aus Politik und Zeitgeschichte, B 42/97, S. 23 ff.

[14] Zur „Risikoinformation“ als Steuerungsinstrument vgl. Di Fabio, Jus 1997, 1 ff.; Pitschas, Staatliches Management für Risikoinformation zwischen Recht auf informationelle Selbstbe-

Kontext seiner Entscheidungsverantwortung und der reindividualisierten Lebenslage selbst entscheiden wollen; aber er muß - um dazu in der Lage zu sein - erst über die Hintergründe und Grundlagen dieser von ihm zu treffenden Entscheidung informiert werden. So verlangt er nach dem *informierenden Staat*. Dieser soll mit ihm - dem einzelnen - und mit gesellschaftlichen Gruppen in einen informationsgesättigten *Dialog* eintreten. Dies geschieht zunehmend, wie das Wachstum der Beratungsnachfrage seitens der Bürger offenbart.

Der kommunikative Staat prägt deshalb eigene informationelle Strukturen und Steuerungswirkungen aus. Somit sollte von einer genuinen Informationsfunktion die Rede sein.

II. Verfassungsdirigierte staatliche Informationsvorsorge und Wissensordnung

1. Sozialstaatlich-grundrechtliche und demokratische Pflichtenstellung gegenüber privater Datenverarbeitung

Aus der entfalteten Perspektive der Informationsgesellschaft wird deutlich, wie die Kommunikationsverfassung des modernen Staates gegenüber einer verantwortungsbewußten und funktional differenzierten Gesellschaft einem noch kaum diskutierten Wandel unterliegt.

Dieser fußt auf *drei Entwicklungslinien*, nämlich auf dem informations- und medien-technologischen Fortschritt, auf der informationellen Selbstregulierung des informierten Bürgers und auf der Privatisierung der Informations- und Kommunikationsangebote („Informationsmärkte“).

Freilich stehen diese Veränderungen nicht außerhalb des Rechts. Schon wegen seiner *sozialstaatlichen* Verpflichtung zur Informationsvorsorge fällt dem kommunikativen Staat gegenüber Bürgern und privaten Institutionen eine gesteigerte Pflicht zu, Zugang und Teilhabe an Informationen über das

stimmung und gesetzlichem Kommunikationsvorbehalt, in: Hart, Privatrecht im "Risikostaat", 1997, S. 215 (238 ff.).

Gemeinwesen und die Vorgänge darin auch im „schlanken“ Staat zu ermöglichen sowie öffentliches Wissen zum Gemeingebrauch zur Verfügung zu stellen. Zugleich verlangen die *Grundrechte* und die *sozial- wie demokratiestaatlichen* Bindungen der öffentlichen Hand, daß die staatliche Kommunikationsverantwortung auf die neuartigen Informations- und Kommunikationsabhängigkeiten und -gefährdungen der Bürger rechtlich geordnet und angemessen reagiert. Dies bedingt eine veränderte Deutung der informationellen Selbstbestimmung.[15] In deren Konsequenz rückt der Datenverkehr im Privatsektor nunmehr in das Rampenlicht. Denn Information ist in Zukunft der entscheidende Faktor sowohl für die persönliche Lebensgestaltung als auch für die unternehmenswirtschaftliche Produktion. Die vernetzte Kommunikationswelt führt zu einem Bedeutungswandel von Datenfluß und Datenschutz.

2. Staatskommunikation und Wissensordnung als „Kernaufgaben“

Die Informationsfunktion des kommunikativen Staates verändert ferner dessen eigenen Aufgabenbestand. Früher wie heute wird der Verfassungsstaat zwar durch die Relativität der Staatsaufgaben geprägt: diese finden sich im Wandel der Verfassungen jeweils verringert oder vermehrt - und im übrigen ganz nach den gesellschaftlich-politischen Optionen der Zeit in den Rang staatlicher Aufgabenerfüllung erhoben. Denn insoweit sich der „moderne Staat“ als politische Organisation der Gesellschaft entwickelt hat, nimmt er werkzeughaften Charakter an. Er ist sich nie Selbstzweck, sondern er dient der Gesellschaft stets zur Sicherung elementarer Existenzbedingungen ihrer Mitglieder.

Dennoch läßt sich bei aller prinzipiellen *Offenheit der Staatsaufgaben* ein gewisser Kernbestand identifizieren, den jeder moderne Staat für sich als unveränderlich reklamieren muß. So unterliegt heute keinem Zweifel, daß u. a. die öffentliche Sicherheit zu den klassischen Hoheitsaufgaben ge-

[15] Bull, Der Schutz der informationellen Selbstbestimmung in der multimedialen Aera-Thesen zum Wandel des Datenschutzes, in: Hamburger Datenschutzhefte, 1997, S. 1.

hört.[16] Zukünftig müssen wir indessen auch *die Informationsversorgung der Gesellschaft* und deren *Wissensordnung* zu diesen Kernaufgaben des Staates zählen. Namentlich dort, wo grundrechtliche Schutzpflichten die staatliche Informationsvorsorge bedingen und die Informationsverantwortung des Staates im Privatsektor zur Entfaltung führen, werden *Staatskommunikation* und *Wissensordnung*[17] zum unerläßlichen Auftrag. Zugleich gilt es, dafür eine angemessene *Infrastruktur* zu entwickeln.

3. Das Beispiel des Umweltinformationsgesetzes

Wie diese informationelle Infrastruktur im Bereich der Staatskommunikation zu gestalten ist, zeigt das deutsche Umweltinformationsgesetz, das der Umsetzung der Richtlinien 90/313/EWG des Rates vom 7. Juni 1990 über den freien Zugang zu Informationen über die Umwelt (UIG) dient.[18] Die Richtlinie sieht ein Jedermanns-Recht auf Einsicht in die bei den Behörden vorliegenden umweltbezogenen Daten vor. Dadurch werden viele Begrenzungen der bisherigen Verwaltungsöffentlichkeit in der Bundesrepublik Deutschland aufgehoben. Denn die Richtlinie löst den Zugang zu Behördeninformationen über die Umwelt bzw. über Umweltvorhaben vom Bezug zum jeweiligen Verwaltungsverfahren; es gestaltet den Informationsanspruch des Bürgers als ein eigenständiges Recht aus.

Allgemeiner ausgedrückt, vermitteln die Richtlinie des Rates und mit ihr das deutsche Umweltinformationsgesetz zum freien Zugang zu Informationen über die Umwelt nicht nur ein Einsichtsrecht in behördliche Umweltakten. Vielmehr werden Kommunikation als ein Instrument und Öffentlichkeit als ein Forum der Zusammenführung öffentlicher und privater Umweltinteressen eingesetzt, wodurch erreicht werden soll, daß die Öffentlichkeit die kooperativen Willensbildungsprozesse staatlicher Umweltvor-

[16] Scholz, Staatliche Sicherheitsverantwortung zu Lasten Privater?, in: FS K. H. Friauf, Heidelberg 1996, S. 439 (444).
[17] Zu deren Verständnis und Reichweite näher Pitschas, Allgemeines Verwaltungsrecht als Teil der öffentlichen Informationsordnung, in: Hoffmann-Riem/Schmidt-Aßmann/Schuppert (Hrsg.), Reform des Allgemeinen Verwaltungsrechts. Grundfragen, Baden-Baden 1993, S. 219 (237., 244 ff.).
[18] Abl Nr. L 158/56 - 90/313/EWG.

sorge zwischen öffentlich-rechtlich organisierten und privaten Akteuren mittels des Austauschs und der Bewertung von Informationen stimuliert. Darin liegen eine prinzipielle Absage an die „geschlossene“ öffentliche Verwaltung in den Mitgliedstaaten der Europäischen Union und zugleich der Aufbruch zu „gläsernen“ Verwaltungen. Die in ihnen geborgenen Daten unterliegen prinzipiell individueller bzw. gesellschaftlicher Teilhabe. [19]

4. Rechtsstaatliches Bedingungsgefüge

Der Auf- und Ausbau einer derartigen *informationsrechtlichen Infrastruktur* umfaßt auch die Fortschreibung der rechtsstaatlichen Bedingungen für die Wahrnehmung der staatlichen Informationsfunktion. So bedarf es einerseits funktional-äquivalenter Sicherungen gegenüber einem Staatshandeln, das sich auf die dargestellte Informationsvorsorge der Gesellschaft einrichtet und ansatzweise auch bereits eingestellt hat. Schon längst gewinnen Informationsmaßnahmen als staatliches Lenkungsinstrument neue Qualität und neue Bedeutung. Sie entfalten sich als ein spezifischer Macht- und Einwirkungsfaktor auf die privaten Selbstgestaltungskräfte.

Auf der anderen Seite muß sich der Staat der privaten Datenverarbeitung verstärkt annehmen. Ausfluß dessen sind u. a. das Telekommunikationsgesetz von 1996 sowie das Informations- und Kommunikationsdienstegesetz vom 22.07.1997.[20]

5. Informations- und Kommunikationsverantwortung der öffentlichen Verwaltung

Die skizzierte normative Infrastrukturverantwortung verweist zugleich auf die öffentliche Verwaltung als Handlungssystem des „arbeitenden Staates“ (L. v. Stein). Denn zum einen spiegeln sich die Probleme im Privatsektor, die mit dem Aufbau und dem Betrieb einer (globalen) Informationrechts-

[19] Anders dagegen Giesen, DuD 10/1997, S. 588 ff.
[20] Telekommunikationsgesetz v. 25.07.1996 (BGBl I S. 1120); Informations- und Kommunikationsdienste-Gesetz v. 22.07.1997 (BGBl I S. 1870).

Infrastruktur zusammenhängen - Schutz der Privatsphäre, Schutz des geistigen Eigentums, universeller Zugang zu Informationsnetzen, Zugang zu Forschung und Entwicklung sowie zu neuen Märkten - auch in der Suche nach einem optimalen Einsatz der IuK-Technik im öffentlichen Sektor unter Berücksichtigung seiner Gemeinwohlbindung wider. Ein Beispiel hierfür bilden die rechtlichen und sonstigen Fragen der *Verschlüsselungstechnik*, die bei der Erkundung von personenbezogenen Daten durch die öffentliche Verwaltung - etwa der Überprüfung der e-mail-Kommunikation unter Bürgern - den Schutz der Privatsphäre sicherzustellen hat („Datensicherung“).[21] Gleiches gilt für den Zugang zu Informationen, über die der öffentliche Sektor u. a. in der *Risikoverwaltung* verfügt.[22] Überdies und andererseits beeinflußt der Aufbau und Betrieb einer weltweiten Informations-Struktur die weitere Entwicklung der trans-, supra- und internationalen Verwaltungsbeziehungen.

a) Die Bereitstellung entsprechender rechtlicher Normen zur Steuerung dieser informationsbezogenen Rechtsstrukturentwicklung ist Sache des *Gesetzgebers*. Er hat die staatliche Kommunikationsverantwortung zu konkretisieren und insoweit den Wesentlichkeitsvorbehalt einerseits sowie die Grundrechte andererseits zu beachten. Zugleich allerdings trifft die öffentliche Verwaltung eine spezifische eigene („autonome“) *Informationsverantwortung*, die über eine eigenständige Verfassungslegitimation verfügt.[23] Bei Wahrnehmung dieser Verantwortung ist die öffentliche Verwaltung über den Rohstoff „Information“ und seine Verarbeitung im Kontakt mit dem Bürger an bereichspezifische Kommunikations- und Interaktionslasten gebunden. Personenbezogene Leistungen etwa im Sozialbereich erfordern eine hohe Datendurchlässigkeit zwischen verschiedenen sozialen Sicherungssystemen. Darüber führt die Konstruktion eines Spannungsverhältnisses von Verbrechensbekämpfung und Datenschutz im Sozialamt („Sozialamt will Straftäter nicht verraten“) nur vordergründig hinweg.[24]

[21] Kelm/Kossakowski, DuD 4/1997, S. 192 ff.
[22] Zu eng Giesen (Fußn. 19), S. 588 ff.
[23] Diese Verantwortung (und Kompetenz) übersieht Albers (Fußn. 11), S. 121 ff.
[24] Zuletzt dazu Beckmann, ZFiS (Zeitschrift für Innere Sicherheit in Deutschland und Europa) 2/1997, S. 73 ff.

Kommunikation ist darüber hinaus nicht bloße Übertragung von Nachrichten oder Informationen; sie stellt vielmehr stets und zugleich *soziale Interaktion* dar. Darauf, daß diese auch tatsächlich zustandekommt, hat der kommunikative Staat in seiner Strukturgebung für die Verfahrensordnung der öffentlichen Verwaltung hinzuwirken. So hat der Gesetzgeber des Verfahrensrechts für die Sozialverwaltung beispielsweise den richtigen Weg eingeschlagen, wenn er in § 25 Abs. 2 SGB X vorsieht, in den Akten enthaltene Angaben über gesundheitliche Verhältnisse bei Akteneinsicht dem Verfahrensbeteiligten durch einen Arzt vermitteln zu lassen.

b) Die administrative Informations- und Kommunikationsverantwortung ist somit vielgestaltig. Sie gründet auf einem prozeduralen Verwaltungsverständnis, das die Koordination der Informationsversorgung ermöglicht, gleichzeitig aber dazu zwingt, die IuK-Technik sozialverträglich in die informations-technologisch gestützte Kommunikation einzubauen, ohne die Notwendigkeit einer integrierten EDV-Organisation zu übersehen. Diese wiederum erfüllt die Ansprüche rechtsstaatlicher Effizienz.

   Auf diesem Hintergrund lassen sich unterschiedliche Anwendungsfelder der *Verwaltungskommunikation* im öffentlichen Sektor identifizieren. Sie liegen beispielsweise im Bereich der *Informations- und Leitsysteme*, die in Gestalt von Bürger- und Stadtinformationen nicht nur Einheimischen, sondern auch Touristen zu einer besseren Orientierung im Gastland verhelfen. Geographische und Umweltinformationssysteme vernetzen komplexe Daten mit Raumbezug, während Wirtschaftsinformationssysteme regional und landesweit Gewerbeansiedlung und Wirtschaftsförderung dienen. Grenzüberschreitende berufliche Beratungs- und Berufsförderungssysteme unterstützen darüber hinaus die Beschäftigungspolitik der Staaten. Schließlich helfen Verkehrsinformationssysteme nicht allein Stadtplanern und Autofahrern, Feuerwehr und Polizei, sondern auch und vor allem bei der Entflechtung des Verkehrs.

   Der konsequente Einsatz der Steuerungsressource „Information“ betrifft darüber hinaus die *Effizienzsteigerung in der administrativen Leistungserbringung* und die verbesserte Kooperation mit dem Bürger/ Kunden. Dies gilt um so mehr, als wir uns heute im öffentlichen Sektor

mit der Notwendigkeit einer grundlegenden Verwaltungsmodernisierung auseinandersetzen müssen, die jedenfalls in den Industrienationen unter der griffigen Bezeichnung eines „New Public Management" internationale Zusammenhänge herstellt. Speziell der *IuK-Technik* kommt dabei eine besondere, wichtige Rolle zu. Sie kann dazu beitragen, durch Verbreitung und Koordination der Informationen in der öffentlichen Verwaltung hierarchische Denkweisen und bürokratische Verwaltungsmodelle durch ein anderes Denken und anderes Verwalten aufzubrechen. Der *Zwang*, die Produktivität innerhalb der Verwaltung und im Vergleich dieser mit der Unternehmenswirtschaft zu steigern sowie den wachsenden Anforderungen an Qualität und Schnelligkeit des Verwaltungshandelns bzw. -verfahrens zu genügen, wandelt sich mit der Verfügbarkeit der IuK-Technik zu einer Chance, vorhandene Rationalisierungsbedarfe nunmehr konsequent und ohne die Schranke einer datenabschottenden Organisationsstruktur ausschöpfen zu können.[25]

Dies gilt z. B. für die verbesserte Ansprechbarkeit der Verwaltung, multimediale Kontakte der Bürger mit den Sachbearbeitern im Rahmen einer dezentralisierten Ressourcenverantwortung, für die interaktive Antragsbearbeitung bis hin zum Aufbau elektronischer Ämter für den gebündelten Zugang zu vielen Dienstleistungen der Verwaltung. Immer zahlreicher werden deshalb sog. „Bürgerämter" und Servicecentren mit „front offices" und „back offices". Zugleich unterliegen die Strukturorganisation und die Geschäftsprozesse der öffentlichen Verwaltung im Zeichen der administrativen Informations- und Kommunikationsverantwortung prinzipiellen Veränderungen durch den Übergang zu einer „lernenden" Organisation und die „Entregelung" des Verwaltungsverfahrens bei gleichzeitiger Einrichtung von „Behörden-controlling" und einer „Verfahrensprivatisierung".

III. Perspektivenwechsel des Informationsrechts

1. Zwischenbilanz

[25] Hierzu und zum folgenden vgl. Reinermann, Verwaltungsentwicklung und Verwaltungsinformationssysteme, in: Lüder (Hrsg.), Fünfzig Jahre Hochschule für Verwaltungswissenschaften Speyer, Berlin 1997, S. 425 (432 ff.).

Resümieren wir die Knotenpunkte der bisherigen Argumentation: In der Entwicklung der Informationsgesellschaft verändert sich die Ausgangslage der bisherigen rechtlichen Steuerung des Informationshandelns durch den Staat bzw. Private und damit auch die Funktion des Datenschutzrechts: Multimediale Information öffnet dessen Zweckenge und -bindung; private Informationsmärkte entstehen und der Bürger drängt nach selbstregulierter Informationsgewinnung.

Dadurch verändert sich die Rolle des Staates in doppelter Weise. Im Hinblick auf das gewandelte Verhältnis der Staatsfunktionen zueinander und in bezug auf das staatliche Steuerungspotential prägen einerseits die wachsende politische Dezentralisierung im Wandel der Kommunikationsvorgänge, der Zugewinn an Freiheit seiner Bürger durch Verantwortungsübernahme und Eigeninformation sowie ausgreifende Individualisierungsprozesse die Verpflichtung zur staatlichen Informationsversorgung aus. Staatliche Informationstätigkeit wird zum hauptsächlichen Steuerungsinstrument. Die damit einhergehende Kommunikationsverdichtung in der Gesellschaft führt gleichzeitig zu einem wachsenden bürgerschaftlichen Engagement, dem höhere Ansprüche der Bürger an gesellschaftliche Selbststeuerung und unmittelbare Demokratie entsprechen.

Ordnet man in die Evolution der informatisierten Gesellschaft den skizzierten Wandel der Staatsfunktionen ein, so spielt eine besondere Rolle der gegenwärtige Übergang des Wohlfahrtsstaates zum „situativen“ Rechtsstaat und „distanzierten“ Sozialstaat. Die gesteigerte Informationsfunktion des kommunikativen Staates kennzeichnet diesen Übergang zur prinzipiell *bürgerschaftlichen Selbstorganisation*. Der Staat muß seinerseits künftig die Ausübung gesellschaftlicher Verantwortung „gewährleisten“ und die Bürger in den Stand versetzen, wohlinformiert ihre Eigenverantwortung nach Maßgabe der „Verantwortungsteilung“ auch tatsächlich wahrnehmen zu können. Zugleich treffen den „neuen Sozialstaat“ entsprechende Gewährleistungspflichten, die eine spezifische Verantwortung für Staatskommunikation und Datentransparenz erzeugen.

Im Zusammenhang dieser Verantwortung reift andererseits die Aufgabe des Staates heran, die gesellschaftlich erforderlichen Informations- und Kommunikationsdienstleistungen im Wege einer „Regulierung durch Selbst-

regulierung“ neu zu ordnen („Wissensordnung“). Die Verfügbarkeit, Erfassung und Nutzung von Informationen sowohl im Verhältnis Staat - Bürger als auch im Privatrecht sind dabei anderen normativen Verkehrsschutzanforderungen, als sie das bisherige Datenschutzkonzept vorsieht, nämlich einem selbstreguliertem Datenverkehr zu unterwerfen. Dessen Gewährleistung bildet eine staatliche „Kernaufgabe“ der Zukunft. In deren Bewältigung hat der Staat einerseits Informationsverfügbarkeit zu sichern. Maßgeblich hierfür sind zur Gewährleistung funktionsfähiger Informationsmärkte der Sozialstaatsgrundsatz sowie das Demokratie- und Rechtsstaatsprinzip. Beide drängen den Staat überdies, den einzelnen gegen die neuartigen Gefährdungen der freien Informationsgesellschaft, z. B. durch Staatskommunikation, durch Multimedia-Dienste und andere elektronische Dienstleistungen bzw. den Einsatz von Chipträgern und durch die gesellschaftliche Vermachtung individueller Selbstinformation zu schützen. Dabei sehen sich die Anforderungen des demokratischen Prinzips im modernen Verfassungsstaat oft - aber zu Unrecht - zurückgedrängt. Doch gilt heute mehr als je zuvor: Der Datenverkehrsschutz durch Wissensordnung darf auch im Privatsektor nicht zu einer interessengesteuerten Objektstellung der Bürger führen.

Flankierend hierzu entwickelt sich im rechtlichen Gehäuse verfassungsdirigierter Verantwortung für Staatskommunikation und privaten Datenverkehr die informationsrechtliche Infrastruktur der öffentlichen Verwaltung durch Ausgestaltung ihrer Programmfunktion, Organisations- und Verfahrensstrukturen sowie im Einsatz des geeigneten Personals. Ebenso konkretisiert sich zunehmend der Einfluß der Steuerungsressourcen „Information“ und „Informationstechnik“ auf die administrativen Geschäftsprozesse und die Strukturorganisation der Verwaltung.

2. Funktionswandel der informationellen Selbstbestimmung und des Datenschutzrechts

Multimediale Kommunikation, die zentrale Rolle der Informationsmärkte, ausgreifende Staatskommunikation sowie informationelle Selbststeuerung des Bürgers sind die vier leitbildhaften Entwicklungsdimensionen der künftigen Wissens- bzw. Informationsordnung. Ihre Entfaltung bedarf eines *einheitlichen Rechtskonzepts.*

Mit der Rechtsprechung des Bundesverfassungsgerichts zum Recht auf informationelle Selbstbestimmung[26] sieht sich freilich kein derartiges Konzept einer dimensionalen, selbstregulativen und zugleich rahmensetzenden „Informations- bzw. Wissensordnung“ vorgelegt. Denn die aus der verfassungsrechtlichen Garantie der informationellen Selbstbestimmung nach Ansicht des Bundesverfassungsgerichts folgende Befugnis des einzelnen, grundsätzlich selbst zu entscheiden, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden, wird als spezielles Eigentumsgrundrecht der Information und Kommunikation formuliert, das in der Informationsgesellschaft die Wirklichkeit verfehlt. Zudem qualifiziert diese Ansicht jedwede Ausübung staatlicher Informationskompetenz als einen *potentiellen Freiheitseingriff*. Auch diese Position bedarf im Licht der zuvor ausgeführten Entwicklungslinien der Informationsgesellschaft einer umfassenden Revision. Denn zum einen sind Datenerhebung und -verwendung nicht mehr per se freiheitsgefährdend, sondern ihnen wohnt statt dessen ein *potentieller Freiheitsnutzen* inne. Dem widerspricht die im gegenwärtigen Datenschutzkonzept angelegte „Gefährdungshaftung“ für Informationsverarbeitung ebenso wie zum anderen die funktional begrenzte Zulässigkeit der Informationsverarbeitung in der öffentlichen Verwaltung aufzugeben ist.

Erforderlich wird mit anderen Worten die Neuinterpretation des Rechts auf informationelle Selbstbestimmung unter den Bedingungen der Informationsgesellschaft. Inmitten dieses Paradigmawandels ist zugleich die Neukonzeption des Datenschutzrechts i. S. eines Datenverkehrsrechts aufgegeben. Dabei sollte sich die künftige normative Organisation der Kommunikation an den bestehenden multimedialen, telekommunikativen und informationsglobalen Realstrukturen des Rechtsverkehrs ausrichten. Es geht mithin um die Entwicklung eines neuen verfassungsrechtlichen Strukturkonzeptes der *informationellen Selbststeuerung* in Verbindung mit der Informationsfreiheit und dem Recht des einzelnen auf Information, dem eine staatliche Informationspflicht entspricht. Hinzu tritt für den Privatsektor der verfassungsrechtlich gewährleistete Anspruch des Marktbürgers auf grundrechtsgemäße Wissensordnung unter Berücksichtigung der Kosten von Informa-

[26] BVerfGE 65, 1; 67, 100; 76, 363; 77, 1; 77, 121; 80, 367; 84, 192; 84, 239; 92, 191.

tion und Datentransparenz. Vertragsrecht, Wettbewerbsrecht, Urheberrecht, Internationales Privatrecht, aber auch das Strafrecht und das Völkerrecht strukturieren dabei die Wissenszurechnung und den Informationsschutz i. S. einer international-, straf- und bürgerlich-rechtlichen „Auffangordnung".

Schutzrechte für den einzelnen lassen sich in dieses rechtliche Netzwerk einfügen - wie etwa bei Bild- und Tonaufzeichnungen oder bei der Video-Überwachung -, doch sollten solche Regulierungen immer daran orientiert werden, daß sie die Ziele des freien Wettbewerbs unterstützen. Auferlegte Informationsverzichte können einerseits ökonomisch ebenso belastend sein wie z. B. zu hohe Sozialabgaben. Dabei kommt es jeweils auf die Schutzbereiche an. Andererseits und zugleich bietet der präventive Zivilrechtsschutz ein maßgebliches Ordnungsmuster für den Datenverkehr an.[27]

Mit Blick hierauf fällt es schwer, das überkommene öffentlich-rechtliche Datenschutzrecht als künftigen „Wegweiser" in die selbstregulierte Informationsgesellschaft anzusehen. Vielmehr besteht unabweisbarer Bedarf nach einem umfassenderen und steuerungsspezifischen *Informationsrecht*, in das die einzelnen Rechtsgebiete einfließen und dessen sowohl der öffentliche als auch der private Sektor in Gestalt einer übergreifenden Konzeption bedürften.

3. Öffentliches und privates Informationsrecht

Die Entwicklung dieses Informationsrechts steht zu allererst und immer häufiger vor der Schwierigkeit, Informationshandeln dem Privatrecht *oder* öffentlichen Recht zuzuweisen. Diese Zuordnung ist zwar dann unproblematisch, wenn eine Behörde informiert und damit öffentliche Aufgaben - solche der Gefahrenabwehr, der Risikovorsorge, der Gesundheitsfürsorge u. a. m. - erfüllt. Entscheidend ist dabei der Zusammenhang mit dem Zweck, dem die Information dient. Berät, belehrt, handelt andererseits eine Privatperson, ohne in Verwaltungspartnerschaft zur öffentlichen Aufgabenwahrnehmung befugt zu sein, so gilt selbstredend das Zivilrecht. Diese

[27] Dazu statt aller Möllers, Rechtsgüterschutz im Umwelt- und Haftungsrecht, Tübingen 1996.

hergebrachte Trennlinie verliert allerdings dort an Kontur, wo sich - wie in der „Verwaltungsmodernisierung“ - hoheitliche und private Informationsakteure durchmischen. Jedenfalls erweist sich die Grenzziehung zwischen öffentlichem Recht und Privatrecht in dem Maße als problematisch, in dem - wie gegenwärtig zunehmend - die öffentliche Gewalt gesellschaftliche Kräfte mit einer an sich öffentlichen Aufgabenerfüllung betraut, die selbständiges Informationshandeln umfaßt.

Vor diesem Hintergrund, der letztlich die Privatrechtsordnung bei allfälligen Informationskonflikten als hilfreiche Auffangordnung beruft[28], spricht einiges für die *Vereinheitlichung des Informationsrechts.* Auch die bisherigen Regelungen des Bundesdatenschutzrechts für den öffentlichen und den privaten Bereich sollten darin zusammengeführt werden.

4. Informationsverwaltungsrecht

Die öffentlich-rechtlichen Bezüge des Verwaltungshandelns finden im *Informationsverwaltungsrecht* als einen der Tragpfeiler des Informationsrechts ihren zentralen Platz. Sein Allgemeiner Teil formuliert Grundzüge, während das Besondere Verwaltungsrecht eine beträchtliche Zahl gesetzlicher Ermächtigungen für gezielte Informationsakte - insbesondere für Warnungen - bereithält, wie sich etwa aus dem Gerätesicherheitsgesetz oder aus dem Arzneimittelgesetz und künftig aus dem Umweltgesetzbuch ergibt. In neuerer Zeit sind bereichspezifische Datenschutzregelungen bei Multimedia und Telekommunikation hinzugetreten. Diese *Steuerungsfunktion* des Informationsverwaltungsrechts verbindet sich einerseits mit dem Informationsverfassungsrecht, wie es das Grundgesetz im Rahmen seiner Kommunikationsverfassung bereithält. Hierzu rechnen u. a. Art. 2, 5 und 8 GG als spezielle Kommunikationsgrundrechte sowie Art. 9 Abs. 3, 12 und 14 GG als Träger staatlicher Grundverantwortung für Wirtschaftskommunikation. Art. 20 GG stößt mit der rechtsstaatlichen Verpflichtung der Behörden zu objektiv wahrer, sachlicher und neutraler Information hinzu.[29] Auf der anderen Seite umschließt das Informationsverwaltungsrecht das aufgefä-

[28] Dazu näher Pitschas (Fußn. 14), S. 228 ff.
[29] Zu eng dagegen Albers (Fußn. 11), S. 121 ff.

cherte *Datenschutzrecht*, dessen *Schutzfunktion* zugunsten personenbezogener Daten aktiviert wird.

Darüber hinaus umfaßt das Informationsverwaltungsrecht spezifische Regelungsmuster für die kontinuierliche und anlaßbezogene *Risikokommunikation* zwischen Verwaltung, Bürger und Unternehmenswirtschaft. Dies ist z. B. im Gentechnikrecht, im Chemikalienrecht, aber auch im Atomrecht und im Immissionsschutzrecht der Fall. In den genannten Rechtsgebieten finden wir unterschiedliche Bauformen einer öffentlich-rechtlich regulierten Risikokommunikation.[30]

Informationsverwaltungsrecht als öffentliches Informations- und Kommunikationsrecht folgt dabei in seiner Geltung zwar nach wie vor *rechtsstaatlichen Grundbedingungen.* Dazu gehört das verfassungsrechtliche Verantwortungsprinzip, das auch im Informationssektor staatlich organisierte Unverantwortlichkeit und Freistellung von Kontrolle („Immunität") ausschließt. Statt dessen dürfen staatliche Stellen nur im Rahmen der ihnen gesetzlich zugewiesenen Aufgabenstellung handeln, Informationen erheben, verarbeiten oder weiterleiten. Dies sicherzustellen, bedingt den Ausweis von Zurechnung der Geschäftsprozesse ad personam und eine entsprechende Verantwortlichkeit des Amtswalters. Dementsprechend wird bei der Rechtskontrolle hoheitlicher Informationsakte gerade Zuständigkeitsfragen ein grundsätzlicher Rang zuzuweisen sein. Es besteht eine persönliche Verantwortlichkeit für rechtmäßiges Handeln. Ich habe deshalb Zweifel an dem (europa-)verfassungsrechtlichen Bestand der Europol-Konvention, insofern diese die Informationsarbeit der Behörde einer solchen Verantwortlichkeit durch Immunitätsgewähr entzieht. Dagegen ist die akustische Wohnraumüberwachung („Lauschangriff") verfassungsgemäß.

Freilich sind solche informationellen Einwirkungen der Verwaltung auf die Gesellschaft immer bereichspezifisch und anhand ihrer Zielsetzung bzw. Wirkung zu gewichten. Deshalb sind etwa die automatisierten und pauschalierten Datenübermittlungs- und Datenabgleichsverfahren im Gesundheits- und Sozialrecht anders zu beurteilen als die gezielte Informationslenkung

[30] Pitschas, Öffentlich-rechtliche Risikokommunikation, UTR 36 (1996), S. 175 ff.

zur Verhaltensbeeinflussung im Rahmen des Verbraucherschutzes. Auch diese rechnet zu dem Arsenal administrativer Handlungsformen. Dahinstehen mag hier, ob sie einen staatlichen Informationseingriff darstellt, so daß in Bezug hierauf die Wahrnehmung einer gesetzlich verankerten Verwaltungskompetenz gegeben sein muß. Jedenfalls darf der Verweis auf *grundrechtliche Schutzpflichten* die Kompetenzordnung nicht aushebeln.

5. Funktionale Irritationen

Allerdings macht die voraufgehende Differenzierung unter den Informationsakten der öffentlichen Verwaltung bereits deutlich, daß auch im Informationsrecht das herkömmliche Eingriffs- und Zuständigkeitsdenken in bezug auf die rechtliche Zulässigkeit staatlichen Handelns fragwürdig geworden ist. Vor allem aber gibt die Entwicklung moderner Technologien Anlaß, die eigentumsanaloge und individualisierende Schutzkonzeption des bisherigen Datenschutzrechts zu „öffnen".[31]

Meine *These* hierzu ist, daß Notwendigkeit und Grenzen des Schutzes personenbezogener Informationen rechtlich künftig nach anderen Prinzipien zu bestimmen und entgegen dem bisherigen Verständnis des Rechts auf informationelle Selbstbestimmung zu verorten sind. Verantwortlich hierfür zeichnen die oben dargestellten leitbildhaften Entwicklungsdimensionen der Informationsgesellschaft. Für ihre rechtliche Konkretisierung ist auch das „Abwägungsprinzip" des europäischen Datenschutzrechts von Belang. Besondere Berücksichtigung im Aufbruch des Informationsverwaltungsrechts zu neuen Ufern müssen ferner das „Recht der Informationstechnik" und das „Recht der Datensicherung" finden.

[31] Vgl. auch Albers, (Fußn. 11), S. 119, 123; Wolf, KritJ 1995, S. 340 ff.; P. Kirchhof, HdBStR IX, Heidelberg 1997, § 221 Rdnr. 131.

IV. Verständniswandel des Rechts auf informationelle Selbstbestimmung

1. Informationelle Selbstbestimmung als Rezipientenfreiheit

Im bisherigen rechtsstaatlichen Verständnis setzt der individualisierte *Gesetzesvorbehalt* als „Eingriffsvorbehalt“ einer ausgreifenden Staatskommunikation enge Grenzen. Es dominiert die abwehrrechtliche Perspektive des Rechts auf informationelle Selbstbestimmung. Dieser Beschränkung gegenüber ist jedoch darauf hinzuweisen, daß die überkommenen eingriffs- und vorbehaltsorientierten Grenzziehungen hoheitlicher Informationsverarbeitung dem hier nachgezeichneten Übergang zu massenhafter Nutzung der neuen Medien und Telekommunikationsdienste nicht mehr gerecht werden. Die Entfaltung grundrechtlicher Schutzgüter in eigener, personaler Verantwortung auf der Grundlage der zur Individualisierung und politischen Dezentralisierung erforderlichen Daten sowie in Abgrenzung zu den Schutzinteressen Dritter erfordert nunmehr den Wechsel zu einer teilhabeorientierten Betrachtung. Die Grenzlinien zwischen „Eingriff“ und „Kommunikation“ sind in Bezug auf die Verwaltung und den Privatsektor neu zu ziehen.

a) Dabei kommt es zu einem *Gestaltwandel des Rechts auf informationelle Selbstbestimmung*. In seiner Ausprägung durch die informationsverfassungsrechtliche Rechtsprechung darf es nicht länger allein als ein Abwehrrecht mißverstanden werden. Vielmehr stellt es eine objektive und teilhaberechtliche Norm dar, die den Geltungsbereich der bisherigen Kommunikationsverfassung des Grundgesetzes ausweitet. *Informationelle Selbstbestimmung* will in diesem Sinne nicht mehr nur garantieren, daß Informationen über den einzelnen nur dann erhoben und verarbeitet werden, wenn dieser davon weiß und damit einverstanden ist; *informationelle Selbstbestimmung* will vielmehr auch und zugleich den freien Informationsfluß von Staat und Verwaltung in die Gesellschaft hinein und innerhalb dieser ebenso sichern wie die Teilhabe der Bürger an Informationen und den freien Zugang zu ihnen, ferner deren freie Verwendung bzw. Umsetzung in selbstverantwortete Entscheidungen. Der einzelne soll selbst über das Datenschutzniveau entscheiden kön-

nen; ihm bleibt eine *Option*. Das informationelle Selbstbestimmungsrecht garantiert die *Rezipientenfreiheit*.[32]

Daraus folgt: Datenverarbeitung sollte nicht als potentieller Freiheitseingriff mißverstanden werden. Dem Gedanken, es gäbe eine eigentumsgleiche „Herrschaft" über Daten und in bezug auf sie entstehe gleichsam eine „Gefährdungshaftung" des Staates, der den Verarbeitungsprozeß initiiert habe und dadurch in die Sphäre informationeller Selbstbestimmung über- und/oder eingreife, ist der Abschied zu geben. Statt dessen verbindet sich das Recht auf informationelle Selbstbestimmung mit dem Allgemeinen Persönlichkeitsrecht (Art. 2 Abs. 1 GG) sowie mit dem Grundrecht der Informationsfreiheit und dem Recht auf freie Meinungsäußerung (Art. 5 Abs. 1 Satz 1 GG) objektiv- und teilhaberrechtlich zu einer *informationsverfassungsrechtlichen Wirkgesamtheit*, die über die gegenwärtige Ausdeutung des informationellen Selbstbestimmungsrechts als verfassungsrechtsdogmatisches Abwehrzentrum gegenüber ungehinderter Datenerhebung und -verwendung hinausgeht sowie zugleich die Garantie der Informationsfreiheit erweitert.

Diese (neue) Wirkgesamtheit umfaßt sowohl das Recht des Bürgers auf Informationen über Sicherheit vor Risiken wie seinen Anspruch auf Unterrichtung und Kommunikation zur eigenbestimmten Gefahren- bzw. Risikoabwehr, schließlich auch als Verbraucher das Recht auf selbstbestimmte Entscheidung auf der Grundlage entsprechender Informationen. Dem entgegenstehende personenbezogene Daten öffnen sich der Erhebung und Verwertung; in der vernetzten Kommunikationswelt müssen die Kommunikationspartner beobachten und sich informieren dürfen.[33]

[32] Zu alledem im Ansatz bereits Pitschas, Verfassungsrechtliche Spielräume des Gesetzgebers für Informationseingriffe und andere Maßnahmen der Verbrechensbekämpfung, in: Polizeiführungsakademie (Hrsg.), 10 Jahre nach dem Volkszählungsurteil des Bundesverfassungsgerichts, Münster 1994, S. 53 ff.

[33] Bull (Fußn. 15), S. 2; Kirchhof (Fußn. 31), Rdnr. 131.

2. Strukturkonzept der informationellen Selbststeuerung

In dieser Formung gibt das Grundgesetz ein bislang verborgenes *Strukturkonzept der informationellen Selbststeuerung* zu erkennen. Tragpfeiler dieses Konzepts ist vor allem das Allgemeine Persönlichkeitsrecht nach Art. 2 Abs. 1 GG, das sich ebenso dem Recht auf informationelle Selbstbestimmung als Eckpfeiler einer Ausgleichsordnung für den Gesamtkonflikt zwischen staatlicher Kommunikationsverantwortung, dem gesellschaftlichen Informationsbedarf und individuellem Nutzen von Informationen öffnet, wie es für den Schutz der personalen Rechtsgüterverantwortung auch das „Recht auf Wissen" des Individuums als ein Segment in seinen Schutzauftrag einbezieht.[34]

Die grundgesetzliche Kommunikationsverfassung prägt zugleich *Kriterien* für die Konzeption einer solchen, das abwehrrechtliche Verständnis transzendierenden informationellen Selbststeuerung aus. So gilt zunächst, daß die objektiv wahre, sachliche und neutrale Information in der Informationsgesellschaft keinen Grundrechtseingriff bildet. Daneben ist von Verfassungs wegen die individuelle Rezipientenfreiheit als „informationelle Selbstbestimmung" anzuerkennen. Demgegenüber sind die Eingriffslehre und die Lehre vom Gesetzesvorbehalt nicht geeignet, die Verfassungsmäßigkeit staatlichen Informationshandelns beurteilen zu können; demokratie- und rechtsstaatliche Dogmatik muß in der „Risikogesellschaft" Kommunikation fördern, nicht begrenzen. Staatliche und vermachtete private Informationstätigkeit führen allerdings dann zum Verfassungsverstoß, wenn sie grundrechtliche Schutzgüter verletzen.

3. Vom Datenschutz - zum Datenverkehrsrecht

In der Konsequenz dessen hat das geltende Informationsverwaltungsrecht seine offenkundige Fixierung auf das abwehrrechtliche Verständnis des Rechts auf informationelle Selbstbestimmung zu überdenken. Die durch freien Informationsfluß garantierte Persönlichkeitsentfaltung in eigener

[34] Näher dazu Pitschas (Fußn. 14), S. 243; vgl. auch Albers (Fußn. 11), S. 128 ff.

Verantwortung ist vielmehr durch eine entsprechende Öffnung der Geltungsreichweite und damit auch gegenüber der Verwaltung rechtlich zu instrumentieren. Der Grundsatz lautet: „Empowering the information poor". Es mag zwar sein, daß auf der Seite des Bürgers die Informationsrezeption faktisch nur dann eine Bedeutung erlangt, wenn sie im Kontext pragmatisch definierter Handlungszusammenhänge erfolgt - sei es in Ausbildung, Weiterbildung oder in der Produktion, in der Planung und bei Entscheidungsvorbereitungen. Das festzustellen heißt aber nicht, dem einzelnen nur durch Gesetz sach- und bereichsbezogen zu erlauben, wann er welche Informationen erhalten und verwerten darf. Dann nämlich würde aus dem freiheitssichernden Gesetzesvorbehalt staatliche Bevormundung, nämlich Gängelung des Informierens.

4. Neuorientierung des Datenschutzes im privaten Bereich

Die Entwicklung der neuen Medien wirft zugleich die Frage nach der künftigen Funktion des Datenschutzrechts im *privaten Sektor* auf. Mit Recht wird darauf verwiesen, daß man in der Informationsgesellschaft nicht „die vollkommene Abschottung der Teilnehmer voneinander sichern" könne.[35] Beispiele hierfür sind die Entwicklung und der Einsatz von Chipkarten oder die Videoüberwachung in Bereichen privaten Hausrechts. Anders noch setzt die Frage nach der Ausgestaltung des Datenschutzes bei privaten Krankenversicherungen oder auch Sicherheitsdiensten an. Jeweils aber sollten Datenschutzüberlegungen in den Zusammenhang des privatrechtlichen Rechtsgüterschutzes eingefügt und Datenverkehrspflichten entwickelt werden, die in wertender Betrachtung den Kommunikationsprozeß in selbsteröffneten Verkehrsbereichen ordnen. Es geht dabei um den Aufbau von *Wissensnormen*, die auch private Schutzpflichten (z. B. gegenüber Kindern) auf Informationsmärkten zu sichern hätten.

Dem Staat ist im Zusammenhang dieser Selbststeuerung nicht jeder Zutritt in private Kommunikationsdienste gestattet; doch darf individuelle Verschlüsselung keineswegs dazu führen, daß Internet-Nutzung den Boden für

[35] Bull (Fußn. 15), S. 2 (These 10).

kriminelle Taten bereitet. Auch die gesetzliche Verpflichtung der Anbieter von Telefondiensten, der Polizei, den Nachrichtendiensten und Behörden auf Verlangen die Bestandsdaten ihrer Kunden zu übermitteln, ist deshalb nicht zu rügen.[36]

Vorrang behält indessen die *Selbstregulierung* des Informationsverhaltens. Es bedarf marktgerechter Strategien des Wissenserwerbs und der Wissenszurechnung sowie des Verkehrsschutzes personenbezogener Daten.[37] Dabei dürfte künftig das „Datenschutz-Audit", auf dessen Grundlage die Eignung gesellschaftlicher Vorkehrungen zum Datenschutz zu zertifizieren wäre, eine gewichtige Rolle spielen.[38] Gleichwohl wäre es geradezu treuherzig anzunehmen, daß Staat und Verwaltung oder auch machtvolle Private die in der Herrschaft über Informationen liegende Macht durch Wissensverteilung nicht nutzen würden. Der grundrechtliche Ausgangspunkt der informationellen Selbstbestimmung verlangt deshalb auch den Schutz der Persönlichkeit gegenüber Informationseingriffen von privater Hand.[39] Doch darf dieser Schutz „privatisiert" werden. *Gesellschaftliche Kontrollbedürfnisse* und *-aufträge* sowie die Notwendigkeit der Entwicklung spezieller Kontrollberufe sind mithin zu bejahen: Insofern Kommunikationsverdichtung freiheitsbegünstigend wirkt - darauf wurde oben hingewiesen -, sollten auch gesellschaftlichen Instanzen jenseits bloßer Auskunftsbefugnisse an der Wissensordnung im Privatsektor sowohl institutionell als auch individuell beteiligt werden. Dies könnte über die Einrichtung repräsentativer gesellschaftlicher Kontrollkommissionen ebenso geschehen wie über die Mitwirkung Privater bei der Wahrnehmung der staatlichen Aufgabe „Informationsversorgung". Auf diese Weise käme es zu der voraufgehend empfohlenen *dualen Informationsverantwortung* („Datenschutz-Audit"), wie wir sie im übrigen - als partnerschaftliche Umweltverantwortung - bei Unternehmenszertifizierungen im Umweltschutz („Öko-Audit") bereits kennen.

[36] Anders z. B. Hamm, DuD 4/1997, S. 186 ff.
[37] Jacob, Datenschutz am Scheideweg - Die neuen Herausforderungen für das Recht des Bürgers auf informationelle Selbstbestimmung, ZFiS (Fußn. 24) 2/1997, S. 67 (68 f.); Drexl, ZHR 161 (1997), S. 491 (492, 503 ff.).
[38] Roßnagel, DuD 9/1997, S. 505 ff.
[39] Kirchhof (Fußn. 31), RdNr. 131 a. E.

5. Die „Europäische Dimension“

Der Perspektivenwechsel des Informationsrechts hat, soweit er anders geartete rechtliche Ordnungsmodelle sowie Grundsätze für die informationsrechtlichen Beziehungen des Staates zur Gesellschaft sowie für die Verwaltungskommunikation bereitstellt, die rechtlichen Direktiven zu beachten, die von der Europäischen Union erlassen worden sind. Das Europäische Parlament und der Rat der Europäischen Union haben diesbezüglich eine *Datenschutzrichtlinie* verabschiedet, die noch im Jahr 1998 in der Bundesrepublik Deutschland umgesetzt werden muß.[40]

Wir kommen deshalb nicht an einer Korrektur des eigenen Rechts vorbei, wie die Leitmaximen und die Regelungsansätze dieser Richtlinie verdeutlichen.[41] Dabei ist aber die Balance zwischen Datenschutz *und* freiem Datenverkehr zu gewährleisten. Die Umsetzung der Datenschutzrichtlinie in der Bundesrepublik Deutschland wird zeigen, ob dem Perspektivenwechsel des Informationsrechts, wie er voraufgehend entfaltet wurde, Rechnung getragen wird.

V. Zusammenfassung: Informationsrecht als Steuerungsrecht ganzheitlicher Informationsverarbeitung

Ziehen wir Bilanz: Der Paradigmawandel des Datenschutzrechts ist unverkennbar. Dessen *neue Konzeption* setzt auf die Informationsaufgabe der Exekutive und die informationelle Selbststeuerung der Privatrechtsgesellschaft im „schlanken“ Staat. Diese bleibt freilich verfassungsgebunden.

Allerdings sind die mit der Verfügbarkeit von Informationen im Rahmen einer integrierten und ganzheitlichen Informationsverarbeitung verknüpften *Gefahren* nicht zu übersehen. Zwischen den Interessen der „Informationsherren“ im privaten Sektor und denen des Marktbürgers können Gegensätze

[40] Dazu im Überblick Derleder, Das Europarecht und die Informationsgesellschaft, in: Krämer/Micklitz/Tonner (Hrsg.), Recht und diffuse Interessen in der Europäischen Rechtsordnung, Baden-Baden 1997, S. 111 ff.
[41] Damman/Simitis (Fußn. 1), Einleitung, Rdnr. 42 ff.

auftreten, die sich sowohl auf die Nutzung des gewollten Informationsaustausches als auch auf die Verhinderung des Datenflusses beziehen können. Zu den unerwünschten Informationsflüssen zählen etwa die Fälle der Geheimhaltung und allgemein die der Verheimlichung von Informationen. Im Rahmen der Staatskommunikation kann es ferner zu „Informationseingriffen“ kommen. Auch sind Fälle denkbar, in denen der Staat seinerseits bestimmte Informationen nicht zur Kenntnis nehmen will. Er kann aber auch daran interessiert sein, den Zugang von Informationen beim Bürger zu erzwingen (förmliche Zustellung von Schriftstücken) oder die Abgabe von Informationen zu erreichen (Meldedaten, Statistik).

Gegenwärtig versucht das im Bundesdatenschutzgesetz und bereichspezifisch verankerte *Datenschutzrecht***,** den Umgang mit personenbezogenen Informationen bei solchen Interessenkonflikten vor allem abwehrbezogen zu regulieren. Wie jedoch die dimensionale Entfaltung des Informationsrechts gezeigt hat, bedarf es anstelle dieses Ansatzes eines objektivierten *Datenverkehrsrechts*, das den Gegenstand, die konstituierenden Sachfragen und die Leitprinzipien einer künftigen Informationsordnung im öffentlichen und Privatrechtssektor teilhabebezogen konturiert und dabei die informationelle Selbststeuerung des Bürgers in ihrer doppelten Bedeutung integriert, nämlich sowohl die unbefugte Datennutzung unterbindet als auch seine freie und ungehinderte Information ermöglicht. Diese *ganzheitliche* Entwicklung des Informationsrechts steht in der Bundesrepublik Deutschland noch aus; sie wird indessen durch den europarechtlichen Regulierungsdruck unausweichlich.

Datenschutz - Herausforderung durch neue Technik und Europarecht

Stefan Walz

1. Umsetzung der EG-Richtlinie - Minimalismus vs. Modernisierung

Die Diskussion über die Anpassung des deutschen Datenschutzrechts an die EG-Richtlinie 95/46/EG („Datenschutzrichtlinie") spielt sich ab zwischen den Polen eines defensiven Minimalismus einerseits und einer an den Entwicklungen der IuK-Technologie orientierten Modernisierung andererseits.[1] Die Datenschutzbeauftragten gehören zur zweiten „Fraktion": Sie verlangen, daß die Gelegenheit der BDSG-Novellierung genutzt wird für eine *Reaktion auf neue Technikrisiken* wie z. B. Videoüberwachung, Chipkartentechnologie und Vernetzung. Die 54. Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat diese Forderungen im Oktober 1997 noch einmal bekräftigt.[2]

Doch laufen alle Teilnehmer an der Novellierungsdebatte die gleiche Gefahr, nämlich die Diskussion über die Zukunft des Datenschutzes auf die Ebene der rechtlichen Regulierung zu verengen. Es gilt zu vermeiden, daß juristische Sandkastenspiele stattfinden, die ohne nennenswerten Einfluß auf die Entwicklung der Informationsgesellschaft bleiben.

---

[1] Vgl. die Podiumsdiskussion der 19. DAFTA, Köln 1995, Tagungsbericht von Jaspers, RDV 1996, 18 f.

[2] DuD 12/1997, 735; s. a. Entschließung der 51. Konferenz vom März 1996, DuD 7/1996, 425; für eine umfassende Novellierung des BDSG auch Brühann/Zerdick, CR 1996, 429 ff.; Weichert, DuD 12/1997, 716 ff.; Schild, DuD 12/1997, 720 ff.

Die Debatte über die Richtlinie in Deutschland wurde während ihrer Ausarbeitung, also seit 1990, von der Ministerialbürokratie, aber auch von den Wirtschaftsverbänden, vorrangig „strukturkonservativ“ geführt mit der Zielsetzung, zugespitzt formuliert, unser - angeblich (s. 4.2) - bewährtes deutsches System vor der Aufnahme von aus ausländischen Rechtsordnungen stammenden Regelungselementen möglichst weitgehend zu schützen.[3] Betrachtet man die bis jetzt bekanntgewordenen (Vor-)Entwürfe aus dem Bundesinnenministerium[4] und die zugehörigen Reaktionen, hat sich an diesem Ansatz bis heute wenig geändert.[5]

2. „Patchwork“ aus einzelstaatlichen Rechtssystemen

2.1 Anstöße für Alternativen zum deutschen System

Ohne Zweifel stellt die Richtlinie keinen konzeptionellen Neuentwurf „aus einem Guß“ dar, sondern ein *„patchwork“ aus unterschiedlichen einzelstaatlichen Datenschutzsystemen:* Der Sonderschutz für die sensitiven Daten (Art. 8) stammt u. a. aus Frankreich, das Registrierungssystem (Art. 18 ff.) kennen fast alle unsere Nachbarländer, die Anerkennung der von Verbänden ausgehandelten Verhaltensregeln (Art. 27) kommt aus den Niederlanden usw.. Die Grundstruktur der Richtlinie ist allerdings sehr „deutsch“ ausgefallen. Belege für diese These sind u. a. die Begriffsbestimmungen, das Prinzip des „Verbots mit Erlaubnisvorbehalt“, sowie die Enumerierung von Zulässigkeitstatbeständen, die denen des BDSG sehr ähnlich sind. Andere Länder wie Großbritannien oder Frankreich haben also erheblich größeren Umstellungsaufwand als Deutschland.

Für alle Mitgliedstaaten allerdings gilt der gleiche strukturelle Nachteil: Ihre Datenschutzgesetze, aus deren Einzelelementen die Richtlinie zusammengesetzt ist, sind selbst wiederum auf dem *Hintergrund eines inzwischen überholten Technikszenarios* der siebziger und ersten achtziger Jahre entstanden. Bestes Beispiel dafür ist die in der Richtlinie vorgesehene generelle Registrierpflicht für automatisierte Verarbeitungen (Art. 18 Abs. 1), die

[3] Vgl. die Darstellung der „besonderen deutschen Interessen“ bei Weber, CR 1995, 297, 298 f.; s. a. Werthebach (Staatssekretär im Bundesinnenministerium), RDV 1997, 1 ff.

[4] Siehe unter http://www.dud.de; letzter Stand ist der vom BMI an die Länder und die Verbände gesandte Text vom 01.12.1997.

[5] Vgl. die Stellungnahme der GDD zum BDSG-Entwurf der Fraktion BÜNDNIS 90/DIE GRÜNEN, BT-Drs. 13/9082 v. 14.11.1997, RDV 1997, 272 f.

noch ausgeht von der Vorstellung weniger, klar abgrenzbarer DV-Verfahren in einer Großrechnerlandschaft. Da sich die in der EG „jüngsten" Gesetze Italiens und Griechenlands an der bereits verabschiedeten Richtlinie orientieren mußten, ist es auch kein Paradox, daß sie zwar neu, aber gleichwohl ohne wirklich innovative Elemente sind.

Die immer wieder zu hörenden Klagen über die „Systemwidrigkeit" einiger Elemente der Richtlinie - bezogen auf das deutsche Regelungssystem[6] - sind also nicht nur überzogen, vielmehr verkennen sie auch die *Chance*, die darin liegt, daß wegen des Drucks der Umsetzung der Richtlinie über *Alternativen zu unserem deutschen Modell* nachgedacht werden muß. Dazu zwei Beispiele: *Verhaltensregeln* (Art. 27) bieten einen Rahmen, in dem sich Verbände oder sonstige Repräsentanten von „data-usern" und „data-subjects" über ihre jeweiligen Interessen verständigen und faire Verarbeitungsbedingungen aushandeln können, etwa im Bereich des Direktmarketing oder der Versicherungen. Unseren gewohnten hoheitlich-normativen Rechtsvorstellungen sind sie zwar fremd. Aber: Verhaltensregeln delegieren Handlungskompetenzen und Regelungsverantwortung. Sie sind Elemente der Selbstregulierung, von „prozeduralem Recht", das Rechtstheoretiker gerade für sich rasch verändernde gesellschaftliche Sachverhalte und Interessenlagen empfehlen[7]. Daß „codes of conduct" auch ihre Schwächen im Hinblick auf Repräsentativität und Umsetzung in den jeweiligen Branchen haben, zeigt die niederländische Erfahrung.

Zweites Beispiel ist die *Datenschutzkontrolle* (Art. 28): Die anderen EG-Länder hatten und haben wenig Verständnis für die besonderen Befindlichkeiten des deutschen „dualen" Kontrollsystems mit unterschiedlichen Zuständigkeiten, Befugnissen und hierarchischen Einbindungen von Datenschutzbeauftragten und Aufsichtsbehörden.[8] Die Richtlinie geht konsequenterweise von einem einheitlichen Überwachungsstandard in Verwaltung und Wirtschaft aus. Für unsere EG-Partnerstaaten sind mit anderen Worten wirksame Eingriffsbefugnisse auch in der Privatwirtschaft ebenso selbstverständlich wie die einheitliche und „völlig unabhängige" Wahrnehmung der Aufsichtsfunktion für den öffentlichen wie für den nicht-

[6] Vgl. z. B. Werthebach (Fußn. 3), 2.
[7] Grundlegend Teubner, ARSP 1982, 13 ff.
[8] Nachw. bei Giesen, DuD 9/1997, 529 f.

öffentlichen Bereich.[9] Bei der anstehenden Novellierung muß daher § 38 BDSG erheblich nachgebessert werden.[10]

2.2 Stärkung der individuellen Rechtsposition

Es gibt weitere Gründe, die Anforderungen der Richtlinie nicht defensiv abzuwehren, sondern offensiv zu akzeptieren. So stärkt die Richtlinie - gegenüber dem deutschen Niveau - *die Rechtspositionen des Einzelnen* gegenüber den Daten über ihn verarbeitenden Stellen. Das novellierte BDSG muß daher u. a.

- die Benachrichtigung des Betroffenen und die Information über seine Individualrechte verbessern,

- die Widerspruchsrechte stärken, auch gegenüber rechtmäßigem Datenumgang,

  sowie

- das Verbot automatisierter Persönlichkeitsprofile einführen, wie es für beamtenrechtliche Entscheidungen bereits in § 56 f Abs. 4 BRRG verankert ist.

So wichtig aber die Harmonisierung der einzelstaatlichen Datenschutzrechte „nach oben" ist, aus integrationspolitischer Sicht wichtiger ist der folgende Gesichtspunkt: Die Richtlinie ist Ausdruck der *neuen grundrechtlichen Fundierung*, die sich die Europäische Union 1992 im Maastricht-Vertrag gegeben hat und die vom Amsterdamer Vertrag vom 2. Oktober 1997 nicht geändert worden ist. Art. F Abs. 2 des EU-Vertrages stellt ausdrücklich fest, daß sich die Gemeinschaft nicht nur an die vom Europäischen Gerichtshof in langjähriger Rechtsprechung herausgearbeiteten gemeinsamen Verfassungsgrundsätze der Mitgliedstaaten gebunden fühlt, sondern an geschriebenes materielles europäisches „Verfassungsrecht", nämlich an die Europäische Menschenrechtskonvention von 1950 (EMRK). Die EMRK wiederum gewährleistet in Art. 8 explizit den Schutz des Privatlebens.

---

[9] A.A. Lepper/Wilde, CR 1997, 703 ff.
[10] So zu Recht Brühann/Zerdick, CR 1996, 429, 435; s. a. Bizer, DuD 8/1997, 481.

3. Adäquanzprinzip - die transatlantische Debatte

Art. 25 der Richtlinie verlangt für die Datenübermittlung aus der EG in Drittstaaten ein *„angemessenes" Schutzniveau im Zielland*. Sonst drohen - äußerstenfalls - Verbote von Datentransfers durch die Kontrollinstanzen der Mitgliedstaaten. Wegen der engen internationalen Handelsverflechtungen und der damit verbundenen Datenströme haben dieses Adäquanzprinzip und seine möglichen Konsequenzen für den grenzüberschreitenden elektronischen Geschäftsverkehr eminente praktische Bedeutung. Dementsprechend stark fallen die Reaktionen in den hauptsächlich betroffenen Staaten außerhalb der EG aus, vor allem in den USA.

Die Ausgangspunkte von EG und USA sind kontrovers: Die europäische Seite, d. h. die EG-Kommission und die Datenschutzbehörden, zählen zum hard-core *materieller* Adäquanz vor allem klare Zulässigkeitsbedingungen (insbesondere die Zweckbindung), ein funktionierendes Beschwerdesystem für Bürger und Verbraucher und eine effiziente Aufsichtsinstanz. Die Gewährleistung dieser Verarbeitungsbedingungen soll *vorzugsweise* durch gesetzliche Querschnittsregelungen erfolgen. Doch liegen Regelungsformen und Regelungsebene nicht zwingend im Sinne der europäischen Systeme fest; *„funktionale" Adäquanz* des Datenschutzniveaus im Drittstaat soll ausreichen.[11]

Die US-amerikanische Seite dagegen - d. h. die am Dialog beteiligten Beamten der Clinton-Administration, Wirtschaftsvertreter und Hochschullehrer - lehnen in ihrer großen Mehrheit gesetzliche Regelungen ab, jedenfalls in der in der EG üblichen Form allgemeiner Datenschutzgesetze. Dies sei einer common-law-Rechtsordnung systemfremd und im übrigen auch überflüssig; Datenschutz solle und könne ausreichend (nur) durch die *Selbstregulierung* der betroffenen Wirtschaftskreise sichergestellt werden.[12]

Die „Europäer" wiederum replizieren, daß die Effizienz des self-regulation-Systems in den USA nachhaltig zu bezweifeln ist. Dies könne insbesondere durch die von der EG-Kommission in Auftrag gegebene Studie der amerikanischen Rechtsprofessoren *Reidenberg* und *Schwartz* über den Stand des

[11] Vgl. u. Fußn. 15.
[12] Vgl. dazu die Beiträge in dem vom US Department of Commerce herausgegebenen Sammelband „Privacy and Self-Regulation in the Information Age", Washington 1997.

Datenschutzes in den USA belegt werden.[13] Auch die Behauptung der Systemwidrigkeit *gesetzlicher* Regelung wird bestritten durch Hinweis auf die sektoral zahlreich vorhandene datenschutzbezogene Gesetzgebung etwa im Fair Credit Reporting Act oder im Video Privacy Protection Act. Schließlich wird Kanada als Gegenbeleg herangezogen insofern, als dieser Staat trotz gemeinsamer common-law-Tradition nicht nur Datenschutzgesetze für den öffentlichen Bereich in Bund und Ländern aufweist, sondern auch seine Bereitschaft erklärt hat, diese Gesetzgebung auf die private Wirtschaft auszudehnen.

Derzeit ist die *transatlantische Debatte,* die auf einer Vielzahl von Tagungen und Kongressen geführt wurde und wird[14], in diesen Ausgangspositionen etwas festgefahren. Sicherlich wird es zu Kompromissen kommen und sich die Einschaltung der Welthandelsorganisation (WTO) vermeiden lassen, doch bedarf es dazu noch intensiver bilateraler Gespräche nicht zuletzt zwischen EG-Kommission und US-Regierung. Die Gruppe nach Art. 29 der Richtlinie, die zusammengesetzt ist aus Vertretern der einzelstaatlichen Datenschutzinstanzen, hat zur Versachlichung des Dialogs im Sommer 1997 ein ausführliches Positionspapier als Diskussionsgrundlage vorgelegt.[15]

4. Adäquanzprinzip - Konsequenzen für Europa

Drei Konsequenzen der Regelung in der EG-Richtlinie über den Datenexport in Drittstaaten und des transatlantischen Disputs darüber sind bisher noch wenig beachtet worden.

4.1 „Forum-Shopping“

Zum ersten besteht die *Gefahr* des *„law-shopping“* oder des *„forum-shopping“*, kombiniert mit wirtschaftlichem und/oder politischem Druck von Datenexporteuren und ihren Verbänden. Da die Richtlinie den nationa-

[13] Schwartz/Reidenberg, Data Privacy Law, Charlottesville, Virginia 1996; vgl. dazu meine Rezension in DuD 3/1998, 180.
[14] Vgl. meinen Bericht von der 18. Internationalen Datenschutzkonferenz 1996 in Ottawa, CR 1996, 707 f.; s. a. Westin, Data Protection in the Global Society, Conference Report über eine Tagung des AICGS Berlin am 15.11.1996, <http://www.jhu.edu/~aicgsdoc/>.
[15] Veröffentlicht in DuD 2/1998, 97.

len Gesetzgebern für die Umsetzung eine nicht unerhebliche Bandbreite läßt, sind unterschiedliche Schutzniveaus auch innerhalb der EG zu erwarten. Bezugspunkt für die Bewertung der Adäquanz im Drittstaat wird das jeweilige nationale Recht des Landes sein, aus dem die Angaben übermittelt werden. Selbst bei im wesentlichen textgleichen und den Art. 25 und 26 genau nachformulierten Regelungen könnten sich daher divergente Beurteilungsmaßstäbe ergeben. Denkbar wäre dann, daß in mehreren Mitgliedstaaten operierende Unternehmen sich für die Beurteilung der Zulässigkeit ihrer Übermittlungen in Drittländer den Mitgliedstaat mit dem schwächsten Schutz und/oder mit den „kooperativsten" Aufsichtsbehörden heraussuchen. Sie könnten sich dann gegenüber den strengeren Kontrollinstanzen anderer EG-Staaten auf die dort bejahte Zulässigkeit berufen oder gleich ihre die EG-Grenzen überquerenden Datenströme über die dortige Filiale lenken. Wird „Flexibilität", um nicht zu sagen Nachgiebigkeit, bei der Beurteilung der Adäquanz ausländischer Rechtssysteme zum Standortfaktor für Gesellschaften mit umfangreichem grenzüberschreitenden elektronischen Geschäftsverkehr, wird politischer Druck solcher Unternehmen auf Datenschutzbehörden und/oder deren Regierungen zunehmen. *Standfestigkeit der Kontrollinstanzen und die absolute Unabhängigkeit ihrer Stellung und Tätigkeit sind* unverzichtbare Voraussetzungen dafür, einen Unterbietungswettbewerb zu Lasten der Schutzinteressen der von Datenexport betroffenen EG-Bürger zu vermeiden.

4.2 Selbstkritische Evaluation des deutschen Modells

Zweite Konsequenz: Wer wie die EG-Staaten mit ihrer Datenschutz-Richtlinie „Angemessenheit" des Datenschutzniveaus außerhalb seiner Grenzen verlangt, muß sich seiner eigenen Standards sicher sein. *Selbstkritische Evaluation des eigenen nationalen Datenschutzsystems* ist dafür notwendige Bedingung. Zu Recht fragt die US-Seite die Europäer, wie gut eigentlich die Modelle in den Gemeinschaftsstaaten *in der Praxis* funktionieren.

Will man darauf antworten, stößt man auf ein fundamentales empirisches Defizit. Wir wissen wenig oder nichts Gesichertes

- über die Risikoperzeption der Bevölkerung (z. B.: Welche Datenschutzrisiken ängstigen am meisten? Welche Datenschutzverstöße werden als gravierend empfunden?),

- über die tatsächliche soziale Verteilung von Datenschutzrisiken (z. B.: Sind Angehörige der Unterschichten oder der Mittelschichten mehr von Adreßhandel und Direktmarketing betroffen?),

- über die Inanspruchnahme von Gegenrechten, Widerspruchsmöglichkeiten oder sonstigen datenschutzsichernden Verhaltensweisen (z. B.: Wie häufig wird der Nutzung zu Werbezwecken widersprochen? Wie oft werden erfragte Angaben verweigert ?),

- über Implementationsdefizite des allgemeinen wie des bereichspezifischen Datenschutzrechts (z. B.: Wer von den Millionen von Datennutzern kennt und/oder wendet wissentlich und/oder unwissentlich Datenschutzgesetze korrekt oder unkorrekt an?),

- über die tatsächliche Effizienz der Datenschutzbeauftragten und Aufsichtsbehörden (z. B.: Sind zahlreiche Eingaben Ausweis funktionierender Öffentlichkeitsarbeit oder unzulänglicher Kontrolltätigkeit?).

Natürlich gibt es Gründe für dieses *Wissensdefizit*. Zunächst und vor allem fehlt es an einem klaren Kriterienraster für die systematische Evaluierung von Datenschutzgesetzen und Datenschutzinstanzen. Das „Produkt Datenschutz“ ist nicht an seinem Markterfolg meßbar; es kommt als Ergebnis eines komplexen Prozesses zahlreicher Akteure zustande. Die Definition des angestrebten Zustands optimaler „privacy protection“, die Abwägung zwischen „berechtigten Interessen“ der Datennutzer und „schutzwürdigen Belangen“ der Betroffenen erfolgt jeweils subjektiv und hängt ab von Lebenswelten, Interessenlagen, Bildungsstand usw.. Zwar können die regelmäßigen Jahres- und Tätigkeitsberichte der Datenschutzinstanzen deren Aktivitäten statistisch und damit ggf. auch empirisch evaluierbar ausweisen. Gemessen wird damit aber nur die „efficiency“, also das Verhältnis von Aufwand und Ertrag, nicht aber die „effectiveness“, also das Verhältnis des

„Outputs“ dieser Behörden zu einer - wie auch immer definierten - realen Verbesserung des Datenschutzes.

Kurz: *Es fehlt eine ganzheitliche Perspektive des Datenschutzsystems*, eine Perspektive, die das Datenschutzrecht, die Datennutzer, die Datenkontrolleure und die Betroffenen sowie deren Interaktionen umfaßt.[16] Diese Zustandsbeschreibung müßte Ansporn sein für eine verstärkte Interaktion zwischen Datenschutzbeauftragten und Bürgern, vor allem aber für ein verstärktes Engagement von Sozialwissenschaftlern. Anders ausgedrückt: Datenschutz muß viel mehr als bisher Gegenstand empirischer Sozialforschung werden. Ohne eine holistische Perspektive bleibt es bei der Fehlallokation knapper Datenschutzressourcen und dem Fehler, die Diskussion über Verbesserungen zu stark auf die Regulierungsebene zu konzentrieren.

4.3 Einwilligung als „Grundrechtsfalle“?

Die dritte Fragestellung, die durch die transatlantische Debatte akzentuiert wird, betrifft einen Eckpfeiler des (nicht nur) deutschen Datenschutzmodells, die *Einwilligung*. Idealiter soll die Einwilligung Ausdruck und Konsequenz des Grundrechts auf informationelle Selbstbestimmung sein. Die Realität zeigt jedoch, daß sie zunehmend als Hebel für die Einschränkung des gesetzlichen Schutzstandards genutzt wird. Dies gilt insbesondere in ihrer Form als standardisierte Vertragsklausel etwa bei Banken und Versicherungen. § 6 BDSG, der immerhin einige Betroffenenrechte für durch Vertrag unabdingbar erklärt, hilft hier nicht weiter.

US-Ökonomen und -Sozialwissenschaftler gehen wesentlich weiter. Sie hinterfragen - auf der Grundlage des ganz anderen Verfassungs- und Sozialmodells ihres Landes - gesetzlich verordnete Einschränkungen der Dispositionsbefugnis des Individuums in dessen (vorgeblichen?) Interesse prinzipiell kritisch. Sie fragen ganz unbefangen: *Why should privacy not be part of the market?*[17] Warum sollte Datenschutz einschließlich der Betroffenenrechte nicht Teil von Markt- oder Vertragsbeziehungen sein, wenn funktionierender Wettbewerb mit gleich starken Vertragspartnern besteht, der

[16] Vgl. dazu Raab/Bennett, Taking measure of privacy: can data protection be evaluated?, International Review of Adminstrative Sciences, 1996, 535 ff., 553.
[17] Vgl. Noam, Privacy and Self-Regulation, Markets for Electronic Privacy, in dem in Fußn. 12 nachgewiesenen Sammelband, 21 ff.

Verbraucher bei verschiedenen angebotenen Verarbeitungsvarianten frei über die Verwendung seiner Daten entscheiden und ggf. für die Nutzung sogar ein Entgelt oder einen Preisnachlaß verlangen kann? Wenn z. B. eine Telefongesellschaft niedrigere Gebühren als die Konkurrenz anbietet, dafür aber verlangt, daß ihr der Kunde die Auswertung der Verbindungsdaten für Nutzungsprofile oder zu Marketingzwecken erlaubt, warum sollte der Betroffene nicht in diese Zweckänderung zugunsten eines Rabatts einwilligen oder auf sein Widerspruchsrecht verzichten dürfen?

Dies heißt: Wenn einerseits die *Einwilligung, Widerspruchsrechte oder sonstige Wahlmöglichkeiten des Betroffenen* unverzichtbare Elemente eines wirksamen „Selbstdatenschutzes" sind und als Instrumente gesamtgesellschaftlich erwünschter zunehmender Entscheidungsspielräume des Individuums an Bedeutung gewinnen, andererseits die Schutzgarantien der gesetzlichen Regelungen nicht unterlaufen werden sollen, muß man sich intensiver als bisher mit den Grenzen der Individualautonomie im Datenschutzrecht, d. h. ihrer *Abgrenzung gegenüber unabdingbarem zwingendem Recht*, beschäftigen.[18] Wo die freie Ausübung des Rechts auf informationelle Selbstbestimmung aufhört und die staatliche Interventionspflicht zugunsten der Schwächeren beginnt, muß in der Informationsgesellschaft mit ihren vielfältigen interaktiven elektronischen Verkehrsformen neu definiert werden. Kernelement solcher Überlegungen wird die Definition der Voraussetzungen für die *„Freiwilligkeit"* sein, die die EG-Richtlinie explizit als Bedingung für eine wirksame Einwilligung nennt (Art. 2 lit. h).

5. Globale Technik versus nationales Recht?

Mit Erlaß der EG-Richtlinie gilt es auch die Frage nach der sinnvollen Regelungsebene für die Bewältigung gesellschaftlicher Technikfolgen neu zu thematisieren. Ohne Zweifel: *Globalisierung der Technikentwicklung und Nationalstaatlichkeit des Technikrechts passen auf Dauer nicht zusammen.* Dies belegt die Entwicklung des INTERNET. Doch wer annimmt, wegen der globalen Vernetzung sei nationales Telekommunikations- oder Datenschutzrecht bereits jetzt weitgehend obsolet, verkennt, daß die große Mehrzahl der vom BDSG, vom TKG oder vom neuen Multimediarecht erfaßten Verarbeitungs-, Datenabruf- und Telekommunikationsvorgänge sich noch

[18] Vgl. dazu Simitis, in Simitis u. a., BDSG, 4. Aufl., § 4 Rdnr. 27.

immer innerhalb der deutschen Grenzen abspielt. Auch grenzüberschreitende Sachverhalte elektronischer Interaktion unterfallen ganz oder teilweise einzelstaatlichen Rechtsordnungen.[19]

Gleichwohl werden *Steuerungsdefizite* des Rechts auch und gerade bei Datenschutz und Datensicherung[20] unvermeidlich, wenn bestimmte Grundstandards sowohl für die technische Normung als auch für die Zulässigkeit der Nutzung grenzüberschreitender Netze nicht international vereinbart werden. Die EG versucht dies auf der europäischen Ebene mit zahlreichen Richtlinien, Verordnungen und Empfehlungen. Zu nennen ist in diesem Kontext vor allem die am 1. Dezember 1997 vom EU-Ministerrat endgültig angenommene „ISDN-Richtlinie", die Teilelemente des Datenschutzes in der Telekommunikation harmonisieren soll.[21] Zu erwarten ist allerdings, daß angesichts der Globalisierung von Datenströmen und Kommunikationsvorgängen selbst die EG als Regelungsebene künftig nicht (mehr) ausreichen wird. Vorschläge für verbindliches Völkerrecht, etwa in Form einer „Internet-Konvention", sind daher folgerichtig. Das Thema kann an dieser Stelle nicht vertieft werden. Erforderlich ist jedenfalls eine differenzierte Einschätzung dahingehend, daß die IuK-Entwicklung sich derzeit in einer Phase befindet, in der *sowohl grenzüberschreitende als auch nationale Regulierung ihren jeweiligen Stellenwert* haben, der sich allerdings zunehmend zugunsten überstaatlicher Normsetzung verschiebt.

6. Konvergenz von Technologien und Rechtsgebieten

Die *Konvergenz von Datenverarbeitung, Rundfunk und Telekommunikation* wird in wichtigen Elementen zu *inhaltlicher Konvergenz* der diese unterschiedlichen Technologien bisher regelnden *Gesetze* führen. Genauer ausgedrückt: Soweit Digitalisierung und Vernetzung Datenschutzrisiken erzeugen, müssen die Schutzanforderungen konsequenterweise „quer" durch herkömmliche Rechtsgebiete harmonisiert werden. Die Multimedia-Entwicklung wird die klassische Aufteilung von Presserecht, Rundfunk-

[19] Vgl. zur Einordnung des Internet nach deutschem Datenschutzrecht Schaar, CR 1996, 170, 172 ff.

[20] Vgl. dazu den Sammelband Wilhelm (Hrsg.), Information-Technik-Recht, Rechtsgüterschutz in der Informationsgesellschaft, Darmstadt 1993.

[21] Richtlinie des Europäischen Parlaments und des Rates über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre im Bereich der Telekommunikation, ABl. der EG, L 24 v. 30.01.1998, 1.

recht, Datenschutzrecht und Telekommunikationsrecht zumindest teilweise aufheben. Der technische Fortschritt ist mithin - neben dem „Outsourcing“ öffentlicher Aufgaben - ein weiterer Faktor, der die traditionelle Abgrenzung zwischen öffentlichem und Privatrecht porös macht.

Illustratives Beispiel: Programme für den Zugriff durch Netznutzer sollen - zumindest optional - Anonymität gewährleisten und Nutzungsprofile verhindern, um soziale Kontrolle zu vermeiden. Dies gilt völlig gleich, ob man eine elektronische Zeitung liest (Presserecht), einzelne Rundfunksendungen interaktiv anfordert (pay-per-view, Rundfunkrecht), telefoniert (Telekommunikationsrecht) oder einen Tele- bzw. Mediendienst (Teledienstegesetz/TDG bzw. Teledienstedatenschutzgesetz/TDDSG, Mediendienstestaatsvertrag/MDStV) abruft (vgl. § 4 Abs. 1 TDDSG, § 13 Abs. 1 MDStV). Die Entwicklung des deutschen Multimediarechts - auch der derzeit vorbereitete Staatsvertrag über den digitalen Rundfunk gehört hierher - mit der Tendenz zu übereinstimmenden Datenschutzregelungen geht daher in die richtige Richtung.[22]

7. Datenschutzfreundliche Technik

Datenschutzfördernde Techniken (Privacy Enhancing Technologies, PETs) wie Verschlüsselung, anonymisierte Zugriffsverfahren etc. werden derzeit von vielen als „Königsweg“ eines modernen Datenschutzes angesehen. Zweifellos sind sie *wichtige Instrumente informationeller Selbstbestimmung in der Informationsgesellschaft.* So verhindert z. B. eine anonyme Zugangssoftware zu Datenbanken und Telediensten den „gläsernen“ Netzbürger.[23] Die gesetzliche Verpflichtung, solche Techniken einzuführen (s. o. 6.), stößt allerdings auf erhebliche *ökonomische Gegeninteressen*. So sind z. B. Telenutzungsdaten von großem Wert für die Ermittlung der Kundenakzeptanz von Angeboten oder für Werbezwecke. Und: § 4 Abs. 1 TDDSG und § 13 Abs. 1 MDStV lassen den Diensteanbietern die Hintertür offen, daß anonyme Zugangsmöglichkeiten nur insoweit angeboten werden müssen, als dies „technisch möglich und zumutbar ist“.

[22] Vgl. dazu Schrader, CR 1997, 707 ff.
[23] Siehe auch AK Technik der Konferenz der Datenschutzbeauftragten, DuD 12/1997, 709 ff.

Daher besteht jetzt ein Wettlauf mit der Zeit: Nur wenn datenschutzfreundliche Verfahrenselemente so früh wie möglich in die Systemgestaltung einbezogen werden, läßt sich eine spätere Berufung auf technische Unmöglichkeit oder Unzumutbarkeit von vornherein verhindern. Aktuelles Beispiel für die Notwendigkeit schneller Reaktion ist die für den Empfang digitalen Bezahl-Fernsehens vorgesehene Set-Top-Box.[24]

Gegen die Weigerung von Unternehmen, datenschutzfreundliche Techniken einzusetzen, hilft vor allem das Risiko der Bestrafung durch den Markt: Riskanten technischen Systemen droht *Akzeptanzverlust* bei den (Tele) Kunden. Wird Vertrauen in eine Technik - etwa in die Sicherheitsfeatures beim Tele-Banking - auch nur ein einziges Mal nachhaltig und durch das Medienecho verstärkt erschüttert, läßt es sich nur langfristig und kostspielig wieder herstellen.[25] Zur Durchsetzung von datenschutzfördernder Technik genügen allerdings negative Risikoszenarios nicht. Vielmehr braucht „der Datenschutz“ dazu vor allem Interessenallianzen, etwa mit den Verbraucherschützern bei den Telediensten oder mit der an elektronischem Geschäftsverkehr interessierten Wirtschaft bei der Verschlüsselung.

Die datenschutzfreundliche Gestaltung von Systemen und Verfahren allein reicht aber nicht. Sie wird nur dann effektiv, wenn Anwender bzw. Verbraucher über *ausreichende Mediennutzungs- bzw. Technikkompetenz* verfügen. Netzteilnehmer müssen mit anderen Worten genügend über die Risiken der Netznutzung und ihre Hardware- und Softwarebezogenen Sicherungsmöglichkeiten informiert sein. Ohne hohe Benutzerfreundlichkeit und viel know-how-Vermittlung bleibt der technische Selbstdatenschutz auf „Computerfreaks“ begrenzt.

Schließlich muß der Stellenwert technischer Vorkehrungen im Gesamtsystem des Datenschutzes (s. o. 4.2) realistisch bewertet werden. Auch wenn sich Grundrechtsschutz und Verbraucherschutz des Netzbürgers teilweise überlappen, auch wenn die „Drittwirkung“ des Rechts auf informationelle Selbstbestimmung in vertragliche Beziehungen eingreift: Der Bürger als

[24] Vgl. zu den Anforderungen an die Vermittlung und Abrechnung digitaler Fernsehsendungen die Entschließung der 52. Konferenz der Datenschutzbeauftragten, DuD 12/1996, 756 ff.

[25] Zur Hypothese, daß die Technikeinstellung der Bevölkerung stark von Einzelereignissen abhängt, vgl. „Erste Ergebnisse einer repräsentativen Umfrage des Büros für Technikfolgenabschätzung beim Deutschen Bundestag (TAB) zur Technikakzeptanz“, TAB-Brief Nr. 12/1997, 16.

Grundrechtsträger wird deswegen noch lange nicht reduziert auf den Verbraucher als Vertragspartner.

Technischer Datenschutz kann wertorientierten Grundrechtsschutz durchsetzen helfen, nicht aber ihn ersetzen.[26]

[26] Vgl. Walz, in: Büllesbach (Hrsg.), Datenschutz im Telekommunikationsrecht, Köln 1997, 279 ff. (Podiumsdiskussion).

Die Umsetzung der EU-Richtlinie: Verpaßte Chancen?

Hansjürgen Garstka

Die EU-Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr schreibt eine Umsetzung in das deutsche Datenschutzrecht bis zum 24. Oktober 1998 vor. Schon frühzeitig verlautete aus dem Bundesinnenministerium, man wolle nur die allernotwendigsten Änderungen am Bundesdatenschutzgesetz vornehmen: An eine grundsätzliche Neustrukturierung des deutschen Datenschutzrechts sei nicht gedacht. Dementsprechend sehen auch die Entwürfe für die Novellierung des BDSG aus, die das Bundesinnenministerium in der letzten Zeit vorgelegt hat. Nicht nur daß kaum eine Chance genutzt wurde, weiterweisende Aspekte der Richtlinie in das BDSG einzubringen oder gar fortzuentwickeln, auch zwingende Änderungen werden nicht vorgenommen. Wird der vorliegende Novellierungsentwurf Gesetz (es sieht allerdings derzeit nicht mehr danach aus), wären große Chancen zur Schaffung eines modernen Datenschutzrechts verpaßt.

Reichweite und Grundstrukturen

Eine erhebliche Diskrepanz der Reichweite zwischen Richtlinie und BDSG ergibt sich daraus, daß die Richtlinie wegen ihrer Verankerung in Art. 100 a der Römischen Verträge (Harmonisierung im Hinblick auf den Binnenmarkt) nicht diejenigen Tätigkeiten umfaßt, die in die Titel V (Außen- und Sicherheitspolitik) und VI (Justiz und Inneres) des Maastricht-Vertrags fallen (Art. 3 Abs. 2). Das BMI meint damit einen hinreichenden Grund zu haben, eine Reihe der auf Grund der Richtlinie erforderlichen Änderungen des BDSG insbesondere für die Gesetze im Bereich der Inneren Sicherheit (z. B. Bundesverfassungsschutzgesetz, BKA-Gesetz) nicht übernehmen zu

müssen. Hierunter fallen etwa Bestimmungen über die Datenübermittlungen ins Ausland, die verbesserte Transparenz der Datenverarbeitung sowie die Verstärkung der Rechte der Betroffenen. Dem muß energisch widersprochen werden. Es ist gerade eine Errungenschaft des deutschen Datenschutzrechts, auch die Sicherheitsbehörden grundsätzlich in vollem Umfang in die datenschutzrechtlichen Regelungen einzubinden und nur im erforderlichen Fall gezielt Privilegien für die Sicherheitsbehörden vorzusehen. Dies gilt verschärft für die Länder, wenn diese ihrerseits die Richtlinie umsetzen. Gerade im Bereich des Polizeirechtes darf es keine Absenkung des dort ohnehin nicht optimalen Datenschutzniveaus geben.

Ungeachtet des Sicherheitsbereichs haben die Länder im übrigen ebenfalls einen starken Anpassungsbedarf: So fallen z. B. das gesamte Sozialwesen, die Gesundheitsfürsorge, der Bereich der Versorgungsbetriebe oder der Umgang mit Arbeitnehmerdaten in den Bereich der EG-Richtlinie.

Ein grundsätzliches Strukturproblem bei der Umsetzung der Richtlinie ist die dort verankerte Gleichbehandlung des öffentlichen und des nicht-öffentlichen Bereiches. Diese für das deutsche Rechtsverständnis zunächst ungewöhnliche Struktur macht bei näherem Hinsehen insbesondere vor dem Hintergrund aktueller Entwicklungen Sinn. Schon bisher war es schwierig, diejenigen öffentlichen Stellen, die sich in der Regel privatrechtlicher Rechtsformen für die Abwicklung ihrer Aufgaben bedienen, datenschutzrechtlich angemessen zu behandeln. So zwang schon immer das fiskalische Verhalten der Verwaltung zu gewissen datenschutzrechtlichen Verrenkungen. Die Möglichkeit, statt auf die Erfüllung der öffentlichen Aufgabe auch hier auf die Zweckbestimmung der Vertragsverhältnisse abzustellen, hätte mancherlei Merkwürdigkeiten verhindert - beispielsweise bei der datenschutzrechtlichen Beurteilung des Kaufs von Büromaterialien. Die aktuellen Formen der Übertragung öffentlicher Aufgaben auf Privatunternehmen (z. B. Outsourcing) machen es umgekehrt notwendig, auch öffentlich-rechtliche Figuren auf das Verhalten privater Unternehmen anzuwenden. Eine Öffnung des datenschutzrechtlichen Regelungssystems dahingehend, daß die Befugnisnormen für öffentliche und nicht-öffentliche Stellen einem gleichartigen System unterliegen, wäre daher nicht nur sinnvoll, sondern auch im Hinblick auf die Verwaltungsreform zeitgemäß. Nichts dergleichen findet sich in den bisher vorgelegten Entwürfen.

Begrifflicher Rahmen

Mehr noch als im deutschen Recht üblich legt die Richtlinie Wert auf die Definition der später verwendeten Begriffe. Obwohl auf den ersten Blick eher öde, eröffnen jedoch die in Art. 2 enthaltenen Begriffsbestimmungen beim näheren Hinsehen ganz neue Perspektiven, die von den Novellierungsentwürfen nicht aufgegriffen werden. Drei Beispiele seien genannt.

Die Definition der „personenbezogenen Daten“ (Art. 2 lit.a) stellt im Gegensatz zum derzeitigen deutschen Recht darauf ab, ob bei Daten, bei denen die Person nicht bestimmt, aber bestimmbar ist, diese Bestimmbarkeit über ihre individuelle Identität hergestellt werden kann. Das heißt, ein Personenbezug liegt nur dann vor, wenn dessen Inhalt auch tatsächlich die Persönlichkeitssphäre des Betroffenen erfaßt. Das derzeitige deutsche Recht kennt eine derartige Einschränkung nicht, was dazu zwingt, auch objektbezogene Daten, bei denen der Personenbezug eine allenfalls marginale Rolle spielt, ebenfalls unter das strenge Regime des Datenschutzrechtes zu stellen (z. B. Grundstücksdaten).

Eine wesentliche Frage für die Fortentwicklung des Datenschutzes ist, ob auch im privaten Bereich der Geltungsbereich des Datenschutzgesetzes auf alle Formen der Verarbeitung personenbezogener Daten, also auch auf Akten, Videobänder oder Audiokassetten ausgedehnt werden sollte. Zur Begründung, dies nicht zu tun, verweist die Bundesregierung auf die Richtlinie, die sowohl für den öffentlichen als auch für den nicht-öffentlichen Sektor eine Beschränkung auf die Verarbeitung von Daten in Dateien vorsieht. Allerdings unterscheidet sich die Dateidefinition der Richtlinie in einem wesentlichen Punkt von dem des deutschen Datenschutzrechts: Für den Dateibegriff der Richtlinie reicht es bei nicht-automatisierten Dateien aus, daß die Datensammlung „strukturiert“ ist und die Daten „nach bestimmten Kriterien zugänglich“ sind. Das für die derzeitige deutsche Definition wesentliche Merkmal des gleichartigen Aufbaus, das nach dem Änderungsentwurf lediglich in „nach äußerlich vergleichbaren Merkmalen aufgebaut“ geändert werden soll, fehlt. Da sicherlich bei den meisten Akten davon ausgegangen werden kann, daß sie jedenfalls in einem Mindestmaß strukturiert und die Daten auch zugänglich sind, erfüllt ein Großteil der derzeitigen Aktenverarbeitung den Dateibegriff der Richtlinie. Von der Richtlinie allenfalls in den Erwägungsgründen erwähnt, nicht aber ausdrücklich aufgenommen sind Datensammlungen, die auf modernen Medien wie Multime-

dia, Chipkarten oder Netzen gespeichert werden. Um für die künftigen Entwicklungen einen umfassenden Datenschutz sicherzustellen, werden auch diese Formen der Datenverarbeitung in den Geltungsbereich des nicht-öffentlichen Teils einbezogen werden müssen.

Hinter der notwendigen Umbenennung der „speichernden“ bzw. in einigen Ländern „datenverarbeitenden“ Stelle in „verantwortliche Stelle“ steckt mehr als Sprachästhetik, ohne daß der Änderungsentwurf dies aufnimmt. Die Definition der Richtlinie stellt ausdrücklich auf die Entscheidung über Zwecke und Mittel der Verarbeitung von personenbezogenen Daten ab, nicht wie das derzeitige deutsche Recht auf den technischen Vorgang der Speicherung. Die europäische Sichtweise ließe es zu, gerade vor dem Hintergrund der zunehmenden Verteilung von Datensammlungen auf die verschiedensten Träger zu klaren Zuordnungen der datenschutzrechtlichen Verpflichtungen zu kommen. Auch die bisher schon praktisch so behandelte Verantwortlichkeit von Konzernen für das immer stärker wuchernde Gestrüpp der ausgegründeten Unternehmenszweige ließe sich damit klar abbilden, ohne Figuren wie Auftragsdatenverarbeitung oder Funktionsübertragung überstrapazieren zu müssen.

Materielle Anforderungen

Entsprechend den Vorgaben der Europaratskonvention von 1981, die insbesondere vom britischen Datenschutzrecht aufgegriffen wurde, enthält die Richtlinie "Grundsätze in bezug auf die Qualität der Daten". Der Änderungsvorschlag übernimmt diese Prinzipien nicht, wohl in der Annahme, daß die darin enthaltenen Prinzipien sehr allgemein gehalten und ohnehin in Einzelregelungen umgesetzt werden müssen. Gleichwohl können programmatische Aussagen wie etwa diejenige, daß die Daten „fair“ (die deutsche Übersetzung „nach Treu und Glauben“ reduziert dies mißverständlicherweise auf den zivilrechtlichen Aspekt) und „auf rechtmäßige Weise“ verarbeitet werden müssen, gleichwohl bei der Interpretation der Bestimmungen im einzelnen hilfreich sein. So ist durchaus nicht zwingend, daß die Verarbeitung personenbezogener Daten, die dem Befugniskatalog des Datenschutzgesetzes oder anderer Gesetze entsprechend durchgeführt wird, tatsächlich auch das Kriterium der Fairneß erfüllt. Auch wäre eine Klarstellung im deutschen Gesetz wünschenswert, daß die Verarbeitung rechtswid-

rig erhobener Daten nicht zulässig ist - dieser im anglo-amerikanischen Recht geläufige Grundsatz wird hier immer wieder in Frage gestellt.

Die besondere Behandlung „sensibler“ Daten in der Richtlinie ist ebenfalls bereits in der Europaratskonvention angelegt und sogar in die UNO-Richtlinien von 1990 übernommen worden (die interessanterweise die einfache Mitgliedschaft in einer „association“ bereits als sensibles Datum betrachten). Es wird sicherlich nicht ausreichen, diese besonderen Daten beiläufig zu erwähnen und dann lediglich bei der Verwertung für private Zwecke (insbesondere zur Werbung) eine Vermutung zu begründen, daß die Verarbeitung dieser Daten gegen das schutzwürdige Interesse der Betroffenen verstößt. Eine der interessantesten Fragen ist, ob nicht die Richtlinie zwingend die Verarbeitung personenbezogener Daten durch Religionsgesellschaften einbezieht. Dies müßte zu einer Modifizierung der deutschen Regelung führen, die die Religionsgesellschaften gänzlich aus dem Geltungsbereich ausklammert.

Auch die in den Änderungsvorschlägen zum Ausdruck kommende Auffassung, das bisherige Medienprivileg könne - wenn auch als rahmenrechtliche Regelung - beibehalten werden, ist mit der Richtlinie nicht vereinbar. Vielmehr ist danach die Privilegierung der Medien auf die Fälle zu beschränken, in denen diese sich „als notwendig erweist, um das Recht auf Privatsphäre mit den für die Freiheit der Meinungsäußerung geltenden Vorschriften in Einklang zu bringen“ - was schwerlich eine Vollprivilegierung der journalistischen Tätigkeit meinen kann.

Rechte der Betroffenen

Bei den Rechten, die den Betroffenen gegenüber der verantwortlichen Stelle eingeräumt werden, geht die Richtlinie wohl am weitesten über das hinaus, was das deutsche Datenschutzrecht bisher vorsieht. Außer einer Ausweitung der Auskunftsrechte und der Einführung erweiterter Informationsrechte enthalten vor allem das Widerspruchsrecht gegen (rechtmäßige) Datenverarbeitung (Art. 14) sowie das Recht, sich gegen automatisierte Einzelentscheidungen zu wenden (Art. 15), völlig neuartige Aspekte.

Gerade das Widerspruchsrecht wirkt auf den ersten Blick befremdlich, vom Innenministerium ist immer wieder darauf hingewiesen worden, daß es ge-

gen rechtmäßiges Verhalten von Behörden und Unternehmen keinen Widerspruch der Betroffenen geben könne. Allerdings gibt es bereits jetzt gewisse Ansätze: § 28 Abs. 4 BDSG erlaubt den Widerspruch gegen die Verwendung von Daten zu Werbezwecken, auch wenn diese grundsätzlich zulässig ist. In ähnlicher Weise lassen sich eine ganze Reihe von Fallkonstellationen denken, in denen ein derartiger Widerspruch aus persönlichen Gründen akzeptiert werden sollte, zumal wenn man das Widerspruchsrecht auch auf die Art der Verarbeitung der Daten erstrecken würde. So lassen sich gerade beim Arbeitnehmerdatenschutz Konstellationen denken, wo derartige Widersprüche ihren Sinn hätten, zumal wenn sie auch kollektiv vorgebracht werden könnten.

Das Verbot des französischen Datenschutzrechts, Entscheidungen ausschließlich auf die Ergebnisse automatisierter Verarbeitung zu stützen, das im übrigen in das Beamtenrechtsrahmengesetz Eingang gefunden hat (§ 56 f Abs. 4), ist in die Richtlinie in abgeschwächter Form aufgenommen worden. Hiernach muß jeder Person das Recht eingeräumt werden, keiner für sie negativen Entscheidung unterworfen zu werden, die ausschließlich auf Grund einer automatisierten Verarbeitung zum Zwecke der Bewertung einzelner Aspekte der Person ergeht. Mithin wird hier auf die automatische Generierung von Bewertungen abgestellt, wie wir sie etwa beim Scoring im Zusammenhang mit Kreditkarten kennen. Der Änderungsvorschlag hält sich zwar an die Richtlinie, doch wäre es angemessener gewesen, die französische Vorgabe zu übernehmen: Nicht nur dann, wenn Bewertungen automatisch generiert werden, sondern auch dann, wenn Fakten erhoben und automatisch weiterverarbeitet werden (z. B. Geschwindigkeitskontrolle mit automatischer Erkennung des Kfz-Zeichens, Online-Zugriff auf die Fahrzeugdaten sowie automatischem Ausdruck des Verwarnungsbescheides), besteht ein Interesse, jedenfalls grundsätzlich eine Kontrolle durch eine verantwortliche Person sowie den Betroffenen vorzusehen. Solche Verfahren sind nicht nur bei pauschalisierten Entscheidungen im Straßenverkehr, sondern auch in vielen anderen Bereichen (wiederum z. B. im Arbeitsverhältnis, wo auf Grund automatischer Messung ohne Einschaltung anderer Personen Gehaltskürzungen vorgenommen werden könnten) denkbar.

Kontrolle des Datenschutzes

Eine der heftigsten Kontroversen über die Umsetzung der Richtlinie betrifft die Stellung und die Befugnisse der Datenschutzbeauftragten, in der Richtlinie „Kontrollstellen“ genannt. Zu begrüßen ist, daß im Laufe der Beratungen in die Richtlinie die internen (behördlichen und betrieblichen) Datenschutzbeauftragten nicht nur eingeführt, sondern gegenüber dem derzeitigen deutschen Recht auch noch mit weiteren Aufgaben und Befugnissen ausgestattet worden sind.

Die externen „Kontrollstellen“, die von den Mitgliedstaaten einzurichten sind, nehmen nach der Richtlinie „die ihnen zugewiesenen Aufgaben in völliger Unabhängigkeit“ wahr. Infolge der Grundstruktur der Richtlinie betrifft dies sowohl die Kontrolle über den öffentlichen als auch über den privaten Bereich. Die derzeitige Organisation der Datenschutzkontrolle in den meisten Bundesländern, in denen diese von einer in die Weisungsstränge der Ministerien eingebetteten Organisationseinheit (in der Regel ein Referat) wahrgenommen wird, ist hiermit nicht vereinbar. Entgegen der Vorlage des Bundesinnenministeriums wird dies vom Bundesjustizministerium ebenfalls so gesehen.

Daran ändert auch der Hinweis auf angebliche Protokollnotizen im zuständigen Ratsarbeitskreis nichts, nach denen mit dem Begriff „völlige Unabhängigkeit“ die Unabhängigkeit von der überprüften Stelle gemeint sein soll. Mit dieser Auffassung ist die deutsche Delegation allein geblieben. Auch spielen hinsichtlich des endgültigen Regelungsbedarfs Protokollnotizen keine Rolle. Für die Herauslösung der Aufsichtsbehörde für den privaten Bereich aus den ministeriellen Zusammenhängen spricht vor allem auch, daß die Richtlinie zwei Beratungsinstitutionen etabliert hat: Die Datenschutzgruppe einerseits, die aus den unabhängigen Kontrollstellen besteht (Art. 29), sowie einen Ausschuß, der sich aus den Vertretern der Mitgliedstaaten und somit aus Vertretern der zu kontrollierenden Ministerien zusammensetzt. Diese beiden Institutionen stehen daher in einem gewissen Spannungsverhältnis zueinander. Die mit der Richtlinie beabsichtigte Balance wäre dann gestört, wenn einzelne Staaten die gleichen Vertreter auf der einen und der anderen Seite sitzen hätten.

Den Kontrollstellen müssen wirksame Einwirkungsbefugnisse zur Verfügung gestellt werden, die sich nicht auf die bisher im deutschen Daten-

schutzrecht verankerten Befugnisse zur Mangelfeststellung und Beanstandung (nicht einmal letzteres ist im privaten Bereich vorgesehen) beschränken können. Diese sind nicht wirksam, wenn auch auf Drängen der deutschen Delegation als eine Alternative die Befugnis eingeführt wurde, „eine Verwarnung oder eine Ermahnung an den für die Verarbeitung Verantwortlichen zu richten“. Dem Sinn dieser Bestimmung kann es dem ganzen Kontext nach nur entsprechen, wenn über die Beratungsfunktion hinaus tatsächlich Eingriffsmöglichkeiten gewährt werden. Erwägungsgrund 63 der Richtlinie betont nochmals, daß die Kontrollstellen mit den notwendigen Mitteln für die Erfüllung dieser Aufgabe auszustatten sind, d. h. mit Untersuchungs- und Einwirkungsbefugnissen. Das, was das derzeitige deutsche Datenschutzrecht vorsieht und nach den Entwürfen beibehalten werden soll, wird dem - zumal vor dem Hintergrund der kommenden Entwicklung der Informationsgesellschaft - nicht gerecht.

Die Datenschutzrichtlinie der Europäischen Union

Alfred Büllesbach

Problemdarstellung

Die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr enthält in dem Erwägungsgrund 5 eine grundsätzliche Beschreibung des Anliegens.

„(5) Die wirtschaftliche und soziale Integration, die sich aus der Errichtung und dem Funktionieren des Binnenmarktes im Sinne von Art. 7a des Vertrages ergibt, wird notwendigerweise zu einer spürbaren Zunahme der grenzüberschreitenden Ströme personenbezogener Daten zwischen allen am wirtschaftlichen und sozialen Leben der Mitgliedstaaten Beteiligten im öffentlichen wie im privaten Bereich führen. Der Austausch personenbezogener Daten zwischen in verschiedenen Mitgliedstaaten niedergelassenen Unternehmen wird zunehmen. Die Verwaltungen der Mitgliedstaaten sind aufgrund des Gemeinschaftsrechts gehalten, zusammenzuarbeiten und untereinander personenbezogene Daten auszutauschen, um im Rahmen des Raums ohne Grenzen, wie er durch den Binnenmarkt hergestellt wird, ihren Auftrag erfüllen oder Aufgaben anstelle der Behörden eines anderen Mitgliedstaates durchführen zu können."

Dieser Erwägungsgrund beschreibt die Absicht, die Erwartung und die Dimensionen des Datenaustausches in europäischen und außereuropäischen Gebieten. Die sozialen und wirtschaftlichen Beziehungen haben sich internationalisiert und kommunizieren über globale Netzinfrastrukturen. Auf dieser Basis werden weltweit Kooperationen verabredet, findet weltweit Wirschaftsaustausch, Handel und Forschungskooperation statt. Mit dieser

Entwicklung und mit Unterstützung der Informationstechnik ist es darüber hinaus möglich, virtuell Unternehmen an verschiedenen Standorten zu etablieren. Dieser Prozeß ist ohne Informationstechnologie wirtschaftlich nicht mehr zu bewältigen. Neue Marktdynamik, verschärfter nationaler und internationaler Wettbewerb, neue Produkte, neue Geschäftsstrategien führen zum Wandel von Unternehmen und Unternehmensformen und zur Entwicklung neuer Informationstechnologiestrategien die in ein umfangreiches Informationsmanagement münden. Mehr und mehr setzt sich durch, daß ein solches ganzheitliches Informationsmanagement nicht mehr nur unter der technischen Perspektive reiner Sicherheit, sondern unter der umfangreichen Informationsaufbereitung und Bewertung einer Informationsordnung und den daraus zu ziehenden Erkenntnissen notwendig ist. In diesem Gesamtprozeß ist die Erkenntnis gereift, daß Information, ob personen- oder unternehmensbezogen, ein schützenswertes Gut ist.

Europa als Motor

Die Europäische Union hat diese Entwicklung frühzeitig aufgegriffen und in ein umfangreiches Regelungswerk, das sich mit vielfältigen Maßnahmen und Zielen beschäftigt, eingebettet. Ausgehend von einer zunehmenden wissenschaftlichen und technischen Zusammenarbeit, der Einführung neuer Telekommunikationsnetze und dem damit verbundenen grenzüberschreitenden Verkehr personenbezogener Daten ist die EU-Datenschutzrichtlinie in einem größeren Regelungszusammenhang zu sehen.

Unter dem Aspekt der Deregulierung sind zu nennen die Telekommunikationsendgeräterichtlinie vom 27. Mai 1988, die Richtlinie „Open Network Provision (ONP)“ vom 24. Juli 1990, die Telekommunikationsdienstrichtlinie vom 28. Juli 1996 und schließlich die Richtlinie zur Einführung des vollständigen Wettbewerbs vom 22. März 1996.

Getragen von den Gedanken des Schutzes geistigen Eigentums, des Urheberrechtes, des Schutzes personenbezogener Daten und der Privatsphäre sowie der Gewährleistung technischer und organisatorischer Sicherheit bei der Datenverarbeitung und in Netzen erließ die EU Schutznormen. Zu erwähnen sind die Richtlinie des Rates über den Rechtschutz von Computerprogrammen vom 14. Mai 1991 und in Ergänzung hierzu die EU-Datenbankrichtlinie vom 26. Februar 1996. Hinsichtlich des Datenschutzes geht

es um die hier im Zentrum stehende Datenschutzrichtlinie vom 24. Oktober 1995 und um die Telekommunikationsdatenschutzrichtlinie vom 15. Dezember 1997. Beide Richtlinien verpflichten die Mitgliedstaaten, die zu ihrer Umsetzung in nationales Recht erforderlichen Rechts- und Verwaltungsvorschriften bis zum 24. Oktober 1998 zu erlassen.

Struktur der Datenschutzrichtlinie

Die Struktur der EU-Datenschutzrichtlinie gliedert sich in allgemeine Bestimmungen (Art. 1 bis 4) in denen der Gegenstand der Richtlinie, Begriffsbestimmmungen, Anwendungsbereich und anwendbares einzelstaatliches Recht geregelt wird. Das Kapitel II regelt in 9 Abschnitten Bedingungen für die Rechtmäßigkeit der Verarbeitung personenbezogener Daten. Der Umfang erstreckt sich über die Art. 5 bis 21, wobei Grundsätze in bezug auf die Qualität der Daten, die Zulässigkeit der Datenverarbeitung, die Verarbeitung besonderer Kategorien personenbezogener Daten, die Information der betroffenen Person, Auskunftsrechte, Widerspruchsrecht, automatisierte Einzelentscheidung, Sicherheit der Verarbeitung sowie Meldeverfahren und Vorabkontrolle normiert werden. Das Kapitel III enthält Regelungen über Rechtsbehelfe, Haftung und Sanktionen (Art. 22 bis 24). Im Kapitel IV ist die Übermittlung personenbezogener Daten in Drittländer geregelt (Art. 25 und 26), die insbesondere unter dem Aspekt weltweiten Wirtschaftsaustausches von besonderer Bedeutung ist. Kapitel V sieht in Art. 27 vor, daß die Mitgliedstaaten und die Kommission die Ausarbeitung von Verhaltensregeln fördern. Das Kapitel VI befaßt sich mit der Kontrollstelle (Art. 28) und der Datenschutzgruppe (Art. 29 und 30). Schließlich regelt das Kapitel VII gemeinschaftliche Durchführungsmaßnahmen, zu denen im Art. 31 ein Ausschußverfahren und in den Art. 32 bis 34 Schlußbestimmungen zu nennen sind.

Rechtsgrundlagen dieser EU-Datenschutzrichtlinie sind Art. 100a EGV (Rechtsangleichung) und Art. 7a EGV (Verwirklichung des Binnenmarktes). Inhaltlich stützt sich die Richtlinie auf Art. 8 MRK in Verbindung mit Art. F Abs. 2 EUV (Schutz der Privatsphäre).

Inhalt der Richtlinie

Der Anwendungsbereich der Datenschutzrichtlinie erstreckt sich auf alle Verarbeitungen personenbezogener Daten, sobald die Tätigkeiten des für die Verarbeitung Verantwortlichen in den Anwendungsbereich des Gemeinschaftsrechts fallen. Ausnahmen (Art. 3 Abs. 2 EU-Richtlinie) sind die in den Titeln V und VI des Vertrages der Europäischen Union genannten Tätigkeiten wie die Öffentliche Sicherheit, die Landesverteidigung, die Sicherheit des Staates (einschließlich seines wirtschaftlichen Wohles, wenn die Verarbeitung die Sicherheit des Staates berührt), die Tätigkeit des Staates im strafrechtlichen Bereich und die Verarbeitung für eigene und familiäre Zwecke.

Voraussetzungen für die Zulässigkeit der Verarbeitung personenbezogener Daten sind in Art. 7 geregelt. Hierzu gehören die Einwilligung, die Erforderlichkeit zur Vertragserfüllung, rechtliche Verpflichtung des Verantwortlichen der Datenverarbeitung, die Wahrung lebenswichtiger Interessen der betroffenen Personen, die Wahrnehmung einer öffentlichen Aufgabe oder Ausübung öffentlicher Gewalt und die Verwirklichung berechtigter Interessen des Verantwortlichen der Datenverarbeitung, sofern nicht das Interesse des Betroffenen überwiegt.

Art. 8 regelt das Verbot der Verarbeitung bestimmter personenbezogener Daten, wozu Daten über rassische oder ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit und Sexualleben gehören. Jedoch sind zu diesem Grundsatz in Art. 8 Abs. 2 bis 4 und 7 Ausnahmen vorgesehen. Solche Ausnahmen sind die Einwilligung der betroffenen Person, die Notwendigkeit aus arbeitsrechtlichen Gründen, der Schutz lebenswichtiger Interessen des Betroffenen oder eines Dritten, die Verarbeitung im Rahmen der Mitgliedschaft in einer nichtwirtschaftlich tätigen Organisation, die Veröffentlichung durch die betroffene Person, die Verarbeitung der Daten im Rahmen der Gesundheitsvorsorge. Die Mitgliedstaaten können bei wichtigen öffentlichen Interessen weitere Ausnahmen vorgeben.

Verarbeitungsgrundsätze in bezug auf die Datenqualität sind in Art. 6 geregelt. Zu nennen sind die Verarbeitung nach Treu und Glauben und auf rechtmäßige Weise, die Verarbeitung für festgelegte eindeutige und rechtmäßige Zwecke (Art. 6 Abs. 1b und c), die Daten müssen sachlich richtig

und wenn nötig auf dem neuesten Stand sein, die Daten dürfen nicht länger als für die Realisierung des Zweckes erforderlich gespeichert und identifizierende Merkmale dürfen nicht länger als erforderlich aufbewahrt werden. Von diesen Prinzipien sind lediglich bezüglich der Weiterverarbeitung zu historischen, statistischen oder wissenschaftlichen Zwecken Ausnahmen zugelassen.

Der betroffenen Person sind bei der Datenerhebung die Verantwortlichen für die Datenverarbeitung zu nennen, auf die Zwecke, für die die Daten bestimmt sind, ist sie hinzuweisen und schließlich über Freiwilligkeit, Empfänger der Daten, Auskunftsrechte etc., zu informieren. Die betroffene Person hat ein Auskunftsrecht (einschließlich über den logischen Aufbau), ein Recht auf Berichtigung, Sperrung, Löschung (in der Regel einschließlich der Mitteilung der Dritten, an die die Daten übermittelt wurden) und Widerspruch (z. B. bei Weitergabe zu Werbezwecken).

Von besonderem Interesse ist schließlich die Zulässigkeit der Übermittlung personenbezogener Daten in Drittländer. Kriterium für die Bewertung der Zulässigkeit einer Übermittlung in ein Drittland (ein Land, das nicht Mitglied der EU ist) ist die Gewährleistung eines angemessenen Schutzniveaus in diesem Drittland. Dies wird nach folgenden Kriterien bewertet: Art der Daten, Zweckbestimmung, Dauer der geplanten Verarbeitung, Herkunfts- und Bestimmungsland, Rechtsordnung des Drittlandes, Standesregeln, Sicherungsmaßnahmen und weitere Umstände. Ist kein angemessenes Schutzniveau (Art. 25 Abs. 2) gewährleistet, so können abweichend hiervon Ausnahmen greifen und die Übermittlungen personenbezogener Daten in Drittländer dennoch rechtlich zulässig sein. Solche Ausnahmen sind die Einwilligung des Betroffenen, die Durchführung eines Vertrages zwischen der betroffenen Person und dem Verantwortlichen der Datenverarbeitung, die Erfüllung eines Vertrages im Sinne der betroffenen Person, die Wahrung wichtiger öffentlicher Interessen, die Geltendmachung von Rechtsansprüchen, die Wahrung lebenswichtiger Interessen der betroffenen Person, die Übermittlung aus öffentlichen Registern und die Genehmigung durch einen Mitgliedstaat nach Vorlage entsprechender Vertragsklauseln - wenn der für die Verarbeitung Verantwortliche ausreichend Garantien hinsichtlich des Schutzes der Privatsphäre, der Grundrechte und der Grundfreiheiten der Person sowie hinsichtlich der Ausführung der damit verbundenen Rechte bietet.

Wichtige Unterschiede zwischen der EU-Datenschutzrichtlinie und dem BDSG

1. Beim Begriff „personenbezogene Daten“ ist auf besondere Zuordnungen und mehrere spezifische Elemente (Ausdruck physischer, psychischer, psychologischer etc. Identität) abgestellt.

2. Der Dateibegriff ist neu formuliert und umfaßt die strukturierte Sammlung personenbezogener Daten ebenso wie die verteilten Datensammlungen.

3. Neu ist die Einführung des für die Verarbeitung Verantwortlichen, wobei auf die Entscheidungsbefugnisse über Zwecke und Mittel abgestellt wird.

4. Insbesondere unter dem Aspekt der Datenverarbeitung im Auftrag ist die Definition des Dritten bedeutsam. Dritter ist nicht, wer unter der unmittelbaren Verantwortung des Verantwortlichen der Datenverarbeitung Daten verarbeitet.

5. Die Einwilligung der betroffenen Person enthält keine Vorschrift über die Form der Einwilligung.

6. Die Beschränkungen des Anwendungsbereiches nach Art. 3 Abs. 2 sind im BDSG nicht vorgesehen.

7. Im Vergleich zum BDSG enthält Art. 4 ein Kollisionsrecht hinsichtlich des anwendbaren Rechtes bei grenzüberschreitender Verarbeitung der Mitgliedstaaten.

8. Bei der Erhebung personenbezogener Daten bei der betroffenen Person sieht die EU-Richtlinie Informationen vor über die Identität des für die Verarbeitung Verantwortlichen, die Zweckbestimmung der Verarbeitung und weitere Informationen wie beispielsweise die Empfänger, den Hinweis auf die Freiwilligkeit und auf das Bestehen von Auskunfts- und Berichtigungsrechten etc..

9. Nach Art. 15 besteht ein grundsätzliches Verbot automatisierter Einzelentscheidungen. Hiernach räumen die Mitgliedstaaten der betroffe-

nen Person ein, einer solchen automatisierten Entscheidung nicht unterworfen zu werden, wenn die Datenverarbeitung zum Zwecke der Bewertung einzelner Aspekte ihrer Person erfolgt, wie beispielsweise berufliche Leistungsfähigkeit, Kreditwürdigkeit, Zuverlässigkeit oder Verhalten.

10. Die EU-Richtlinie regelt keine Verpflichtung zur Bestellung eines betrieblichen Datenschutzbeauftragten, sieht aber die Möglichkeit der Bestellung vor (Art. 18 Abs. 2 EU-Richtlinie).

11. Hinsichtlich der Sicherheit der Verarbeitung wird in Art. 17 der für die Verarbeitung Verantwortliche verpflichtet, geeignete technische und organisatorische Maßnahmen durchzuführen, die erforderlich sind für den Schutz der Daten gegen die zufällige oder unrechtmäßige Zerstörung, den zufälligen Verlust, die unberechtigte Änderung, die unberechtigte Weitergabe oder den unberechtigten Zugang - insbesondere im Rahmen der Verarbeitung von Daten in einem Netz.

12. In Erweiterung von § 37 Abs. 2 BDSG, in dem die Bereitstellung einer Dateienübersicht geregelt ist, enthalten die Art. 18, 19 und 21 der EU-Richtlinie die Pflicht zur Einrichtung und Führung eines Registers über die Struktur und die Kategorien der Datenverarbeitung bei einer Kontrollstelle oder bei einem Datenschutzbeauftragten.

13. Neu ist die Vorabkontrolle (Art. 20). Hiernach nehmen Vorabprüfungen die Kontrollstelle bzw. der Datenschutzbeauftragte vor Beginn der Verarbeitung bei spezifischen Risiken für Rechte und Freiheiten der Person vor.

14. Die EU-Richtlinie sieht eine Art modifizierte Gefährdungshaftung mit der Möglichkeit der Beweislastumkehr auch im privatwirtschaftlichen Bereich vor (Art. 23); § 8 BDSG regelt die Verschuldenshaftung mit Beweislastumkehr.

15. Betreffend die Übermittlung personenbezogener Daten an Drittländer bei Gewährleistung eines angemessenen Schutzniveaus (siehe obige Darstellung) enthält das BDSG keine ausdrückliche Regelung, aber es gibt eine herrschende Interpretation, nach der schutzwürdige Interessen nicht beeinträchtigt werden dürfen.

Ziel: Abbau von Wettbewerbshindernissen und Stärkung des Binnenmarktes

Das Ziel wird nur dann optimal erreicht, wenn die EU-Richtlinie in den Mitgliedstaaten möglichst einheitlich umgesetzt wird. Betrachtet man die gegenwärtigen Novellierungsdiskussionen in den Mitgliedstaaten, so zeigt sich jedoch, daß nationale Besonderheiten deutlich in die neuen Regelungen Eingang finden. Für den europaweiten Wirtschaftsverkehr ist das genannte Ziel der Schaffung eines europäischen Wettbewerbsraumes ohne Wettbewerbsverzerrungen allerdings nur mit einer einheitlichen Datenschutzstruktur zu erreichen. Dies gilt für den allgemeinen Datenschutz ebenso wie für spezifische Datenschutzregelungen, z. B. Telekommunikationsdatenschutz.

Von besonderem Interesse wird schließlich künftig die Umsetzung der Regelungen in Art. 25 und 26 der EU-Richtlinie sein. Die gegenwärtig geführten Gespräche zwischen Europa und den Vereinigten Staaten zeigen die Schwierigkeiten auf, die bestehen, wenn es darum geht, in einem Drittland festzustellen, ob ein angemessenes Schutzniveau besteht. Die Lösung dieses Problems ist für die Entwicklung von Wirtschaftsbeziehungen von großer Bedeutung und gilt nicht nur für die Beziehung zwischen Europa und den Vereinigten Staaten, sondern ebenso für andere Wirtschaftszentren dieser Welt, z.B. Japan, China und den gesamten asiatischen Raum.

Das Ende der Nationalstaaten im Netz

Joachim Rieß

1. Globalisierung

Motor der Globalisierung sind die Finanzmärkte. Die Telekommunikation ermöglicht eine Form der Globalisierung der Finanzmärkte, die die räumliche Trennung der Märkte tendenziell aufhebt und ihre Ungleichzeitigkeit auf die Stunden der Zeitverschiebung der Eröffnung der verschiedenen weltweiten Börsenplätze reduziert. Die Kommunikationstechnologie bildet die Infrastruktur für die Globalisierung. Der elektronische Geschäftsverkehr vereinfacht die Geschäftsabwicklung und beschleunigt die Reaktionsfähigkeit. Er ist für internationale Geschäfte besonders geeignet und eröffnet den Anbietern neue Märkte. Die Kommunikationstechnologie hat für die Neukonfiguration der gegenwärtigen Weltwirtschaft eine fundamentale Bedeutung. Man muß jedoch einem technologischen Determinismus widerstehen. Sowohl auf der Makro- als auch auf der Mikroebene können Informationstechnologien in einer Vielzahl von Organisationsformen strukturiert sein. Ohne der Weltwirtschaft eine besondere Struktur aufzuzwingen, bietet die Telekommunikation eine Basis für ganz unterschiedliche Prozesse der Internationalisierung, Transnationalisierung und Globalisierung.[1] Umgekehrt aber ist die Globalisierung, wie wir sie heute erleben, im Sinne der tendenziellen Aufhebung von zeitlichen und räumlichen Trennungen auf diesem Globus ohne die Telekommunikation nicht möglich.

[1] Gordon: Wie Globalisierung zu meistern ist, in: Fricke (Hrsg.): Jahrbuch Arbeit und Technik 1997, S. 58 (59).

2. Nationalstaaten

Der Globalisierung der Finanz-, Produktions-, Dienstleistungs- und Absatzmärkte stehen weiterhin Nationalstaaten oder Staatengemeinschaften - wie die EU - gegenüber. Deren Souveränität ist durch die globalen Verflechtungen stark eingeschränkt. Das Gewaltmonopol, gebunden an das Territorialprinzip, greift bei globalen Akteuren häufig nicht.

Ich möchte dies am Beispiel des Devisenhandels verdeutlichen: Das Volumen weltweiter Devisentransaktionen wird auf etwa 1,3 Billionen US-Dollar täglich geschätzt?[2] Keine Regierung verfügt über die Devisenreserven, um in diese Transaktionen wirksam eingreifen zu können. Ein Staat kann mit Hilfe seiner Reserven höchsten einen Teil der Kapitalströme in eine bestimmte Richtung lenken und so Wechselkursanpassungen verzögern. Eine Anpassung an die Bedingungen, die dem Markt durch die realen Gegebenheiten der jeweils aktuellen Wirtschaftslage aufgezwungen werden, kann er nicht verhindern.

Die Souveränität von Staaten hat ihre Grenzen. Über das Währungsgefüge wird nicht in den Hauptstädten, sondern an den Orten des Devisengeschäfts entschieden: Hongkong, Singapur, New York, London, Frankfurt. Ein wachsender Teil dieser Transaktionen wird elektronisch über Kommunikationskanäle abgewickelt, die sich den Bestrebungen der Regierungen, sie zu überwachen oder zu blockieren, entziehen.

Wir befinden uns in einer gesellschaftlichen Übergangsphase, die das Modell des modernen Nationalstaates, in Frage stellt. Der Nationalstaat ist ein Kind des westfälischen Friedens, der 1648 hier in Münster - zwischen dem Kaiser und den Franzosen ausgehandelt - mit folgenden Botschaften den 30jährigen Krieg beendete:

1. Jedes Land/jeder Monarch hat das Recht, einen eigenen autonomen, souveränen Staat zu bilden und seine Interessen nach eigenem Gutdünken zu verfolgen.

2. Jeder souveräne Staat kann seine inneren Angelegenheiten ohne Einmischung von außen regeln.

[2] Toulmin: Ursachen, Erscheinungsformen und Auswirkungen: Was ist Globalisierung, was nicht?, in: Fricke (Hrsg.): Jahrbuch Arbeit und Technik 1997, S. 15 (17).

3. Die gemeinsamen Merkmale der Bürger jedes Staates reichen aus, um eine Nation zu begründen.

Die politischen Theorien des Nationalstaates von Hugo von Grotius bis Max Weber formulierten Gesellschaft und Wirtschaft auf den jeweiligen Nationalstaat bezogen. Das Modell des bürgerlichen Staates also, des Gleichgewichts zwischen Citoyen und Bourgeois findet innerhalb des Nationalstaates statt. Dieses Modell funktioniert nicht mehr: Der Bourgeois ist aus dem Nationalstaat ausgetreten.

Global besteht hier ein Machtvakuum, das zunehmend durch eine neue Art von Organisationen gefüllt wird, den NROs - Nichtregierungsorganisationen. Dazu gehören Menschenrechtsorganisationen wie Amnesty, Hilfsorganisationen, Fachverbände und Wissenschaftsorganisationen, die multinational arbeiten. Dazu gehören auch die Task Forces (z. B. Internet Enginiering Task Force - IETF - und das CERT) im Internet, die ohne politische Macht und nichtkommerziell Aufgaben des Gemeinwohls wahrnehmen. Sie haben keine Macht im Sinne von Gewaltmonopol, sondern einzig moralischen Einfluß und Einfluß mittels Kompetenz.

Der Wandel der Kommunikationssysteme läßt, sei es über Satellit oder das Internet, nicht nur die multinationalen Medien, sondern auch die Nichtregierungsorganisationen (NROs) an Einfluß gewinnen. Auch nach 1945 haben viele Regierungen den Zugang zu internationalen Telefonleitungen beschränkt. Seit den siebziger Jahren aufgrund der Verfügbarkeit von Satelliten, Fax und heute des Internets sind ihre Kontrollmöglichkeiten erheblich geschrumpft.

In einem globalen, dezentral organisierten Netz wie dem Internet sind gezielt steuernde Eingriffe eines Nationalstaates nicht wirksam durchsetzbar. Die Internetfreaks pflegen aufgrund dessen den Mythos, daß das Internet ein gesetzesfreier Raum sei. Dies ist ein Mythos, aber trotzdem richtig. Für Handlungen im Internet finden zwar Gesetze Anwendung, doch sind sie häufig nicht durchsetzbar. Der Nationalstaat stößt hier im wahrsten Sinne des Wortes an seine Grenzen. Die hoheitliche Gewalt bezieht sich immer auf ein Territorium. Das Internet ist ein neuer „körperloser Sozialraum“, der sich dem Territorialbegriff entzieht. In diesem Raum gibt es kein nationalstaatliches Gewaltmonopol und keine Souveränität. An diesem Mangel der Rechtsdurchsetzung kann eine nationale Gesetzgebung allein nichts ändern.

In der Netzwelt wird sich der Nationalstaat an Ohnmachtserfahrungen gewöhnen müssen. [3]

3. Das Ende des nationalstaatlichen Datenschutzkonzeptes muß der Anfang eines mehrseitigen multinationalen Datenschutz- und Sicherheitskonzeptes sein

Was hat das mit Datenschutz zu tun? Das Datenschutzkonzept ist immer noch ein nationalstaatliches - trotz der EU-Richtlinie. In Deutschland hat das Recht auf informationelle Selbstbestimmung, als Ausfluß des allgemeinen Persönlichkeitsrechtes, Grundrechtsqualität. Bis Anfang der neunziger Jahre stand im Mittelpunkt des Datenschutzes das Verhältnis Bürger - Staat. Höhepunkt war das Volkszählungsurteil. Der Schwerpunkt neuer datenschutzrelevanter Fragen verlagert sich auf das Verhältnis Kunde und Anbieter. Im Verhältnis Bürger - Staat sind die Datenschutzregelungen als Rechte des Bürgers und Begrenzung des Gewaltmonopols und der Eingriffsrechte des Staates in ihrer Ausrichtung eindeutig. Sie entsprechen auch dem Gleichgewichtsmodell des demokratischen Rechtsstaates. Der breite Konsens in der Ablehnung der Volkszählung liegt hier begründet.

Im Verhältnis Kunde - Anbieter sind Beziehungen und Interessen vielschichtiger. Datenschutz ist Bestandteil der privatautonomen Gestaltung der Rechtsbeziehungen, sei es durch Einwilligung oder Vertrag. Meistens beinhalten die Vertragsbeziehungen nur incidenter den Umfang der zulässigen Datenverarbeitung. Die Vereinbarungen werden zudem bestimmt von Marktmacht.

1991 wurden mit der Telekommunikationsdienste-Unternehmens-Datenschutzverordnung (TUDSV) erstmals bereichspezifische Regelungen im Telekommunikationsdatenschutz geschaffen, die explizit den Datenschutz im Verhältnis zwischen bestimmten privaten Unternehmen und den Kunden regelten. Der dogmatische Ausgangspunkt ist hier neben dem Datenschutz das Fernmeldegeheimnis. Mit dem Teledienstedatenschutzgesetz im Informations- und Kommunikationsdienstegesetz sind im August 1997 weitere Regelungen hinzugekommen. Diese gesetzgeberischen Aktivitäten lassen eine Schwerpunktverlagerung in der öffentlichen Wahrnehmung erkennen.

[3] Roßnagel: Globale Datennetze: Ohnmacht des Staates - Selbstschutz des Bürgers, ZRP 1997, S. 26 (27).

Sowohl Verbraucher, die öffentliche Verwaltung als auch Unternehmen müssen darauf vertrauen können, daß ihre Transaktionen nicht abgefangen, ausgewertet oder verändert werden. Für die elektronische Kommunikationskultur sind Sicherungen der Integrität, der eindeutigen Urheberschaft und der Vertraulichkeit wie sie in der Schriftkultur mit Briefumschlag, Unterschrift, Stempel und Siegel jahrhundertelang gepflegt wurden, noch nicht etabliert. Dabei birgt die elektronische Kommunikation neue und andere Risiken der Manipulation, des Bruchs der Vertraulichkeit und der Ausforschung des Kommunikationsverhaltens. Für die weitere Entwicklung des elektronischen Geschäftsverkehrs kommt es maßgeblich darauf an, daß folgende Fragen einer Lösung zugeführt werden: Eindeutige Identifikation des Vertragspartners, vertrauliche Datenübermittlung, Verbindlichkeit und Beweisbarkeit einer elektronischen Willenserklärung sowie sichere Zahlungsverfahren. Es bedarf einer mehrseitigen Sicherheit als integralem Bestandteil der Kommunikationstechnik.[4] Neben einem Systemschutz (anonymes und pseudonymes Browsing) bedarf es der Selbstschutztechniken (Zugriffsschutztools, Verschlüsselungstools), die die Nutzer selbstverantwortlich einsetzen müssen.[5] Dem Nutzer müssen vertrauenswürdige Dienstleistungen z. B. von Trusted Third Parties bzw. Zertifizierungsstellen angeboten werden.

Der Datenschutz wird in der Telekommunikation zu einem Element einer mehrseitigen Sicherheit als integralem Bestandteil der Kommunikationstechnik.

Diese mehrseitige Sicherheit muß multinational und global auf verschiedenen Ebenen etabliert werden: Im Bereich der multinationalen Unternehmen, auf der Ebene multinationaler Vereinbarungen zwischen den Staaten [6] und auf der Ebene von Nichtregierungsorganisationen.

[4] Müller/Pfitzmann (Hrsg.): Mehrseitige Sicherheit in der Kommunikationstechnik - Zusammenfassendes Resultat des von der Gottlieb Daimler- und Karl Benz-Stiftung geförderten Kollegs „Sicherheit in der Kommunikationstechnik“, Juli 1997.

[5] Büllesbach/Garstka: Systemdatenschutz und persönliche Verantwortung, in: Müller/ Pfitzmann (Hrsg.), a.a.O.

[6] KOM (97) 503 Mitteilung der Kommission an den Rat: Sicherheit und Vertrauen in elektronische Kommunikation - ein europäischer Rahmen für digitale Signaturen und Verschlüsselung.

4. Privacy enhancing technology

Es entsteht ein globaler Markt von Privacy enhancing technology (PET) und vertrauenswürdigen Dienstleistungen. Dieser Markt muß gefördert, nicht behindert werden. Dieser Markt braucht den aufgeklärten Nutzer. Dem Nutzer müssen Instrumente an die Hand gegeben werden, um seine informationelle Selbstbestimmung technisch wahren zu können. Eine Schlüsseltechnologie im wahrsten Sinne des Wortes für PET ist die Kryptographie. Sie ist die Kulturtechnik für die elektronische Kommunikation zum Schutz der Vertraulichkeit, der Urheberschaft und der Integrität - vergleichbar Briefumschlag und Siegel. Kryptographische Verfahren dienen sowohl dem Schutz der Ausübung von Grundrechten als auch der Rechtssicherheit.

Die internationale Auseinandersetzung um die Regulierung des Einsatzes kryptographischer Verfahren, das Exportverbot der USA, die Genehmigungsverfahren für den Einsatz kryptographischer Verfahren in Frankreich kreist um den Versuch, das nationalstaatliche Gewaltmonopol in den Netzen wiederherzustellen. Natürlich können Verschlüsselungsverfahren für kriminelle Zwecke verwendet werden. Aber die Verschlüsselungsverfahren sind veröffentlicht und keiner kann daran gehindert werden, sie zu nutzen. Genehmigungsverfahren, Key Recovery und Schlüsselhinterlegung werden keinen Kriminellen an der Nutzung von Verschlüsselungsverfahren hindern. Es wäre ungefähr so, als wenn man den Bankräuber nach seinem Waffenschein fragen würde. Aber es geht hier um mehr, als um das richtige Mittel der Kriminalitätsbekämpfung. Die Kryptokontroverse hat eine hohe symbolische Bedeutung. Es geht um den - untauglichen - Versuch das nationalstaatliche Gewaltmonopol im Netz herzustellen.

5. Überwachung im Netz

Das Recht auf informationelle Selbstbestimmung und das Fernmeldegeheimnis als klassische Grundrechte gegenüber dem Staat bleiben trotz der dargestellten Veränderungen relevant. Von der Öffentlichkeit fast unbemerkt sind eine Vielzahl neuer Überwachungsvorschriften in das Telekommunikationsgesetz aufgenommen worden, zuletzt mit dem Telekommunikationsbegleitgesetz. Vorgeblich sollten nur die Ermittlungs- und

Abhörbefugnisse des Staates unter den neuen Bedingungen der Deregulierung gewahrt werden.
Tatsächlich sind die Abhörmöglichkeiten ausgeweitet worden. Mir scheint das geradezu eine Folge der staatlichen Ohnmachtserfahrungen nach dem Motto zu sein: Wir wissen zwar nicht genau, was da läuft, aber wir müssen potentiell alles überwachen können. Eine Sichtweise, die der Exekutive leichtfällt, da es für sie kostenneutral ist. Zahlen muß diese Überwachungsinfrastruktur die Wirtschaft. Dabei mangelt es an ganz anderem. Wieviel Ermittlungsbehörden haben Internetanschlüsse und das entsprechende technische Equipment ?

Die Betreiber von Telekommunikationsanlagen haben grundsätzlich auf eigene Kosten die technischen Einrichtungen zur Umsetzung von gesetzlich vorgesehenen Überwachungsmaßnahmen zu gestalten und vorzuhalten (§ 88 Abs. 1 TKG). Bislang waren nach § 100 b Abs. 3 StPO, Art. 1 Abs. 2 G10 und § 39 Abs. 1 Außenwirtschaftsgesetz nur Betreiber von Fernmeldeanlagen, die für den öffentlichen Verkehr bestimmt sind, zur Bereitstellung der technischen Vorrichtungen für Abhörmaßnahmen verpflichtet. Die Überwachungseinrichtungen müssen im Einvernehmen mit der Regulierungsbehörde gestaltet werden und der Betrieb der Telekommunikationseinrichtung darf erst aufgenommen werden, wenn die Überwachungseinrichtungen funktionstüchtig installiert sind und dies der Regulierungsbehörde schriftlich angezeigt wurde.

Nach dem Begleitgesetz zum TKG ist jeder, der geschäftsmäßig Telekommunikationsdienste erbringt oder an der Erbringung solcher Dienste mitwirkt, dazu verpflichtet. Bislang sind Betreiber, die Telekommunikationsanlagen anderen geschäftlich überlassen, zur Überwachung und der Bereitstellung entsprechender Einrichtungen erst auf Anforderung der Ermittlungsbehörden oder Bedarfsträger verpflichtet. Zukünftig sollen alle, die geschäftsmäßig Telekommunikationsdienste erbringen oder an der Erbringung mitwirken - das ist sehr weit gefaßt - präventiv entsprechende Überwachungseinrichtungen in ihre Telekommunikationseinrichtungen einbauen.

Weiterhin sind diejenigen, die Telekommunikationsdienste geschäftsmäßig anbieten, verpflichtet, Kundendateien zu führen, auf die die Ermittlungs- und Sicherheitsbehörden über die Regulierungsbehörde online Zugriff haben. Die Abrufverfahren müssen so gestaltet werden, daß die Anbieter von

den Zugriffen auf ihre eigenen Kundendaten keine Kenntnis erlangen können. Die Kosten für die Überwachungseinrichtungen müssen von den Betreibern getragen werden. Diese Art des unmittelbaren behördlichen Zugriffs auf private Daten ist einmalig.

Auf Kosten der Betreiber und zu Lasten des Telekommunikationspartners soll hier eine unverhältnismäßige Überwachungsinfrastruktur vorgehalten werden. Um mit Max Weber zu sprechen, wird hier das Gehäuse der Hörigkeit der Zukunft geschaffen.[7] Wer ist sich sicher, daß der gewaltige Transformationsprozeß in die Informationsgesellschaft immer in demokratischen Bahnen verläuft?

6. Eine Nichtregierungsorganisation für den Datenschutz

Das Konzept einer mehrseitigen Sicherheit ist auf vielseitige Vereinbarungen angelegt unter Einbeziehung der Technikgestaltung, eines Dienstleistungsmarktes für vertrauenswürdige Kommunikation und eines multinationalen Ordnungsrahmens mit unabhängigen Institutionen, die dies kontrollieren. Die Interessen für die unterschiedlichen Elemente einer mehrseitigen Sicherheit sind unterschiedlich ausgeprägt. Gerd Heidenreich hat einen schönen science fiction geschrieben: „Die Nacht der Händler“. In diesem Roman wird die Welt zu Beginn des nächsten Jahrtausends beschrieben. Umspannt von einem dichten Netz der Datenkommunikation zeichnet sich eine globale Katastrophe ab: auf unbegreifliche Weise verschwinden Geldmengen auf dem Weg von Börse zu Börse auf den Computern, lösen falsche Aktienkurse Panikverkäufe aus, werden Bankvermögen wie von schwarzen Löchern verschluckt. Die Spur führt zu einer Sekte zurück, die Ende der neunziger Jahre allen Bildmedien und künstlichen Welten den Kampf angesagt hatte.

Die Sicherheit des elektronischen Geschäftsverkehrs ist Thema. Der Schutz der Persönlichkeitsrechte muß genauso Thema werden. Ein neuer science fiction für den Datenschutz nach George Orwell steht noch aus.

[7] Weber: Wirtschaft und Gesellschaft, Tübingen 1980, S. 835.

7. Thesen

1. In der globalen Netzwelt gibt es kein nationalstaatliches Gewaltmonopol und keine Souveränität. Der demokratische Rechtsstaat wird sich hier an Ohnmachtserfahrungen gewöhnen müssen.

2. Das Ende des nationalstaatlichen Datenschutzkonzeptes muß der Anfang eines mehrseitigen multinationalen Datenschutz- und Sicherheitskonzeptes sein.

3. Es entsteht ein globaler Markt von Privacy enhancing technology (PET) und vertrauenswürdigen Dienstleistungen.

4. Mehrseitige Sicherheit und Datenschutz muß multinational und global auf verschiedenen Ebenen etabliert werden. Im Bereich der multinationalen Unternehmen, auf der Ebene multinationaler Vereinbarungen zwischen den Staaten und auf der Ebene von Nichtregierungsorganisationen.

5. Die Eigenverantwortung des Anwenders muß gestärkt werden. Er muß unbeschränkt Selbstschutztechniken einsetzen können. Kryptographische Verfahren als eine wichtige Sicherungstechnologie zum Schutz von Daten in der Telekommunikation müssen Anwendern und Anbietern ohne staatliche Beschränkungen und Eingriffe zur Verfügung stehen.

6. Die Kryptokontroverse hat eine hohe symbolische Bedeutung. Es geht um den - untauglichen - Versuch, das nationalstaatliche Gewaltmonopol im Netz herzustellen.

7. Die gesetzlichen Überwachungsmöglichkeiten in Deutschland für Telekommunikationsnetze sind überzogen und müssen auf ein angemessenes Maß zurückgeführt werden.

Datenschutz im Zeitalter von Globalisierung und gesellschaftlichem Kontrollbedürfnis

Andy Müller-Maguhn

Zunächst möchte ich versuchen, den Paradigmenwechsel in der Welt der IUK-Technologie und der gesellschaftlichen Ausgangslage ein wenig zu erläutern und auf die Thematik des Datenschutzes zu übertragen. Der Begriff Paradigmenwechsel ist ja gerade etwas in Mode gekommen, wird aber oft nur verstanden als die Veränderung von einer bestimmten Art und Weise die Dinge zu sehen zu einer anderen. Ich assoziiere mit dem Begriff Paradigmenwechsel eher eine Dauerveranstaltung, weil die Entwicklung der Informationstechnologie vor allem eine Beschleunigung der Entwicklung selbst zur Folge hat. Übertragen auf den Begriff des Datenschutzes, bzw. dem aus der Verfassung abgeleiteten Recht auf informationelle Selbstbestimmung hat sich nicht nur die technologische Grundlage verändert, sondern vor allem das Selbstverständnis des Staates, die diesbezügliche Betrachtungsweise und insofern auch etwas die Gefahrenlage für den Umgang mit persönlichen Daten.

Vom Bild der gemeinsamen Infrastruktur, der Gewährung von Grundrechten und der demokratischen Institution Staat her sind die Stichworte heute nicht nur Globalisierung, sondern vor allem Neoliberalismus und das Selbstverständnis des Staates zur Erstellung wirtschaftlich sinnvollstmöglicher Rahmenbedingungen, um vor allem das eine zu schaffen: Arbeitsplätze. Wenn man die Bangemannsche Vision von der Informationsgesellschaft in wenigen Worten zusammenfassen möchte, so lautet die Kurzformel: Liberalisierung der Märkte + Informationstechnologie = Arbeitsplätze. Das Stichwort „Arbeitsplätze“ scheint mir eine Art Zauberwort zu sein, auf das Politiker dressiert sind. Wenn man Politiker zu einer bestimmten Handlung bringen möchte, muß man Ihnen offensichtlich nur erklären, dies würde zu vielen neuen Arbeitsplätzen führen.

Insofern scheinen mir die Forderungen der 70er und 80er Jahre, wie etwa die nach einer maschinenlesbaren Regierung zwar nicht überholt, aber doch aus einem Weltbild stammend, wo die Bedrohung der „Staat“ mit seinem „Gewaltmonopol“ war und die Orwellsche Vision zur Sensibilisierung diente. Diese Negativkultur hat natürlich auch Ihre Nachteile; das daraus abgeleitete Recht auf informationelle Selbstbestimmung wurde jedenfalls nur bedingt als Leitbild der Entwicklung adaptiert. Oder, um es kürzer zu formulieren, damit es so etwas wie den Überwachungsstaat als Negativ-Leitbild geben kann, setzt dies die Existenz des Staates in einer bestimmten Form zunächst einmal voraus. Ob diese Existenz in den Visionen des Neoliberalismus noch enthalten ist, wage ich zu bezweifeln.

Die heutige Entwicklung mit den Auseinandersetzungen um Reglementierung von Kryptographie etwa geht insofern nicht unbedingt davon aus, daß die Bedrohung vom nationalen Überwachungsstaat ausgeht; vielfältige Interessen der Wirtschaftsspionage und der weltweiten Überwachung sind am Beispiel der Vorgehensweise der Regierung der USA ablesbar. Der Export von kryptographischen Produkten - also Verschlüsselungstechnik - war ja in den USA schon seit Jahrzehnten eingeschränkt. Die Produkte unterlagen als Munition wie Waffen entsprechenden Einschränkungen - nur der Export solcher Kryptoprodukte war erlaubt, bei dem sichergestellt war, daß die amerikanischen Geheimdienste die verschlüsselten Informationen mitlesen konnten. Mit dem offiziellen Ende des kalten Krieges wurde auch die Legitimationsgrundlage der Geheimdienste verschoben und diese zunehmend für die Wirtschaftsspionage verpflichtet. Entsprechend veränderte sich die Gesetzeslage, so daß die Exportkontrolle nicht mehr dem Verteidigungsministerium (DOD - Department of Defense) unterliegt, sondern folgerichtig dem Wirtschaftsministerium (DOC - Department of Commerce).

Unter dem Gesichtspunkt der Wirtschaftsspionage macht der hier betriebene enorme Aufwand auch schon fast Sinn. Die Kosten des „globalen“ Telekommunikationsüberwachungssystems Echelon etwa, das von der NSA betrieben wird, lassen sich mit dem „Überwachungsstaat“ kaum rechtfertigen. Absurderweise ist das Argument „Überwachungsstaat“ heute in der politischen internationalen Diskussion ja ein vergleichsweise positives, das von den Vertretern der Regierung der USA beispielsweise gerne als Rechtfertigungsklausel zur Etablierung des Echelon-Systems und zur Krypto-Regulierung benutzt wird; um so jemanden wie unseren derzeitigen Bundesinnenminister Kanther auf seine Seite zu bekommen, ist das natürlich das „richtige“ Argument. Ob sich der Überwachungsstaat allerdings wirt-

schaftlich rechnet, oder ob es sich nicht letztlich um Wirtschaftskriege zwischen globalen bzw. multinationalen Konzernen handelt, die eher noch schlimmere gesellschaftliche Diskrepanzen zur Folge haben, sei zunächst einmal nur als Frage dahingestellt.

Eines glaube ich jedoch mit Gewißheit sagen zu können: Die technischen Probleme einer großflächigen Überwachung mit Hilfe modernster Techniken sind im Kern gelöst. Insbesondere der Hoffnungsschimmer der „Informationsüberflutung“, an dem u.a. das Ministerium für Staatssicherheit der ehemaligen DDR erkrankte, ist für die heutigen Geheimdienste kein Problem mehr. Die etwa im Internet verfügbaren Suchmaschinen zeigen, wie man auch mit großen Informationsmengen mit entsprechend intelligenten Suchalgorithmen sinnvoll gesuchte Informationen extrahieren kann. In Anbetracht dieser sehr wirkungsvollen Werkzeuge wurde auch das Grundprinzip der „Überwachung“ einem vollständigen Paradigmenwechsel unterworfen. Es werden nicht mehr gezielt einzelne Anschlüsse, Teilnehmer, Personen oder Organisationen überwacht, sondern der gesamte Fernmeldeverkehr wird von den Überwachungssystemen erfaßt. Telefongespräche beispielsweise unterlaufen den sog. „Wortbanken“, in denen die gesprochenen Worte mit gespeicherten Stichworten abgeglichen werden und dann entsprechend weiter verfahren wird. Insbesondere die verbleibende Speicherung der Verbindungsdaten aller verfügbaren Kommunikationsnetze ermöglicht es - unabhängig von den gesprochenen Worten und übermittelten Inhalten - über Jahre im nachhinein Organigramme und Kommunikationszusammenhänge aufzuzeigen.

Um jedoch die Betrachtung nicht nur auf die Welt der Geheimdienste und ihrer Überwachungssysteme zu beschränken und eine offensive Vorgehensweise zu betreiben, scheint es mir sinnvoll, zunächst einmal (m)ein Bild von der Entwicklung der Netze und den gesellschaftlichen Entwicklungen hin zur „Informationsgesellschaft“ zu malen: Zunächst einmal erleben wir eine Verlagerung von verschiedenen Lebensbereichen in die Netze. Nicht nur kommerzielle berufliche Aktivitäten, sondern auch die Gestaltung unseres Privatlebens und persönliche Beziehungen werden zunehmend mit Hilfe von Netzwerken und elektronischen Kommunikationsmitteln abgewickelt. Ein Teil des öffentlichen Lebens in der Informationsgesellschaft findet in den Netzwerken statt.

Die Verlagerung in die Welt der Netzwerke bedarf allerdings auch ähnlicher Grundrechte, wie wir sie im sog. „wirklichen Leben“ haben: Ein Recht auf

Teilhabe, vor allem aber auch auf Privatsphäre und gleichberechtigte Zugangsvoraussetzungen. Diese relativ hohen Ansprüche erfordern nicht zuletzt auch politische Strukturen, die sich die Durchsetzung dieser Rechte zu eigen machen und sich um die netz- und gesellschaftspolitischen Probleme kümmern. Die „konventionelle Politik“ und das System der repräsentativen Demokratie scheinen mir nach einigen Jahren Lobbyarbeit und dem Versuch, hier doch zumindest einige fruchtbare Gedanken zu säen, nur in Teilbereichen sinnvolle Institutionen für diese Aufgaben zu sein. Nicht nur, daß sie mit der erforderlichen Fachkompetenz nicht ausgestattet sind und einige Zusammenhänge schlicht nicht verstehen. Auch scheinen mir die Repräsentanten einfach überfordert bei dem Versuch, die notwendige Sachkenntnis in einer so unübersichtlichen Anzahl von Fachgebieten zu behalten und dabei auch noch den klaren Kopf für die zukunftskompatibelsten Entscheidungen zu bewahren.

Sinnvoller scheint mir da, zunächst das entsprechende gesellschaftliche Bewußtsein zu schärfen, und die notwendigen Strukturen für die Erlangung von allgemeiner Medienkompetenz und einen gleichberechtigten Zugang zu schaffen. Das sollte durchaus mit den technischen Mitteln zur Netzwerkkommunikation in der Grundschule anfangen. Die Dezentralisierung von Entscheidungsfindungsprozessen und die Immunisierung der Bevölkerung gegenüber Problembereichen scheint mir hier noch das sinnvollste und zukunftskompatibelste Konzept unserer Zeit zu sein. Das Internet stellt ja bereits ganz andere Mittel der Entscheidungsfindung exemplarisch zur Verfügung, wenn man auch zugeben muß, daß es sich nur bedingt um eine „demokratische“ Veranstaltung im Sinne einer repräsentativen Demokratie handelt. Das Stichwort „Kompetenzhierarchie“ ist hier wohl etwas treffender, wenn ich auch den wenig ausgeprägten Absolutheitsanspruch als positive Errungenschaft explizit erwähnen möchte. Das Prinzip der RFC´s (request-for-comment), bei dem jeder mitarbeiten kann, sich allerdings mit seinen Vorschlägen gegenüber den anderen durchsetzen muß, mag zwar minder demokratisch erscheinen, stellt aber zumindest sicher, daß das erforderliche fachliche Niveau vorhanden ist. Außerdem ist es im Gegensatz zu den Kungeleien einer „repräsentativen Demokratie“ eine deutlich transparentere Form der Entscheidungsfindung. Daß die so entstehenden Beschlüsse auch wieder nur RFC´s heißen („gilt, bis uns was besseres einfällt“), macht mir dieses Prinzip allemal sympathischer als das meiste, was ich dem Diskussionsstil in Bonn entnehme.

Gerade der Aspekt der Globalisierung, bzw. der Internationalisierung betrifft natürlich nicht nur die Begrenztheit nationaler Entscheidungsfindungsprozesse, sondern auch das Bewußtsein und die notwendig global zukunftskompatiblen Vorgehensweisen in vielen Bereichen, wie etwa im Datenschutz oder - um ein etwas plakativeres Beispiel zu wählen - im Bereich der Meinungsäußerung.

Es gibt hier zwei relativ gut trennbare Bereiche, die sich nicht nur am Problem der Meinungsäußerung erläutern lassen. Zum einen gibt es - schon historisch bedingt - unterschiedliche nationale Empfindlichkeiten. Wir Deutschen sind da - mit gutem Grund - gegenüber Nazi-Propaganda etwas sensibler als die amerikanische Regierung mit dem ersten Verfassungsgrundsatz der freien Meinungsäußerung (freedom of speech). Nun wird aber weder die amerikanische Regierung ihre Verfassung aufgrund deutscher Empfindlichkeiten ändern, noch wird die holländische Regierung ihren ebenfalls etwas weitergehenden Anspruch auf freie Meinungsäußerung aufgrund deutscher Empfindlichkeiten äußern. Der Umgang der deutschen Justizbehörden mit der auf einem holländischen Server abrufbaren Zeitschrift Radikal trifft die holländischen Empfindlichkeiten aufgrund ihrer Erfahrung mit der deutschen Justiz während des dritten Reiches an einer sensiblen Stelle.

Es gibt jedoch auch andere Beispiele, warum es nicht sinnvoll sein kann, sich auf den kleinsten gemeinsamen Nenner des Rechts auf freie Meinungsäußerung zu einigen. Wenn sich die chinesische Regierung etwa mit ihren Empfindlichkeiten und ihrer diesbezüglichen Vorgehensweise durchsetzt, würden die Auslandsredakteure des Spiegel vermutlich mit einem Genickschuß niedergestreckt werden.

Auf der anderen Seite - und das ist der erwähnte zweite Bereich - gibt es durchaus globale Empfindlichkeiten, die gleichermaßen gegen menschenunwürdige Angelegenheiten - wie Kinderpornographie - ein relativ geschlossenes Vorgehen bewirken. Im Internet - als einem etwas schnelleren Entwicklungsmedium im Gegensatz zur Welt der konventionellen Politik - gibt es ja schon etliche Jahre die Netiquette, die versucht ein global zukunftskompatibles Vorgehen durchzusetzen und sich gezielt gegen menschenunwürdiges, sexistisches und rassistisches Vorgehen ausspricht. Klar muß jedoch ebenfalls sein, daß es sich um ein Kommunikationsmedium handelt, in dem Streitkultur praktiziert wird und bei etwaigen Verstößen nicht gleich mit den Mitteln eines Polizeistaates vorgegangen wird.

Auch in der Welt des Datenschutzes kann man - leider - durchaus von sehr unterschiedlichen nationalen Empfindlichkeiten reden. Die Firma American Express wirbt beispielsweise im amerikanischen Fernsehen mit einem Spot, wo ein junger Mann sein ganzes Leben lang Holzfäller-Hosen trägt und sich von Zeit zu Zeit neue Holzfäller-Hosen mit seiner American Express Karte kauft. Eines Tages will er sich verheiraten und kauft sich nun - entgegen seiner sonstigen Gewohnheit - einen schwarzen Anzug mit entsprechender schwarzer Hose. Als er diese an der Kasse mit seiner American Express Karte bezahlen will, schlägt das American Express-System Alarm und er wird ans Telefon gebeten, seine Identität zu bestätigen - die freundliche Dame am Telefon erklärt ihm, man wundere sich über seinen Einkauf außerhalb des Profils und hätte einen Mißbrauch seiner Karte vermutet. Der Spot schließt mit den Worten „we care for you“ - der große Bruder umarmt dich sozusagen freundlich. Die andere Seite der Geschichte ist, daß American Express schon vor einiger Zeit verkündet hat, ihr Kerngeschäft bestünde nunmehr in der Vermarktung der Kundenprofile. Das Kreditkartengeschäft wird subventioniert von den bei den Transaktionen anfallenden Daten. Es mag sein, daß man in Amerika mit derartigem Vorgehen sogar noch Kunden werben kann, in Deutschland und auch in anderen Ländern bestehen da wohl schon gewisse Empfindlichkeiten, die einem derart dreisten Vorgehen einen Riegel vorschieben. Wenn ein deutscher Kunde allerdings ein amerikanisches Vertragsverhältnis mit Gerichtsstand in den USA eingeht, kann ihm deutsches Datenschutzrecht auch nicht helfen. Zudem läßt nicht nur die Firma AMEX, sondern es lassen auch viele deutsche Unternehmen wie etwa die Lufthansa ihre Daten vom weltweit größten Datenverarbeitungsdienstleister EDS (Electronic Data Systems) verarbeiten. Die Firma EDS hat Ihren Sitz in den USA, nur wenige Kilometer vom Hauptsitz der NSA entfernt und es gibt Leute, die behaupten, da gäbe es mehr als eine geographische Nähe. Ob das nun wahr ist, scheint mir relativ unerheblich angesichts der Gefahr, die von einer solchen Anballung von Datenbeständen über die Bewohner dieses Planeten ausgeht. EDS verarbeitet nicht nur die Daten vieler Telefongesellschaften, sondern beispielsweise auch des britischen Sozialversicherungssystems. Ich befürchte, daß an den Stellen, an denen derartige Datenbestände gehortet werden, auch Begehrlichkeiten entstehen, diese Daten als Kundenprofile zur zielgerichteten Manipulation von Kaufentscheidungen (ein etwas freundlicherer Begriff ist „Micro-Marketing“ oder „One-to-one Marketing“) zu mißbrauchen.

Im Bereich des Datenschutzes ist allerdings das entsprechende globale Bewußtsein nur bedingt ausgeprägt, das im Sinne der Technologieakzeptanz

Einfluß auf die diesbezügliche Gestaltung von Unternehmen haben könnte. Hier würde ich mir auch von Datenschutzbeauftragten noch mehr die Förderung der entsprechenden Transparenz wünschen, denn sind die Daten erstmal erfaßt, ist die weitere Verwendung oftmals faktisch unkontrollierbar. Zeitgemäß wäre vielleicht die Funktion eines Transparenzbeauftragten neben der Funktion der Datenschutzbeauftragten.

„Die Angabe persönlicher Daten schränkt ihre informationelle Selbstbestimmung ein“, wäre sozusagen ein adäquater Warnhinweis, ähnlich dem: „Rauchen gefährdet ihre Gesundheit“ in anderen Zusammenhängen. Im neuen Paradigma der Computer-Netzwerke werden nicht nur die Strukturen von freien Kommunikationszusammenhängen verstärkt. Nicht nur die Möglichkeiten einer umfassenderen Informationserlangung für den einzelnen steigen, auch die Marketingmechanismen der Aufmerksamkeitsvermarktung - bislang im „alten“ Medium Fernsehen dominant - haben neue Möglichkeiten.

Schließen möchte ich mit einem Zitat aus dem Roman „Schockwellenreiter“ von John Brunner, das mir noch viel zuwenig ins Bewußtsein eingebrannt zu sein scheint: „Wenn es so etwas wie das absolut Böse überhaupt gibt, besteht es darin, einen Menschen wie ein Ding zu behandeln.“

Und das gilt durchaus auch im Umkehrschluß.

Technik oder Recht - Neue Steuerungsinstrumente im Datenschutz

Johann Bizer

1. Rechtsziel des Datenschutzrechts

Das Rechtsziel des geltenden Datenschutzrechts ist der Schutz des einzelnen vor Beeinträchtigungen des *Persönlichkeitsrechts* durch die Erhebung, Verarbeitung und Nutzung seiner Daten. Als Beleg kann § 1 Abs. 1 BDSG (1990) dienen, wonach das Bundesdatenschutzgesetz den Zweck verfolgt ,

> *„den einzelnen davor zu schützen, daß er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird“.*

Dieser Schutz der „Privatsphäre natürlicher Personen bei der Verarbeitung personenbezogener Daten“ ist auch das Ziel der *EG-Datenschutzrichtlinie*, die sich „auf die in den Verfassungen und Gesetzen der Mitgliedstaaten sowie in der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten anerkannten Grundrechte“ stützt (Erwägungsgrund 1, 10).

Modernere Datenschutzgesetze - wie beispielsweise § 1 Nr. 1 HDSG (1986) oder § 1 DSG NW (1988) - orientieren sich in ihren Zweckbestimmungen stärker an dem Inhalt des *informationellen Selbstbestimmungsrechts* als der Befugnis „grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen“.[1] Das zentrale Instru-

[1] BVerfGE 65, 1, 43.

ment dieser Bestimmungsbefugnis ist die „Einwilligung“ des Betroffenen, zu welchen bestimmten Zwecken seine Daten erhoben, verarbeitet und genutzt werden dürfen.[2]

Allerdings unterliegt das Recht auf informationelle Selbstbestimmung einem *Gesetzesvorbehalt*, der den Gesetzgeber zur Einschränkung durch und aufgrund eines Gesetzes im überwiegenden Allgemeininteresse berechtigt, sich jedoch gegenüber den Anforderungen des *Verhältnismäßigkeitsprinzips* rechtfertigen muß.[3]

An diesen Maßstab ist der Gesetzgeber ebenfalls gebunden, wenn er Regelungen erläßt, die die Ausübung der informationellen Selbstbestimmungsbefugnis auch *gegenüber Privaten* sicherstellen. Derartige Regelungen können sich auf die Ausübung verfassungsrechtlicher Schutzpflichten stützen, die allerdings mit konfligierenden Grundrechten derjenigen, die zu eigenen Zwecken personenbezogene Daten Dritter erheben, verarbeiten und nutzen wollen, verhältnismäßig in Ausgleich zu bringen sind. Die unter dem Begriff der Drittwirkung diskutierten grundrechtsdogmatischen Rechtsfragen müssen hier nicht vertieft werden,[4] zumal die EG-Datenschutzrichtlinie eine unterschiedslose Anwendung des Datenschutzrechts auf öffentliche und nicht-öffentliche Stellen fordert. Es genügt hier die Feststellung, daß das Regelungsziel des geltenden Datenschutzrechts - gestützt auf geltendes Verfassungsrecht - die Wahrung der informationellen Selbstbestimmung derjenigen ist, deren Daten durch Dritte erhoben, verarbeitet und genutzt werden.

2. Klassische Steuerungsinstrumente des Datenschutzrechts

Mit welchen Steuerungsinstrumenten versucht nun aber der Gesetzgeber, das informationelle Selbstbestimmungsrecht der Betroffenen zu schützen?

Das klassische Regelungsinstrument des staatlichen Datenschutzrechts ist das *präventive Verbot mit Erlaubnisvorbehalt* der Datenverarbeitung und

[2] Bizer, Forschungsfreiheit und Informationelle Selbstbestimmung, S. 139 f.
[3] BVerfGE 65, 1. 43 f.
[4] Bizer (Fußn. 2), S. 296 ff.

Nutzung, die nur auf der Grundlage einer ausreichenden Rechtsvorschrift oder aufgrund der Einwilligung des Betroffenen zulässig ist. Charakteristisch ist die Formulierung des § 4 Abs. 1 BDSG (s. a. § 13 DSG NW). Danach sind

> *„Verarbeitung personenbezogener Daten und deren Nutzung nur zulässig (...), wenn dieses Gesetz oder eine andere Rechtsvorschrift sie erlaubt oder soweit der Betroffene eingewilligt hat“.*

Dieselbe Konstruktion findet sich auch in neueren Datenschutzregelungen wie beispielsweise in § 3 Abs. 1 TDDSG oder § 12 Abs. 2 MD-STV.

Anknüpfungspunkt des staatlichen Datenschutzrechts ist der *Zweck* der Datenerhebung und -verarbeitung. Das Prinzip der Zweckbindung folgt der Einsicht, daß die Bedeutung eines Datums - und damit auch seine persönlichkeitsrelevante Bedeutung - sich erst aus seinem jeweiligen Kontext ergibt. Die Berufsbezeichnis „Oberbürgermeister“ mag an sich offenkundig sein, in Verbindung mit einer Namensliste von Patienten, die sich vorübergehend in psychiatrischer Behandlung befunden haben, kann sie den beruflichen Abstieg einleiten. Eine einseitige Änderung des Verwendungszwecks bedarf einer gesonderten Legitimation durch Gesetz oder der Einwilligung des Betroffenen.

Die *Zweckbindung* ist bereits dem informationellen Selbstbestimmungsrecht inhärent, denn die Erteilung einer Einwilligung in die Verarbeitung personenbezogener Daten ist seitens des Betroffenen ohne eine Bindung an einen bestimmten Zweck (vielleicht auch Zwecke) nicht denkbar. Um Unsicherheiten sowohl für den Betroffenen als auch den Erklärungsempfänger zu vermeiden, regelt § 4 Abs. 2 BDSG, welche Informationen dem Betroffenen vor seiner Einwilligung mindestens mitzuteilen sind. Dazu gehört insbesondere der Zweck der Speicherung und einer vorgesehenen Übermittlung. Im Rechtsverkehr zwischen Privaten ergibt sich die Zweckbindung bereits aus dem konsentierten Vertragszweck. Insofern ermöglicht eine Regelung wie § 28 Abs. 1 Nr. 2 BDSG (Interessenabwägung) sogar mehr als eine bestehende Vertragsbeziehung als Zweck legitimieren könnte.

In Zusammenhang mit dem Grundsatz *bereichspezifischer Regelungen* („bestimmt und normenklar“) übt der Grundsatz der Zweckbindung einen

gewissen Präzisierungszwang auf den Gesetzgeber aus, der anwendungsbezogene Verwendungszwecke definieren muß, wenn die Mitwirkung des Betroffenen an der Verwendung seiner Daten ausgeschaltet werden soll. Das Erfordernis, den Verwendungszweck bereichspezifisch und normenklar zu regeln, ermöglicht dem Betroffenen, zumindest prinzipiell den gesetzlichen Regelungen entnehmen zu können, zu welchen Zwecken seine Daten verarbeitet und verwendet werden können, und ermöglicht einen Mindeststandard an Transparenz der Verwendung personenbezogener Daten aufgrund gesetzlicher Regelungen.

Adressat des geltenden Datenschutzrechts ist die seine Daten erhebende oder auch nur *speichernde Stelle*, vgl. § 3 Abs. 8 BDSG u. a.. Die Orientierung am Stellenbegriff lebt von der Vorstellung einer örtlich fixierten Verarbeitungsanlage, für die Verantwortlichkeiten festgelegt werden können und deren Träger „faßbar" sind. Für den Betroffenen ist die „Stelle" Anknüpfungspunkt, um die weitere Verarbeitung und Nutzung seiner Daten beispielsweise durch Wahrnehmung seines Auskunftsanspruches kontrollieren zu können.

Maßstab der Datenverarbeitung aufgrund einer gesetzlichen Regelung ist der Grundsatz der *Erforderlichkeit*, dessen tragende Bedeutung der Gesetzgeber häufig durch Übernahme in den Gesetzestext unterstreicht. In vielen Fällen wird der Grundsatz der Erforderlichkeit auch durch sogenannte *Abwägungsklauseln* ergänzt. Vorteil derartiger Regelungen ist ihre Flexibilität für eine Konkretisierung im Einzelfall. Nachteil für den Betroffenen ist die fehlende Vorhersehbarkeit, unter welchen Voraussetzungen die Erhebung und Verarbeitung seiner Daten zulässig ist.

Dürfen personenbezogene Daten aufgrund einer gesetzlichen Regelung erhoben und verarbeitet werden, so ist das informationelle Selbstbestimmungsrecht gleichwohl durch zusätzliche *verfahrensrechtliche und organisatorische Vorkehrungen* zu sichern.[5] Zu diesen zählen neben den Prinzipien der Datensicherheit (Anlage zu § 9 BDSG u. a.) insbesondere auch die Auskunftsrechte des Betroffenen, eine unabhängige Datenschutzkontrolle oder bestimmte Anonymisierungspflichten. Derartige Vorkehrungen können gegenüber bestimmten Eingriffen in das informationelle Selbstbestim-

[5] BVerfGE 65, 1, 49 ff.

mungsrecht auch eine „kompensatorische Funktion“ entfalten, wenn sie durch „Gegenrechte“ und flankierende Schutzregelungen den Eingriff für den Betroffenen noch zumutbar gestalten.[6]

Die technische Seite des Datenschutzes, die *Datensicherheit***,** ist im konventionellen Datenschutzrecht als an die datenverarbeitende Stelle gerichtetes Gebot konzipiert, bestimmte technische und organisatorische Maßnahmen zum Schutz der gespeicherten Daten zu ergreifen. Dieses Konzept der Datensicherheit zielt auf einen an technischen Anlagen orientierten Systemdatenschutz.

3. Veränderungen

Kennzeichen des geltenden datenschutzrechtlichen Regelungsinstrumentariums ist seine nur *reaktive Wirkung* auf Veränderungen der technischen Entwicklung. Zwar hat das Bundesverfassungsgericht dem informationellen Selbstbestimmungsrecht seine verfassungsrechtlichen „Weihen“ unter Hinweis auf die „modernen Bedingungen der Datenverarbeitung“ verliehen,[7] jedoch hat das geltende Datenschutzrecht mit der besonderen Dynamik der Entwicklung der Bedingungen der Datenverarbeitung nicht Schritt halten können. Merkmale dieser Entwicklung sind kurz zusammengefaßt:

Die *Dezentralisierung* der Datenverarbeitung: Die für die erste Generation der Datenschutzgesetze in den 70er Jahren geltende Analyse, die Gefahren für das Persönlichkeitsrecht gingen von zentralen Großrechnern aus, auf denen umfassende Informationen über die Bürger zusammengetragen würden, kann spätestens seit Ende der 80er Jahre keine Gültigkeit mehr beanspruchen. Zentrale Großrechner wurden zunehmend durch dezentrale PC-Lösungen ersetzt, deren Datenbestände sich faktisch einer effektiven Kontrolle entziehen.

Diese Unübersichtlichkeit der Datenverarbeitung wächst durch die sich in den 90er Jahren entwickelnde zunehmende *Vernetzung*, die nunmehr auch den Datenaustausch zwischen dezentralen Rechnern und damit eine Ver-

[6] Bizer (Fußn. 2), S. 208 ff.
[7] BVerfGE 65, 1, 43.

vielfachung dezentraler Datenbestände ermöglicht und damit eine effektive Beschränkung und Kontrolle der Datenverarbeitung erheblich erschwert.

Die exponentiell wachsenden und preiswert verfügbaren Rechnerleistungen ermöglichen die Integration von Text-, Bild- und Tonkommunikation über ein und dasselbe Medium (*Multimedia*), so daß immer mehr Informations- und Kommunikationsmöglichkeiten in einem Medium zusammengeführt werden können. Die *Digitalisierung* der Telekommunikation eröffnet schließlich die Integration von Datenverarbeitung und Kommunikation und über das Internet einen weltweiten Datenaustausch. Diese *Globalisierung* der Datenverarbeitung erschwert einerseits eine nationale Kontrolle der Datenverarbeitungsvorgänge, forciert aber auch politisch das Interesse an einer Verständigung auf weltweit akzeptierte Datenschutzregelungen.[8]

Das *Outsourcing* öffentlicher Datenverarbeitung an private Unternehmen und die *Deregulierung* der Telekommunikation haben die Datenverarbeitung nicht-öffentlicher Stellen in den Vordergrund der Diskussion geschoben. Spätestens seit der EG-Datenschutzrichtlinie sind die allgemeinen Datenschutzprinzipien des öffentlichen auch im nicht-öffentlichen Bereich anerkannt. Unter den Bedingungen moderner IuK-Techniken ist nunmehr praktisch jeder im datenschutzrechtlichen Sinne Betroffene auch ein Nutzer und möglicherweise auch ein potentieller Anbieter. Als Anbieter einer homepage sammelt er Daten über Nutzer und als Nutzer hinterläßt er persönliche Datenspuren.

Neue Gefährdungen dieser Entwicklung für das informationelle Selbstbestimmungsrecht ergeben sich aus den erweiterten technischen Möglichkeiten der Anbieter elektronischer Dienstleistungen (Telekommunikation, Teledienste, Mediendienste), personenbezogene Daten ihrer Nutzer zu erheben, zu speichern und mit anderen Nutzungsdaten aus diesen und anderen Verarbeitungszusammenhängen zu umfassenden *Kundenprofilen* zu verknüpfen und unter dem Gesichtspunkt der Optimierung der eigenen Geschäftstätigkeit auszuwerten.[9] Ansatzpunkte für derartige Auswertungen sind die Erhebung und Verarbeitung der personenbezogenen Daten, die für

[8] Siehe Art. 29er Gruppe, Übermittlung personenbezogener Daten in Drittländer, DuD 2/1998, 97 ff.

[9] Vgl. nur Berlin-Budapest Memorandum, DuD 3/1997, 154 ff.; Damker/Müller, DuD 1/1997, 24; Roßnagel/Bizer, DuD 4/1996, 209 ff.

die Nutzung und Abwicklung elektronischer Dienstleistungen einschließlich ihrer Bezahlung zum Teil auch aus unterschiedlichen Quellen erhoben werden und zur Optimierung der Geschäftstätigkeit zusammengeführt werden.[10]

Die Risiken für die informationelle Selbstbestimmung liegen in der Vielzahl von Einzelinformationen über Art, Umfang und Zeiten der Nutzung einzelner Angebote durch einen bestimmten Kunden. Von Interesse sind aber nicht nur die tatsächlich in Anspruch genommenen Leistungen, sondern auch die *Nutzungspräferenzen* des potentiellen Kunden, die sich beispielsweise aus dem „Blättern" in einem elektronischen Katalog ergeben können und als Grundlage für eine gezielte Bewerbung und Betreuung des potentiellen Kunden dienen können. „Cookies" sind das Synonym für raffinierte Techniken elektronischer Kommunikation, die sich dadurch auszeichnen, daß die Browser der „Nutzer" vom Anbieter veranlaßt ihr eigenes „Kundenprofil" Anbietern unbemerkt übermittelt.

4. Neues Datenschutzrecht

Die geschilderten Veränderungen erfordern eine *Revision und Ergänzung* des bisherigen Datenschutzrechts. Neben dem bislang an dem Schutz vor Risiken, die von technischen IuK-Systemen für das informationelle Selbstbestimmungsrecht ausgehen, orientierten rechtlichen Schutzkonzepten, ist eine rechtliche Motivierung und Flankierung von Selbstschutzkonzepten erforderlich, die um Elemente eines *Technikgestaltungsrechts* zu ergänzen sind. Der Datenschutz ist nicht mehr nur auf einen Systemdatenschutz zu beschränken, sondern um Elemente des *Selbstdatenschutzes* zu ergänzen.[11] Schon der „Rat für Forschung, Technologie und Innovation" hatte in seinen Empfehlungen zur „Informationsgesellschaft" aus dem Dezember 1995 formuliert:

> *„E 22: Eine Novellierung des Bundesdatenschutzgesetzes sollte aufgrund der technischen Veränderungen, die geprägt sind von Vernetzung und Dezentralisierung, möglichst bald erfolgen (...). Dabei sollten die bisherigen Vorschriften zur*

[10] Bizer in: Muksch / Behme, S. 95 ff.
[11] Roßnagel, Festschrift Podlech, S. 227 ff.

Datensicherheit, insbesondere § 9 und die Anlagen des Bundesdatenschutzgesetzes, den Anforderungen der modernen Informations- und Kommunikationstechnik angepaßt werden“.

Im weiteren Text schlägt der Forschungsrat schließlich vor, das *Gebot der Datenminimierung* zu verwirklichen und ein Höchstmaß an Anonymität gegenüber Netzbetreibern und Dienstleistungsanbietern zu gewährleisten.

Grundgedanke einer derartigen Revision und Ergänzung ist die Stärkung der individuellen Autonomie des Nutzers durch technische und organisatorische Maßnahmen gegenüber den veränderten Bedingungen einer dezentralen und vernetzten Verarbeitung personenbezogener Daten. Ein derartiges Konzept setzt einerseits an technischen Voraussetzungen an, versucht aber andererseits auch die Entwicklung und Anwendung datenschutzfreundlicher Technologien anzuregen. Im Ergebnis muß das Datenschutzrecht auch als ein die IuK-Technik gestaltendes Recht begriffen werden.

4.1 Verschlüsselung

Das erste Beispiel eines derartigen Konzeptes ist die Förderung der *teilnehmerautonomen Verschlüsselung*, mit der die Kommunikationspartner die Vertraulichkeit ihrer elektronischen Nachrichten selbst und unabhängig von dem Angebot der Netz- und Dienstbetreiber verschlüsseln können.[12] Mit Hilfe von derartigen Methoden der Verschlüsselung können mit technischen Mitteln rechtlich geschützte Geheimnisse wie die ärztliche Schweigepflicht oder Betriebs- und Geschäftsgeheimnisse wirksam vor dem unberechtigten Zugriff geschützt werden. Teilnehmerautonome Verschlüsselung bewirkt aber auch einen effektiven Schutz des Fernmeldegeheimnisses. Darüber hinaus gewährleistet sie auch die Erfüllung der Anforderungen der Maßnahmen nach der Anlage zu § 9 BDSG. Teilnehmerautonome Verschlüsselung ersetzt jedoch nicht die Verpflichtungen zur Gewährleistung einer Systemsicherheit durch die speichernde Stelle, den Dienstanbieter oder den Netzbetreiber, sondern steht zu ihr in einem *Ergänzungsverhältnis*.

[12] Bizer, in Hammer 1995, S. 184 ff.; Bizer, DuD 1/1996, 5 ff.

Mittlerweile stehen den Nutzern ausreichend leistungsfähige Verfahren zur Verfügung, die mit Standardrechnern ohne größere Schwierigkeiten zu bewältigen sind.[13] Der Einsatz kryptographischer Verfahren zu Zwecken der Verschlüsselung ist mittlerweile Stand der Technik in der Datensicherheit und im Datenschutz.[14] Nach deutschem Recht unterliegt die Verwendung kryptographischer Verfahren im Inland keinen Beschränkungen.[15]

4.2 Anonymes und pseudonymes Handeln

Das Risiko personenbezogener Datenspuren in den offenen Netzen der Telekommunikation läßt sich ebenfalls durch Maßnahmen der Teilnehmer und Nutzer selbst minimieren. So können Dienstleistungen eines Dritten in Anspruch genommen werden, der die Zuordnung der elektronischen Kommunikationsadresse gegenüber Dritten durch die Vergabe eines Pseudonyms verschleiert (*Identiy Protector*).[16] Häufig scheitert in Anwendungsbereichen des Electronic Commerce eine derartige Kommunikation jedoch an dem legitimen Interesse des Partners, die vom Absender beanspruchte Leistung auch bezahlt zu bekommen. Die konventionellen Zahlungsmöglichkeiten wie beispielsweise die Kreditkarte sind jedoch personenbezogene Zahlungsmittel. Auch hier bestehen allerdings prinzipiell Lösungsmöglichkeiten, beispielsweise durch den Einsatz vorbezahlter Wertkarten, mit deren Hilfe Leistungen unmittelbar online bezahlt werden, so daß auf diese Weise eine anonyme Kommunikation möglich ist.[17] Auch ist es nicht erforderlich, daß der Anbieter eines Web-Servers die einzelnen Nutzer seiner Inhalte personenbezogen bestimmen kann.

Pseudonymes Handeln ist möglich, wenn der Nutzer gegenüber dem Anbieter unter einem fremden Namen auftritt.[18] Der Anbieter kann zwar bestimmte Handlungen einer einzelnen Person als Träger des Pseudonyms zurechnen. Solange der Anbieter das Pseudonym aber nicht aufdecken

[13] Siehe Gerling DuD 4, 1997, 197 ff.
[14] Bizer, in: Büllesbach, S. 251 m.w.N.
[15] Bizer, in Hammer 1995, S. 184 ff.; Ausnahme sind Exportbeschränkungen, dazu Roth, DuD 1 und 2/1998.
[16] AK Technik, DuD 12/1997, 713 f.; Borking, DuD 11/1996, 654 ff.
[17] Siehe Knorr/Schläger, 7/1998, 396 ff.; Zur GeldKarte s. u. zu Fußn. 24.
[18] Siehe Bizer/Bleumer, DuD 1/1997, 46. AK Technik, DuD 12/1997, 711 f.

kann, ist eine Zurechnung dieser Handlungen zu einer bestimmten Person nicht möglich.

Pseudonymitätskonzepte können beispielsweise mit Hilfe digitaler Signaturen verwirklicht werden, deren rechtliche Rahmenbedingungen durch das Digitale Signaturgesetz (SigG) in Art. 3 des IuKDG, geregelt wird. Ausdrücklich läßt § 7 Abs. 1 Nr. 1 SigG zu, daß ein *Signaturschlüssel-Zertifikat* auch ein seinem Inhaber „zugeordnetes unverwechselbares Pseudonym, das als solches kenntlich sein muß“ enthalten kann. Die legitimen Interessen des Anbieters sind gewahrt, wenn im Streitfall die Zertifizierungsstelle die Identität des Kunden gegenüber dem Gläubiger aufheben muß. Aufgrund der Kennzeichnungspflicht des Pseudonyms kann der Anbieter im übrigen erkennen, daß sein Kunde unter Pseudonym handelt. Die Verwendung von Pseudonymen wird im neuen Teledienst- und Mediendienstrecht durch die Rechtsregel unterstützt, wonach Anbieter keine personenbezogene Nutzungsprofile erstellen dürfen. Eine Ausnahme gilt für Pseudonyme, jedoch dürfen die unter Pseudonym erfaßten Profile nicht bestimmten Nutzern zugeordnet werden, § 4 Abs. 4 TDDG, § 13 Abs. 4 MD-StV.

Außerdem schreibt das neue Datenschutzrecht den Anbietern von Tele- und Mediendiensten vor, die Inanspruchnahme von Telediensten bzw. Mediendiensten und ihre Bezahlung „anonym oder unter Pseudonym zu ermöglichen“, § 4 Abs. 1 TDDSG, § 13 Abs. 1 MD-StV. Diese Vorgabe steht zwar unter dem Vorbehalt des technisch Möglichen und Zumutbaren, sie bietet aber erstmals eine normative Basis für mehr als nur einen „sanften“ Druck, entsprechende Angebote unter *Einsatz datenschutzfreundlicher Technologien* auch zur Verfügung zu stellen.

4.3 Datenminimierende Systemgestaltung

Ein neues Datenschutzrecht muß aber auch technische Gestaltungsvorgaben für die Entwicklung und den Einsatz technischer Systeme formulieren. Die *Ungleichzeitigkeit* von technischer Entwicklung einerseits und der Fortschreibung des geltenden Datenschutzrechts andererseits hat keine besonderen, strukturell dem Recht inhärenten Gründe. Zwar lassen sich Leistungsschwächen einzelner Rechtsinstrumente in bestimmten Anwendungszusammenhängen diagnostizieren, diese rechtfertigen jedoch nicht den Schluß, das Recht sei als Steuerungsinstrument untauglich, bestimmte tech-

nische Gestaltungshorizonte zu befördern. Die Ungleichzeitigkeit von Recht und Technik im Datenschutzrecht hat andere Ursachen: Sie liegen in dem rechtspolitisch und psychologisch zu erklärenden Defizit, das Datenschutzrecht *auch* als ein technikgestaltendes Recht zu begreifen. Unter Fachleuten der Materie ist unbestritten, daß schon die letzte Novelle des BDSG 1990 von einer bereits zum damaligen Zeitpunkt überholten technischen Wirklichkeit ausging.[19] Der gegenwärtige Referentenentwurf des BDSG vom 08.12.1997[20], mit dem die EG-Datenschutzrichtlinie umgesetzt werden soll, bietet zum gegenwärtigen Zeitpunkt keinen Anlaß, diese Bewertung auch für die kommende Novelle zu revidieren.[21]

Paradigmatisch ist auch hier das neue Teledienst- und Mediendienstrecht, dessen Datenschutzbestimmungen qualitative Zielvorgaben für die „Gestaltung und Auswahl technischer Einrichtungen“ für Teledienste bzw. Mediendienste formulieren. Danach haben sich die Anbieter an dem Ziel auszurichten, „keine oder so wenige personenbezogene Daten wie möglich zu erheben, zu verarbeiten und zu nutzen“, § 3 Abs. 4 TDDG bzw. § 12 Abs. 5 MD-StV. Diese Regelung wird ergänzt durch die oben zitierte Anforderung an die Anbieter, Teledienste oder Mediendienste „anonym oder unter Pseudonym“ zu ermöglichen, § 4 Abs. 1 TDDSG, § 13 Abs. 1 MD-StV.

Als *Zielvorgabe* formuliert überläßt es der Gesetzentwurf dem Anbieter, mit welchen Techniken er das Ziel der Datenminimierung im einzelnen erreichen will. Das staatliche Rahmenrecht gibt lediglich das Gestaltungsziel vor und überläßt seine Umsetzung im einzelnen Herstellern und Anbietern.[22] Die Zielvorgabe kann insbesondere durch das Angebot, anonymer oder pseudonymer Dienstleistungen erfüllt werden. Der Einsatz vorbezahlter Wertkarten ist hierfür ebenso ein Beispiel wie die Abrechnung über Pauschaltarife (Monatsabonnement), die eine leistungsbezogene Erfassung je Nutzer nicht erforderlich machen. Weitere Anreize, derartige Zielvorgaben zu erfüllen, können über anerkannte Prüfzertifikate erreicht werden, die wiederum einer öffentlichen Evaluation unterliegen sollten (s. u. 4.4).

[19] Lutterbeck, DuD 3/1998.
[20] http://www.dud.de.
[21] Weichert, DuD 12/1997, 718.
[22] Bizer, Jahrb. Telekommunikation und Gesellschaft 1997, 147 f.

Die Bedeutung einer frühzeitig an Datenschutzzielen orientieren Technikgestaltung und Bewertung, läßt sich am Beispiel der *GeldKarte* anschaulich verdeutlichen. Nach außen hin erscheint sie als vorbezahlte Wertkarte. Tatsächlich läßt sich aber der Vereinbarung der Banken und Sparkassen von 1996 über die GeldKarte entnehmen, daß „das GeldKarten-emittierende Institut über (jeden) Aufladevorgang zu unterrichten" ist. Auch erfolgt der „Einzug von GeldKarten-Umsätzen (...) ausschließlich über die jeweils zuständigen Verrechnungsbanken".[23] Derartig geführte „Schattenkonten" erlauben eine Rekonstruktion aller über die Karte abgewickelten Bezahlvorgänge und damit zumindest teilweise die Erstellung von Bewegungs- und Konsumprofilen. Bemerkenswert ist, daß die Kunden und Nutzer in den zugehörigen AGB auf diesen Umstand *nicht* hingewiesen werden.[24]

Bei der Vorgabe datenminimierender Systemgestaltung handelt es sich um einen „Prototypen *innovativen Rechts*", da mit einer rechtlichen Verpflichtung die Entwicklung datenschutzgerechter Technologien angeregt und die Voraussetzungen für eine ausreichende Nutzerakzeptanz gegenüber einer Anwendung neuer Medien gewährleistet werden soll.

4.4 Datenschutz-Audit

Einer kritischen Überprüfung bedarf auch die Fixierung des geltenden Datenschutzrechts auf die Mittel des klassischen Ordnungsrechts wie beispielsweise das geltende Verbot mit Erlaubnisvorbehalt, § 4 Abs. 1 BDSG. Die Bedeutung dieses klassischen Steuerungsinstruments liegt in dem Legitimationszwang, den es bei den datenverarbeitenden Stellen auszuüben in der Lage ist. Es stärkt nach außen den Begründungszwang gegenüber dem Betroffenen sowie den datenschutzrechtlichen Kontrollinstanzen, den Datenschutzbeauftragten oder Aufsichtsbehörden. Nach innen vermag das grundsätzliche Verbot, den Warnungen und Empfehlungen des behördlichen oder betrieblichen Datenschutzbeauftragten mit dem Hinweis auf einen Rechtsverstoß Nachdruck zu verschaffen. Jedoch ist das Verbot mit Erlaubnisvorbehalt nicht geeignet, technische Innovation für den Einsatz

[23] Abgedruckt in WM 1996, 2354 ff. Siehe auch Bbg. DSB, 4.TB 1996, S. 21 f., s. a. Knorr/ Schläger, DuD 7/1997, 401.
[24] Fox/Bizer, DuD 7/1997, 378, s. a. Entschließung der 50. Konferenz der DSB, 13.10.1995 zum „Datenschutz bei elektronischen Geldbörsen", 16. TB des BfD, Anl. 11, S. 456.

datenvermeidender Technologien anzuregen und auszulösen. Ansatzpunkt des Verbots mit Erlaubnisverbot ist die Regulierung der Datenströme und Verwendungszwecke, sein Ziel ist aber nicht, eine ***„vorlaufende" und damit präventiv wirkende Technikgestaltung*** zu initiieren.

Einen solchen Effekt könnte aber das in § 17 MD-StV vorgesehende *Datenschutz-Audit* haben.[25] Sein Ziel ist es, zwischen konkurrierenden Anbietern einen Wettbewerb um die Entwicklung und den Einsatz datenvermeidender Technologien auszulösen. Mit diesem Instrument könnte es möglicherweise gelingen, das angebotene Datenschutzniveau zu einem Wettbewerbsargument umzumünzen. Unter dieser Voraussetzung könnte das rechtliche Gebot, die Inanspruchnahme von Telediensten bzw. Mediendiensten und ihre Bezahlung „anonym oder unter Pseudonym zu ermöglichen", § 4 Abs. 1 TDDSG, § 13 Abs. 1 MD-StV, zu einem effektiven Instrument werden, ohne das staatliches Recht Sanktionen aussprechen muß.

Wettbewerb bedarf jedoch der *Transparenz*, die durch in einem Ausführungsgesetz noch zu formulierende Regelungen herzustellen ist. In einem solchen Ausführungsgesetz müßten beispielsweise Kriterien und Verfahren für die Ausstellung eines Prüfsiegels für datenvermeidende Techniken formuliert werden. Andererseits bedarf das Datenschutz-Audit der *Stützung und Absicherung* durch ein flankierendes staatliches Rahmenrecht. Das Datenschutz-Audit zielt als „weiches" Steuerungsinstrument nicht auf ein „Datenschutz-Dumping", sondern soll eine die Marktmechanismen berücksichtigende Effektivitätssteigerung der Steuerungsleistung datenschutzrechtlicher Regelungen bewirken. Das Verhältnis von staatlichem Recht und selbsregulativen Elementen ist jedoch als ein iterativer Prozeß zu verstehen, der auf das Generieren von Erfahrungswissen ausgerichtet ist, um das jeweils erforderliche Verhältnis von Rahmenrecht und Selbstregulierung auszutarieren.

Nicht ausgeschlossen ist, daß die Ausübung der staatlichen Kontrollen in bestimmten Anwendungsbereichen auf Zeit zurückgenommen werden kann, wenn das Datenschutz-Audit ein hohes Datenschutzniveau bewirkt. Eine Beschränkung staatlicher Kontrollbefugnisse ist damit jedoch nicht intendiert. Weil der Erfolg des Audits bei fortschreitender Technik immer nur

[25] Roßnagel, DuD 9/1997, 505 ff.

zeitlich beschränkt sein kann, bedarf es wirksamer „Reservebefugnisse“, auf die im Fall eines Steuerungsversagens zurückgegriffen werden kann. Soll demnach das Datenschutz-Audit eine Stärkung datenschutzfreundlicher Technologien in bestimmten Anwendungsfeldern bewirken, so wird damit gleichzeitig auch eine Stärkung der *Rolle der Datenschutzbeauftragten* als kundenorientierter Technik-Berater eingeleitet werden.[26]

5. Fazit

Das Datenschutzrecht für Tele- und Mediendienste ist Vorreiter für ein neues Datenschutzrecht, in dem die bisherigen Elemente des Systemdatenschutzes durch Elemente des Selbstdatenschutzes und der Technikgestaltung ergänzt werden. Die in diesem Recht enthaltenen Regelungselemente sind adäquate Reaktionen auf die Veränderung der Datenverarbeitung.

6. Literaturhinweise:

52. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 22./23. Oktober 1996, DuD 12/1996, 756 ff.
AK Technik der Datenschutzbeauftragten, Datenvermeidende Technologien, DuD 12/1997, 709 ff.
Art. 29er Gruppe, Übermittlung personenbezogener Daten in Drittländer, DuD 2/1998, 97 ff.
Bachmeier, R.: Vorgaben für datenschutzgerechte Technik, DuD 11/1996, 672.
Bäumler, H.: Wie geht es weiter mit dem Datenschutz?, DuD 8/1997, 450 f.
Bizer, J.: Forschungsfreiheit und informationelle Selbstbestimmung, Baden-Baden 1992.
Bizer, J.: Die Kryptokontroverse. Innere Sicherheit und Sicherungsinfrastrukturen, in: V. Hammer, (Hrsg.), Sicherungsinfrastrukturen - Gestaltungsvorschläge für Technik, Organisation und Recht, Berlin, 1995, S. 179-215.
Bizer, J./ Bleumer, G.: Gateway: Pseudonym, DuD 1/1997, 46.

[26] Bäumler, DuD 8/1997, 450 f.

Bizer, J.: Datenschutz in Neuen Medien, in: Jahrbuch Telekommunikation und Gesellschaft, 1997, 146 ff.
Bizer, J.: Verschlüsselung und staatlicher Datenzugriff. Die deutsche Debatte, in: Alfred Büllesbach (Hrsg.), Datenschutz im Telekommunikationsrecht, Köln 1997, S. 245-270.
Bizer, J.: Datenschutz im Datawarehouse, in: H. Muksch / W. Behme (Hrsg.), Das Datawarehouse-Konzept, 2. Aufl. 1997, Wiesbaden 1997, S. 95 ff.
Borking, J.: Der Identity Protector, DuD 11/1996, 654 ff.
Budapest-Berlin Memorandum: Datenschutz und Privatsphäre im Internet, DuD 3/1997, 154 ff.
Damker, H. / Müller, G.: Verbraucherschutz im Internet, DuD 1/1997, 24 ff.
Engel-Flechsig, S.: Teledienstdatenschutz, DuD 1/1997, 5 ff.
Forschungsrat 1995: Informationsgesellschaft. Chancen, Innovationen und Herausforderungen, 1995.
Fox, D. /Bizer, J.: Wohin mit dem Geld?, DuD 7/1997, 378.
Gerling, R.W.: Verschlüsselungsverfahren, Eine Kurzübersicht, DuD 4/1997, 197 ff.
Knorr, M. / Schläger, U.: Datenschutz bei elektronischem Geld, DuD 7/1998, 396 ff.
Lutterbeck, B.: 20 Jahre Dauerkonflikt: Die Novellierung des Bundesdatenschutzgesetzes, Beitrag in diesem Tagungsband, S. 7.
Roßnagel, A. / Bizer, J.: Multimediadienste und Datenschutz, DuD 4/1996, 209 ff.
Roßnagel, A.: Freiheit durch Systemgestaltung, in FS Podlech, Baden-Baden, 1994, S. 227 ff.
Roßnagel, A.: Datenschutz-Audit, DuD 9/1997, 505 ff.
Schrader, H.-H.: Selbstdatenschutz mit Wahlmöglichkeiten, DuD 3/1998, 128.
Weichert, T.: Anforderungen an das Datenschutzrecht für das Jahr 2000, DuD 12/1997, 718.

Warum brauchen wir Technik? - Zum Verhältnis von Technik und Recht

Andreas Pfitzmann

Wir brauchen Technik, weil wir Datenmißbrauch verhindern oder zumindest erkennen wollen. Dem kann entgegengehalten werden: „Das ist ein Allgemeinplatz, das gilt im Recht immer." Die Datenverarbeitung ist jedoch durch ein Spezifikum gekennzeichnet. Das Spezifikum ist, daß Datendiebstahl keine natürlichen Spuren hinterlassen muß. Denn wenn Daten gestohlen werden sollen, werden sie normalerweise auch dort zurückgelassen, wo sie sich befinden. Es wird einfach eine Kopie gemacht. Wenn wir nicht sehr auf der Hut sind, werden wir Mißbrauch in dem Bereich also nicht einmal erkennen, geschweige denn verhindern können, und zwar mit allen Problemen, die daraus resultieren. Ein Vergleichsbeispiel zur Verdeutlichung: Unabhängig davon, ob Personen tatsächlich beobachtet werden, reagieren sie mißtrauisch, wenn sie sich beobachtet fühlen oder befürchten, beobachtet zu werden. Schon die Befürchtung, beobachtet zu werden, weckt Mißtrauen und wirkt verhaltensändernd, nicht erst die tatsächliche Beobachtung.

Stellen wir uns vor, es wären Daten kopiert worden und wir würden das *erkennen*. Nun wäre die Frage, ob wir dies rückgängig machen können? Einen Gegenstand können Sie, wenn Sie ihn wiederfinden, nachdem er entwendet wurde, sicherstellen und dem Eigentümer zurückgeben. Versuchen Sie das mal mit Daten! Denn selbst wenn Sie jetzt *eine* Kopie der Daten fänden, könnten Sie nie sicher sein, daß es nicht noch weitere Kopien gibt. Um es sehr deutlich zu sagen: Man kann im Internet eine ganze Menge von Dingen, aber was Sie im Internet definitiv nicht können, ist ein Datum, das einmal im Internet war, löschen. Sie können immer ein Einzelexemplar, eine einzelne Kopie löschen, das sei Ihnen unbenommen. Aber eine

Information, die einmal im Internet zugänglich war, in überprüfbarer Weise aus der Welt schaffen, das können Sie nicht. Das heißt also, wenn es uns nicht gelingt, manche Dinge vorbeugend zu verhindern, dann werden wir bei der Schadensbegrenzung oder der Schadensbehebung prinzipielle Probleme haben, die sich von denen unterscheiden, die wir aus der materiellen Welt kennen. Das ist spezifisch für die Informationstechnik: Man muß einen besonderen Aufwand treiben, um bestimmte Dinge zu erkennen. Im Grunde ist Mißbrauch - was Vertraulichkeit angeht - auch nur vorbeugend zu verhindern. In dieser Situation reichen Gesetze alleine nicht aus, weil sie gar nicht richtig vollzogen werden können. Es bedarf einer technischen Basis, die die Durchführung und die Überprüfung des Vollzugs ermöglicht.

In Zukunft wird es nötig sein, die Technik*gestaltung* durch Recht zu beeinflussen und nicht nur den Umgang mit Technik. Zum Beispiel Kryptographie: Etwa um die Zeit 1982/1983 habe ich in einem der Tätigkeitsberichte der Datenschutzbeauftragten noch gelesen, daß die Datenschutzbeauftragten *gegen* Kryptographie seien, denn damit könne man ja auch personenbezogene Daten verschlüsselt über die Netze schicken. Die Datenschutzbeauftragten könnten dann nicht kontrollieren, was mit den personenbezogenen Daten passiert. Inzwischen plädieren etliche Datenschutzbeauftragte für die Kryptographie und es sind eher gewisse andere Instanzen des Staates gegen die Verschlüsselung.

Ein anderes Beispiel betrifft die Kommunikationsumstände: Vor zehn Jahren gab es eine Diskussion darüber, wie lange die Telekom Verbindungsdatensätze speichern dürfe. Herausgekommen ist dabei, daß bestimmte Daten für eine bestimmte Dauer zwar gespeichert werden dürfen, dann jedoch definitiv gelöscht werden müssen. Es mag sein, daß wir mit der Technologie von vor zehn Jahren noch halbwegs sicher die Löschung nachvollziehen konnten. Aber so, wie zumindest heute die Netze sind, habe ich Zweifel, ob die Telekom nachweisen kann, daß sie die Daten *wirklich* löscht, nämlich *alle* Exemplare löscht. Sicher können wir uns dessen jedenfalls nicht sein. Die Konsequenz daraus kann nur sein, daß wir *unbeobachtete* Kommunikation gewährleisten, also nicht nur Kommunikation, die beobachtet und nach einer gewissen Zeit vergessen wird, sondern eine von Anfang an unbeobachtete Kommunikation.

Die einzige Methode, mit der das wirklich sichergestellt werden kann, ist, daß die Kommunikation *unbeobachtbar* gemacht wird. Denn, wenn die Daten erfaßbar sind, z. B. personenbezogene Daten, dann wissen Sie nicht, ob sie jemand erfaßt und was er letztlich damit tut. Das hat Johann Bizer vorhin Datensparsamkeit genannt: Überflüssige Daten dürfen nicht entstehen, dürfen nicht erfaßbar sein. Dabei will man allerdings eigentlich keine Daten sparen - oftmals sind die Techniken, die man dafür braucht, sogar sehr datenintensiv. Was tatsächlich gespart werden soll, ist der Bezug zwischen den natürlichen Personen und ihren Daten.

Mein nächster Punkt ist, daß wir Technik brauchen, um Pseudokonflikte zu vermeiden. Die Welt ist voll von echten Konflikten. Natürlich habe ich nun als Techniker keine guten Vorschläge dafür, wie Sie jetzt den Weltfrieden erreichen oder wie sämtliche Konflikte in der Gesellschaft gelöst werden können. Was wir jedoch vermeiden können, ist, daß wir durch die Technikgestaltung noch zusätzliche Konflikte entstehen lassen. Könnten wir beispielsweise nur noch mit Kreditkarten, also mit unseren „guten Namen“ bezahlen, hätten wir einen Pseudokonflikt geschaffen. Daß jemand nämlich nicht überall namentlich bekannt sein will, wenn er hier und dort etwas bezahlen muß, aber "mit dem guten Namen bezahlen" die einzige vorhandene Technik dafür ist, dann haben wir einen Pseudokonflikt. Denn derjenige, der etwas bezahlen muß, möchte dies anonym tun, kann aber nicht anonym bleiben und derjenige, der das Geld bekommen möchte, erhält zwangsläufig die Information, von wem er das Geld bekommt, ohne daß ihn das möglicherweise wirklich interessiert. Zu allen üblichen, in der Welt zwischen Personen vorhandenen Konflikten käme somit noch ein weiterer Konflikt hinzu. Dies ist überflüssig und kann, ja muß sogar vermieden werden. Also brauchen wir Technik, gutgemachte Technik, datenschutzfreundliche Technik, um keine Pseudokonflikte zu bekommen.

Mein dritter Punkt bezieht sich auf die Gestaltbarkeit von Technik: Wir brauchen Technik, gut gestaltbare Technik, weil die Lebenszeit der Technik außerordentlich lang ist. Das trifft vielleicht nicht auf die Lebenszeit von Ihrem privaten PC zu, den Sie nach zwei Jahren austauschen können, wenn er Ihnen nicht mehr gefällt oder herunterfällt und kaputt geht. Darüber rede ich jetzt nicht, sondern über Infrastruktur. Infrastruktur hat normalerweise eine Planungs- und Vorlaufzeit von etwa zehn Jahren. Dann dauert es in aller Regel zwanzig Jahre, sie wirklich aufzubauen und sie wird in aller Regel vierzig, teilweise mehr Jahre genutzt. Das heißt also, daß Infrastruktur

sehr stabil ist: Das, was wir heute aufbauen, wird die nächste Generation noch benutzen müssen. Sie wird keine Wahl haben. Verglichen damit scheint mir nun das, was ich als Schutzziele - auch als Datenschutzziele - bezeichnen will, eher flexibel und kurzfristig. Im Datenschutz kann man durchaus innerhalb von fünf oder auch zehn Jahren einen Paradigmenwechsel erleben. Nachdem die Datenschützer früher vor allen Dingen nach Rechtsinstrumenten gesucht haben, tut heute datenschutzfreundliche Technik das, was sie wollen.

Wir können nicht davon ausgehen, daß die momentanen Bedürfnisse langfristig über zwanzig, dreißig, vierzig Jahre stabil sind. Daher brauchen wir zumindest in den Infrastrukturen eine Technik, die so gestaltbar ist, daß *jede* Strategie, die in den nächsten vierzig, fünfzig Jahren in der Demokratie miteinander darüber verabredet wird, wie wir diese Technik betreiben wollen, damit machbar ist. Auf jedes System, das Ihnen Anonymität garantiert, kann zudem relativ leicht Identifikation „draufgesattelt“ werden. Aber der umgekehrte Weg, nämlich auf ein System, das primär erst mal alle Daten ansieht und alle Personen identifiziert, Anonymität aufzusetzen, das kostet enorm viele Größenordnungen an Leistung. Datensparsame Techniken im Sinne des geringsten Personenbezuges sind die Basis, auf der alles aufgebaut werden kann. Der umgekehrte Weg läßt sich dagegen nicht einschlagen.

Meine letzte Bemerkung möchte ich zur *mehrseitigen Sicherheit* machen. Wir leben in einer Gesellschaft, in der es einzelne Menschen oder Organisationen gibt, die agieren und legitimerweise ihre Interessen vertreten - ihre Sicherheitsinteressen und ihre Schutzinteressen. Dies muß durch die Systemgestaltung auch in den IT-Systemen möglich sein. Denn wenn Wissen immer stärker auch Macht bedeutet, weil die Bedeutung der Information wächst, dann muß auch hier dezentralisiert werden. Es muß auch in diesem Bereich so etwas wie gegenseitige Kontrolle stattfinden.

Also brauchen wir auch im Datenschutz mehrseitige Sicherheit. Wir alle wollen nicht, daß manche Dinge von uns manchen Leuten bekannt werden. Davor wollen wir sicher sein, so daß das Ziel der technischen Entwicklung feststeht und rechtlich eingefordert werden kann. Umgekehrt kann natürlich auch die beste Technik juristische Vorschriften *nicht* überflüssig machen. Weil Technik Geld kostet, sind mit ihr starke ökonomische Interessen verbunden. Technikentwicklung und -einsatz können nicht allein dem Markt

überlassen werden, sondern brauchen einen rechtlichen Rahmen. Außerdem hat auch die Technik ihre Grenzen. Informationen erreichen - unabhängig von ihrem Weg - immer das Gehirn eines anderen Menschen. Technische Sicherheitsmaßnahmen greifen hier nicht. Ob der andere Mensch die Informationen, die ihn erreicht haben, weitererzählt oder auf welche sonstige Weise er damit umgeht, ist *technisch* nicht zu bewältigen. Spätestens hier sind wir in dem Bereich, in dem rechtliche Regelungen, Etikette und Gepflogenheiten unverzichtbar sind.

Schlußwort

Thilo Weichert

Als die Landesbeauftragte für den Datenschutz von Nordrhein-Westfalen, Professor Hoeren und Professor Holznagel und die Deutsche Vereinigung für den Datenschutz im letzten Frühjahr die heutige Tagung planten, gingen wir davon aus, daß uns ein abgestimmter Entwurf der Bundesregierung zum Bundesdatenschutzgesetz, zum BDSG vorliegen würde. Eine Zielsetzung der Tagung sollte es sein, die Fachdiskussion über ein zeitgemäßes Datenschutzgesetz und damit auch die Gesetzgebung selbst ein Stück voranzubringen. Nach dem ersten Arbeitsentwurf vom Januar 1997 sind zwar weitere, leicht überarbeitete Entwürfe des Bundesinnenministeriums bekannt geworden. Einen diskussionsfähigen Entwurf der Bundesregierung gibt es aber bis heute leider nicht. Doch auch die Arbeitsentwürfe des BMI zeichnen sich durch eine überkommene unzeitgemäße Terminologie aus. Die bisherige komplizierte Struktur des Gesetzes wird durch das Draufsatteln europäischer Regelungsansätze noch komplizierter. Selbst den inhaltlichen Anforderungen der europäischen Datenschutzrichtlinie wird man nicht gerecht. Und den darüber hinausgehenden technischen und praktischen Anforderungen wird erst recht nicht entsprochen. Bestehende Vollzugsprobleme und insbesondere Fortschritte bei der Informations- und Kommunikationstechnologie machen eine Weiterentwicklung des Regelungsansatzes des aktuellen BDSG erforderlich. Diesen Anforderungen versucht ein BDSG-Entwurf der Bundestagsfraktion von Bündnis 90/Die Grünen zu genügen. Die heutige Diskussion hat gezeigt, daß auch dieser Entwurf einer detaillierten Überprüfung und Kritik unterzogen werden muß. Bei ihm handelt es sich aber um eine Diskussionsgrundlage, aus der ein zeitgemäßes Datenschutzrecht erarbeitet werden kann.

Für die Überlegungen, wie ein zeitgemäßer Datenschutz aussehen kann, haben wir heute eine große Zahl von Anregungen erhalten. Es bestand weitgehend Konsens darüber, daß immer speziellere bereichspezifische Regelungen nicht die Antwort sein können auf das Zusammenwachsen der informationstechnischen Anwendungen durch Internet, Telekommunikationsnetze und Multimedia. Unterhalb der Gesetzesebene angesiedelte Regelungskonzepte sind ebenso gefragt wie technische Lösungen zur Sicherung des Datenschutzes. Hilfen zum Selbstschutz der Betroffenen sind ebenso erforderlich wie eine Erhöhung der Kontrolldichte, vor allem im privaten Bereich. Datenschutzverwaltung darf nicht zum Bürokratismus verkommen, sondern muß seine Chance als moderner Dienstleistungsservice für Betroffene, für Verwaltung und für die Wirtschaft wahrnehmen. Die heutige Tagung hat gezeigt, daß die Fachleute bereit sind, ihren Beitrag zur Modernisierung des Datenschutzes zu leisten.

Den Referenten dieser Tagung ein herzliches Dankeschön. Ich denke, im Namen aller Anwesenden zu sprechen, wenn ich feststelle, daß Ihre Anregungen neuen frischen Schwung in die sich manchmal um sich selbst drehende Datenschutzdiskussion gebracht haben. Ich bin mir sicher, daß dies nur ein Anfang war. Weitere Diskussionen sind dringend notwendig, so daß wir in dieser oder in einer ähnlichen Zusammensetzung sicherlich noch öfter zusammenkommen werden. Abschließend noch ein Dankeschön an die Mitarbeiterinnen und Mitarbeiter der Landesbeauftragten für den Datenschutz und des Instituts für Informations-, Telekommunikations- und Medienrecht hier an der Uni, die durch eine perfekte Organisation den Rahmen dafür geschaffen haben, daß wir heute derart angeregt und zugleich entspannt, konstruktiv und zugleich kontrovers diskutieren konnten.