Thomas Vesting

Das Internet und die Notwendigkeit der Transformation des Datenschutzes

A. Leitbilder und Ordnungsmodelle

Vom Datenschutz lässt sich in rechtlicher Perspektive nicht nur mit Blick auf die geltenden nationalen und europäischen Gesetze und Vorschriften sprechen[1], sondern auch im Hinblick auf das hinter dem Datenschutzrecht stehende „Leitbild".[2] Während die Leitbilder, auf die Gesetzgebung und Rechtsprechung referieren, oft implizit bleiben und selten detaillierter ausgearbeitet sind, soll hier mit dem Begriff des Ordnungsmodells ein möglichst widerspruchsfreies System von Regeln bezeichnet werden, eine „Ordnungsidee"[3], die den Reichtum und die Fluidität der empirischen Wirklichkeit bewusst übergeht und deren Komplexität sachlich und zeitlich zusammenfasst. Ordnungsmodelle sind in einem rechtswissenschaftlichen Kontext unverzichtbar.

1 Zum Datenschutz im Internet vgl. nur *V. Boehme-Neßler*, Cyberlaw, München 2001, S. 283 ff.; *T. Hoeren*, Grundzüge des Internetrechts, München 2002, S. 233 ff. Einen Überblick über die wichtigsten internetbezogenen Datenschutzregelungen in Deutschland und anderen europäischen Mitgliedstaaten geben *J. R. Reidenberg/P. M. Schwarz*, Data Protection Law and On-Line Services, Regulatory Responses, Brüssel 1998; eine kritische Bestandsaufnahme zum geltenden deutschen Datenschutzrechts findet sich u. a. bei *A. Roßnagel/A. Pfitzmann/ H. Garstka*, Modernisierung des Datenschutzrechts, 2001, S. 29 ff.; zur US-amerikanischen Diskussion vgl. *J. R. Reidenberg*, Lex Informatica: The Formulation of Information Policy Rules through Technology, Texas Law Review, Vol. 76, S. 553 ff.; *Shapiro*, The Control Revolution, New York 1999, S. 158 ff.; *L. Lessig*, Code and other Laws of Cyberspace, New York, 1999, S. 142 ff.

2 *H. H. Trute*, Der Schutz personenbezogener Informationen in der Informationsgesellschaft, JZ 1998, 822 ff, 823; zum Begriff des „Leitbildes" vgl. auch *Karstens*, Rechtliche Steuerung von Umweltinnovationen durch Leitbilder, in: Eifert/Hoffmann-Riem (Hrsg.), Innovation und rechtliche Regulierung, 2002, S. 50 ff., 52 ff.

3 Vgl. *E. Schmidt-Aßmann*, Das allgemeine Verwaltungsrecht als Ordnungsidee, 1998, S. 1 f.

Die Ordnungsleistung des Rechts ist nicht zuletzt von der Fähigkeit der Rechtswissenschaft zur Systematisierung des gegebenen Stoffes abhängig, und diese Fähigkeit zur Systematisierung kann auch im Datenschutzrecht nicht ohne ein orientierendes Ordnungsmodell entfaltet werden. Die Konstruktion von Ordnungsmodellen durch *rechtswissenschaftliche* Texte ist zunächst einmal ein wissenschaftsinterner Vorgang. Da diese Arbeit aber nicht von der Kritik existierender Leitbilder in Gesetzgebung und Rechtsprechung getrennt werden kann, entfaltet eine derartige Modellbildung zugleich normative Konsequenzen, und zwar auch solche, die das geltende Recht über rechtspolitische Vorschläge hinaus in unterschiedlicher Weise beeinflussen können. Die Legitimität eines derartigen Unternehmens geht daraus hervor, dass die Lernfähigkeit des Rechtssystems nur durch den beständigen Widerstreit über richtiges Recht erhalten werden kann. Nur die laufende Intervention in das Beobachtete bewahrt das Rechtssystem davor, seine Anpassungsfähigkeit unter den Bedingungen technologischen und gesellschaftlichen Wandels zu verlieren. Angesichts der Veränderungen und Herausforderungen, die die „Informationsgesellschaft" für den herkömmlichen Datenschutz aufwirft, muss auch das Datenschutzrecht einen solchen Beitrag zur laufenden Anpassung des Rechtssystems leisten.

B. Der staatszentrierte Ursprung des datenschutzrechtlichen Leitbildes und seine Abstützung und Verstärkung durch das Bundesverfassungsgericht

Der Zweck des Bundesdatenschutzgesetz, „den einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrechts beeinträchtigt wird" (§ 1 Abs. 1 BDSG), richtet sich in seinem Kern gegen die missbräuchliche Verwendung personenbezogener Daten durch den Informationen sammelnden Staat. Diese Zentrierung auf den Staat als datenerhebende „Stelle" kommt zwar schon in der ersten Fassung des BDSG von 1977 nicht mehr so deutlich zum Ausdruck wie noch im Hessischen Datenschutzgesetz von 1970[4], dem ersten Datenschutzgesetz überhaupt. Sie zeigt sich im BDSG aber u. a. darin, dass dieses eine grundsätz-

4 Das Hessische Datenschutzgesetz von 1970 bezog sich nur auf Daten die „ im Bereich der Behörden des Landes und der der Aufsicht des Landes unterstehenden Körperschaften" erhoben werden (§ 1 HDSG von 1970).

liche Asymmetrie zwischen dem machtunterlegenen Bürger und dem machtüberlegenen Staat unterstellt. Das Gesetz beruht auf der Annahme, dass die staatlichen Regierungs- und Verwaltungsorganisationen mit Hilfe elektronischer Großrechenanlagen in der Lage sind, personenbezogene Informationen massenhaft zu sammeln und verarbeiten. Daraus erwächst, so die Unterstellung des Gesetzes, ein neues Potential der staatlichen Kontrolle der Gesellschaft und der Einzelnen. Diese Steigerung von Kontrollmöglichkeiten wird nicht zuletzt technologischen Bedingungen zugeschrieben: Die neue Technologie der automatisierten Datenverarbeitung wird ähnlich wie das alte Fernmeldesystem der Bundespost als *hierarchisch* aufgebautes technisches System gedacht. Innerhalb dieses hierarchischen Systems sind die einzelnen Komponenten miteinander verbunden, zumindest wird eine wechselseitige Zugänglichkeit zwischen allen Verarbeitungs- und Speicherkomponenten unterstellt. Damit schafft das neue technische Medium des Computers systematische Verknüpfungsmöglichkeiten zwischen den Datenbeständen verschiedenster Behörden und zugleich die Bedingungen für eine flächendeckende, einheitliche staatliche Datenverarbeitung. Das Gefahrenpotential der neuen Medientechnologie wird dabei nicht zuletzt durch die räumliche Abgeschirmtheit staatlicher Rechenzentren symbolisiert: Großrechenanlagen werden ähnlich wie große Chemiefabriken, Geheimdienstzentralen, Gefängnisse und obere Bundesbehörden gegen Übergriffe von außen bewacht oder innerhalb allgemein zugänglicher Gebäude in besonderen Sicherheitszonen untergebracht.

Diese Staatszentrierung des Datenschutzrechts ist ihrerseits stark durch die Rechtsprechung des Bundesverfassungsgerichts abgestützt und verstärkt worden. Bereits die frühen Urteile zum Datenschutz beziehen sich immer auf den Informationen sammelnden Staat, sei es in seiner Gesamtheit wie im Mikrozensus-Urteil[5], sei es auf die Datenerhebung durch staatliche Organisationen (Gerichte, Sozialversicherungsträger, Therapieeinrichtungen).[6] Diese Perspektive dominiert auch in der im Volkszählungsurteil aus der Literatur übernommenen Vorstellung eines Rechts auf „informationelle Selbstbestim-

5 BVerfGE 27, 1.

6 Vgl. nur BVerfGE 27, 344, 345; 32, 373, 379; 44, 353, 374. Zur Entwicklung des Datenschutzes im Sozialversicherungsrecht vgl. nur F. Hase, Handbuch des Sozialversicherungsrechts, Bd. 3, § 41 Rn. 1 ff., Bd. 4, § 23 Rn. 2 ff.

mung“.[7] In der Vorstellung einer „informationellen Selbstbestimmung“ sind, wie in allen rechtlichen Institutionen, normative und kognitive Annahmen unlösbar miteinander verbunden. Normativ gesehen ist das Bundesverfassungsgericht im Volkszählungsurteil von einem objektiv-rechtlichen Grundrechtsverständnis ausgegangen, dessen Grundannahmen erstmalig im Lüth-Urteil angedacht worden sind.[8] Etwas vereinfacht formuliert besteht der Kern der Vorstellung objektiv-rechtlicher Grundrechtsfunktionen darin, die Eingriffsabwehrfunktion der Grundrechte, wie sie angeblich der liberalen Gesellschaft entsprochen haben soll[9], im Wohlfahrtsstaat der Gegenwart um die Komponente einer „Schutzpflicht“ zu erweitern, die es in der Gesellschaft zu realisieren gilt.[10] Die Realisierung dieser verfassungsrechtlichen Schutzpflicht wird allerdings nicht als unmittelbar verfassungsrechtliche Aufgabe angesehen, sondern über das politische System umgeleitet: Der parlamentarisch-demokratische Gesetzgeber erzeugt durch eine verfassungsrechtlich angeleitete Gesetzgebung horizontale Bindungswirkungen zwischen Privatrechtssubjekten und schafft damit die Voraussetzungen für einen umfassenden, nicht nur zwischen Privatpersonen und Staat wirkenden Grundrechtsschutz.

Der staatszentrierten Logik der Schutzpflichtkonstruktion folgt auch das Volkszählungsurteil. Das Bundesverfassungsgericht konturiert zunächst die Befugnis des Einzelnen, „grundsätzlich selbst zu entscheiden, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart wer-

7 BVerfGE 65, 1, 43. Dazu aus der umfangreichen Literatur zur Entstehung dieses Rechts vgl. nur *F. Hufen*, Schutz der Persönlichkeit und Recht auf informationelle Selbstbestimmung, in: FS 50 Jahre Bundesverfassungsgericht, 2001, S. 105 ff., 117 ff; *E. Denninger*, Das Recht auf informationelle Selbstbestimmung, in: Hohmann (Hrsg.), Freiheitssicherung durch Datenschutz, 1987, S. 127 ff., 131 ff.

8 BVerfGE 7, 198 (205 ff.).

9 Zur Kritik an dieser Vorstellung vgl. *K.-H. Ladeur*, Negative Freiheitsrechte und gesellschaftliche Selbstorganisation, 2000.

10 Zur Schutzpflicht vgl. *G. F. Schuppert/Ch. Bumke*, Die Konstitutionalisierung der Rechtsordnung, 2000, S. 18 ff.; *D. Grimm*, Die Zukunft der Verfassung 1991, S. 221 ff.; für den Datenschutz *W. Hoffmann-Riem*, Informationelle Selbstbestimmung in der Informationsgesellschaft, AöR 123 (1998), 513 ff., 522 ff.

den.“[11] Diese Befugnis wird zwar eigentumsanalog als Ausschlussrecht und damit scheinbar als Ausfluss der „freien Selbstbestimmung“ vereinzelter Individuen gedacht.[12] Aber schon die doppelte Verankerung des neuen Grundrechts auf „informationelle Selbstbestimmung“ in Art. 2 Abs. 1 *und* Art. 1 Abs. 1 GG[13] deutet darauf hin, dass das Moment der *Selbst*bestimmung dabei weder als absolut noch als primär angesehen werden darf. Sieht man näher hin, zeigt sich, dass mit dem Recht auf informationelle Selbstbestimmung kein subjektives Recht im Sinne einer autonomen „Willensmacht“ gemeint ist, d.h. kein verteiltes Entscheidungsrecht, dessen Form und Inhalt *primär* durch die dezentrale Verfolgung individueller Interessen, Bedürfnisse oder Vorlieben bestimmt würde. Selbstbestimmung bedarf in einer Verfassungsordnung wie der des Grundgesetzes, die durch die „Gemeinschaftsbezogenheit“ und „Gemeinschaftsgebundenheit“ des Individuums geprägt ist[14], der Vorstrukturierung durch den Staat. Das hat unter den „modernen Bedingungen der Datenverarbeitung“[15] eine objektiv-rechtlich verstandene Handlungspflicht des demokratischen Gesetzgebers zum Datenschutz zur Folge. Diese Kompetenzerweiterung relativiert die individuelle Verwendung personenbezogener Informationen zugunsten einer Schutzpflicht, die den Individuen als kollektiver Selbstschutz zugute kommt. Das Grundrecht auf informationelle Selbstbestimmung wird also letztlich durch ein vorgängiges staatliches „Allgemeininteresse“ relativiert bzw. als stark mit der Funktionsfähigkeit eines Staat, Politik und Gesellschaft übergreifenden „freiheitlichen demokratischen Gemeinwesens“ verknüpft angesehen.[16] Nur deshalb ist die Argumentation des Volkszählungsurteils nicht offenkundig widersprüchlich. Das Bundesverfassungsgericht kann unter dieser Voraussetzung schreiben, dass es kein uneingeschränktes subjektives Entscheidungsrecht gegen die

11 BVerfGE 65, 1, 42; auf S. 43 heißt es, dass der Einzelne die Befugnis habe, „grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen“.

12 Zu den eigentumsrechtlichen Analogien der Rechtsprechung des Bundesverfassungsgerichts vgl. nur *S. Simitis*, in: ders. u.a., Kommentar zum Bundesdatenschutzgesetz, 1997, § 1 Rn. 20 ff.; *F. Hase*, Das Recht auf „informationelle Selbstbestimmung“, in: DuR 1984, S. 39 ff., 40.

13 BVerfGE 65, 1, 42, 43.

14 BVerfGE 65, 1, 42, 44; vgl. auch 4, 7, 15 f.

15 BVerfGE 65, 1, 42, 43.

16 BVerfGE 65, 1, 43.

„Erhebung, Speicherung, Verwendung und Weitergabe“ von Informationen durch den Staat gebe[17], ohne damit in Widerspruch zu seiner eigenen Ausgangsannahme zu geraten, der zufolge der Einzelne „grundsätzlich selbst zu entscheiden [hat], wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden.“[18]

Die Gründe für dieses staatszentrierte Leitbild werden klarer, wenn man die andere Seite, die kognitiven Unterstellungen, mit denen das Bundesverfassungsgericht operiert, etwas genauer analysiert. Die Beziehung, an der der grundrechtliche Datenschutz im Volkszählungsurteil orientiert wird, ist die Beziehung zwischen Bürger und Staat. Diese Beziehung wird wie in der politischen Datenschutzgesetzgebung als asymmetrisch gedacht, als Beziehung zwischen „gläsernem Bürger“ und potentiellem „Überwachungsstaat“. Weil der Staat seit seiner Entstehung als absolutistischer Staat ein großes Interesse an Geheimnissen und Geheimhaltung ausgebildet hat[19], wird die Erhebung von Informationen durch öffentliche Stellen und ihre Abschirmung nach außen nicht grundsätzlich abgelehnt (wie es im Übrigen noch heute den gesetzlichen Wertungen des § 29 Abs. 2 VwVfG entspricht[20]). Aber die Ergänzung und Substitution der bis dahin von der staatlichen Verwaltung genutzten Kommunikationsmedien, die Substitution von Karteien und Akten durch Computer wird als Anwachsen, ja als Hypertrophie bürokratischer Handlungsmöglichkeiten interpretiert. Ähnlich wie Carl Schmitt im Aufkommen neuer technischer Kommunikationsmedien in den dreißiger Jahren in erster Linie eine Erweiterung der Machtpositionen des modernen Staates gesehen hatte[21], liest auch das Bundesverfassungsgericht Mediengeschichte als Geschichte *staatlichen* Machtzuwachses: Der Austausch von Karteien und Akten durch elektronische Speichermedien ermögliche es, Informationen unbegrenzt anzuhäufen und „jederzeit ohne Rücksicht auf Entfernungen in Se-

17 BVerfGE 65, 1, 43.

18 Siehe Fn. 8.

19 Vgl. dazu *R. Kosseleck*, Kritik und Krise (1959), 1973, S. 49 ff.

20 Dazu kritisch *F. Schoch*, Informationsfreiheitsgesetz für die Bundesrepublik Deutschland, Die Verwaltung 2002, S. 149 ff.

21 *C. Schmitt*, Machtpositionen des modernen Staates, in: ders., Verfassungsrechtliche Aufsätze, 1973, S. 367 ff.

kundenschnelle“ abzurufen.[22] Der Computer steigere die Kommunikationsmöglichkeiten des Staates und berge neuartige Missbrauchsmöglichkeiten in sich. Stellen der öffentlichen Verwaltung werde die Möglichkeit eingeräumt, „vollständige Persönlichkeitsbilder“[23] anzulegen, deren Verwendungsreichtum vom Einzelnen nicht kontrolliert werden könne.

Die kognitive Grundannahme eines staatlichen Machtzuwachses wird dann in eine normative Sprache übersetzt. Die der staatlichen Verwaltung eingeräumte technische Möglichkeit, mit Hilfe des Computers „vollständige Persönlichkeitsbilder“ anzulegen, erzeugt im Zweifelsfall einschüchternde Effekte für die Staats-Bürger. Das aber kann in einem „demokratischen Gemeinwesen“ weder mit Blick auf das Grundrecht auf „informationelle Selbstbestimmung“ noch mit Blick auf andere (Grund-)Freiheiten wie insbesondere Art. 5 und 8 GG hingenommen werden. Dieses Nicht-Hinnehmbare konturiert zugleich den Inhalt der „Schutzpflicht“: Um das Recht des machtunterlegenen Einzelnen auf „informationelle Selbstbestimmung“ verfassungsrechtlich wirksam zu schützen und Tendenzen der umfassenden Kontrolle der Einzelnen durch den Staat entgegenzuwirken, wird der „demokratische Gesetzgeber“ verpflichtet, klare gesetzliche Handlungsgrundlagen für den verwaltungsförmigen Umgang mit personenbezogenen Daten zu schaffen. Darüber hinaus verlangt das Bundesverfassungsgericht neue ergänzende Instrumente zur Sicherung der Effektivität des Rechts auf „informationelle Selbstbestimmung“, und hier vor allem eine Ergänzung des Grundrechtsschutzes durch Organisation und Verfahren, was dann u. a. zur gesetzlichen Einrichtung von Datenschutzbeauftragten geführt hat (vgl. nur §§ 22 ff. BDSG).

C. Der allgemeine Hintergrund der Erweiterung des Datenschutzrechts auf gesellschaftliche Beziehungen

Nach dem Bundesdatenschutzgesetz richtet sich der einfachgesetzliche Schutz gegen den Missbrauch personenbezogener Daten allerdings nicht nur, wie bislang unterstellt wurde, gegen Beeinträchtigungen durch „öffentliche Stellen“ (§ 1 Abs. 2 Nr. 1 und 2 BDSG), sondern auch gegen Beeinträchti-

22 BVerfGE 65, 1, 42.

23 BVerfGE 65, 1, 42.

gungen durch private Unternehmen und Organisationen (vgl. § 1 Abs. 2 Nr. 3 BDSG).[24] Damit wird der Datenschutz auf den Bereich der Beziehungen zwischen Privatrechtssubjekten erstreckt und die in der Anlage des Bundesdatenschutzgesetzes enthaltene und in der Rechtsprechung des Bundesverfassungsgerichts vorausgesetzte Fixierung auf den seine Befugnisse zur Datenverarbeitung missbrauchenden Staat relativiert. Bereits diese Ausdehnung des Datenschutzes auf gesellschaftliche Beziehungen, an denen der Staat nicht beteiligt ist, ist nicht unproblematisch, die Probleme, die der erweiterte Datenschutz produziert, werden aber insofern begrenzt, als diese Erweiterung nur für gesellschaftliche Beziehungen zwischen Privatrechtssubjekten gilt, in denen Datenerhebung in einem Zusammenhang mit geschäftsmäßigen, gewerblichen oder beruflichen Tätigkeiten erfolgt.

Hintergrund dieser Ausdehnung des Datenschutzes auf gesellschaftliche Beziehungen ist die umfassende elektronische Eigenaufrüstung der Gesellschaft, wie sie mit dem Fortschritt der Medien- und Computertechnologie einhergeht. Obwohl es entgegen einem weit verbreiteten Vorurteil vermutlich nicht einfach zu beurteilen ist, ob die Sammlung und Nutzung personenbezogener Informationen seit den frühen achtziger Jahren, dem Zeitpunkt des Volkszählungsurteils, weiter zugenommen hat, ist es nicht zu bestreiten, dass durch die Leistungssteigerung der Medien- und Computertechnologie viele Ausschnitte der sozialen Kommunikation einer zufallsgesteuerten und teilweise sogar systematischen Kontrolle zugänglich gemacht worden sind. So hat beispielsweise die Installation von stationären Video-Überwachungsanlagen in Supermärkten, Tankstellen, Einkaufsstraßen, Outlet-Centern, Hotel-Empfangshallen, Privatgrundstücken etc. zu einer enormen Intensivierung der Erhebung, Speicherung und teilweise unbefugten Benutzung personenbezogener Daten geführt, die inzwischen sogar eine eigene Sparte des Reality-TV hervorgebracht hat, die Berichterstattung über „zufällig“ gefilmten Spontansex in der Öffentlichkeit. Dieser Trend der Ausdehnung der Möglichkeiten der elektronischen Selbstbeobachtung der Gesellschaft wird künftig durch neue Typen von mobilen Kommunikationssystemen weiter verstärkt werden. So lassen sich etwa in Verbindung mit GPS nicht nur in die Navigationssysteme

24 Zur Gleichstellung von Privatem und Öffentlichem im Datenschutzrecht vgl. nur *Roßnagel/Pfitzmann/Garstka* (Fn.1), S. 48 ff.

von (Luxus-)Autos Ortungssender einbauen, sondern auch in Notebooks, Handys und elektronische Adressbücher.

Darüber hinaus hat die Einführung von Kreditkarten, Kundenkarten und Kundenbindungssystemen aller Art die Sammlung und Speicherung personenbezogener Daten intensiviert. Die Miles-and-More-Karte der Lufthansa hat eben nicht nur Freiflüge für ihre Benutzer zur Folge, sondern auch, dass Ortsbewegungen von Personen genau registriert und über Jahre in privaten elektronischen Speichern archiviert werden können. Auch die Bahn AG hat ihren Fahrkartenverkauf bereits teilweise auf Online-Systeme umgestellt und beabsichtigt noch in diesem Jahrzehnt eine vollelektronische Kontenführung mit jährlichem Abrechnungszeitraum einzuführen. Auch diese technologische Innovation wird zu einer weiteren Verdichtung der Sammlung und Archivierung personenbezogener Informationen führen. Allein das Management solcher Kundendaten ist inzwischen ein florierender Wirtschaftszweig. Beispielsweise erwirtschaftet die für das Management von Kundendaten im Bertelsmannkonzern zuständige Arvato-Group ca. 15 % des Jahresumsatzes des Gesamtkonzerns und erreicht damit einen Umsatz (ca. 20 Mrd. €), der ungefähr dem Umsatz des größten europäischen Presseunternehmens, der Verlagsgruppe Gruner&Jahr, entspricht. Schließlich kann man in diesem Zusammenhang noch an die zunehmende Bedeutung von Smartcards bei der Benutzung von Dienstleistungen aller Art hinweisen, etwa bei der Abrechnung im Pay-TV. Auch in diesem Zusammenhang wird individuelles Verhalten sehr viel genauer als früher elektronisch registriert und gespeichert.

D. Die Übertragung des herkömmlichen Leitbildes des Datenschutzrechts auf das Internet

Während die Erweiterung im Bundesdatenschutzgesetz zunächst auf geschäftsmäßige, gewerbliche oder berufliche Tätigkeiten beschränkt blieb, diente genau diese Beschränkung (innerhalb einer Erweiterung) Anfang der neunziger Jahre als vermeintlicher Nachweis einer „Schutzlücke“ für den Bereich der Internetkommunikation.[25] Die neue netzwerkförmige konnexionistische Struktur der Internetkommunikation, die ja wesentlich durch nicht-

25 Vgl. nur *Boehme-Neßler* (Fn. 1), S. 293.

professionell arbeitende Nutzer geprägt wird (und auch in ihrem technologischen Kern egalitär ist[26]), benutzte die politische Gesetzgebung jetzt als Grund dafür, das Bundesdatenschutzgesetz durch eine bereichsspezifische Datenschutzgesetzgebung zu ergänzen. Die bereichsspezifische Datenschutzgesetzgebung knüpft ihrerseits an die pragmatischen Verwendungsmöglichkeiten des Computers an und folgt den insbesondere aus der Perspektive der Rundfunkregulierung entworfenen diensteorientierten Unterscheidungen des Medienrechts.[27] Die einschlägigen datenschutzrechtlichen Vorschriften, die auf internetbasierte Kommunikationsbeziehungen Anwendung finden können, finden sich daher heute in so unterschiedlichen Gesetzen wie dem Teledienstdatenschutzgesetz (TDDSG) und im Mediendienstestaatsvertrag (§§ 12 ff. MDStV); einschlägig können im Einzelfall aber auch das im Telekommunikationsgesetz (§§ 85 ff. TKG) und der Rundfunkstaatsvertrag (§§ 47 a ff. RStV) sein. Zwar gehen diese bereichsspezifischen Gesetze und Vorschriften den allgemeinen datenschutzrechtlichen Bestimmungen des Bundesdatenschutzgesetzes vor.[28] Die Zielsetzung des umfassenden Schutzes personenbezogener Informationen muss aber auch für die bereichsspezifischen Regeln und Vorschriften als geltend unterstellt werden, auch wenn dieses datenschutzrechtliche Leitbild in den bereichsspezifischen Regelungen nicht noch einmal explizit aufgegriffen wird.

Mit der Ausdehnung des Datenschutzes auf die Internetkommunikation sind einige qualitative Neuerungen der politischen Datenschutzgesetzgebung einhergegangen. Dazu gehört etwa eine Ergänzung des personenbezogenen Datenschutzes um stärker technologieorientierte Regelungen wie z.B. der Grundsatz der Datensparsamkeit in § 12 Abs. 5 MDStV. Diese Neuerungen zielen auf eine datenschutzfreundliche Ausgestaltung der Netzwerkarchitektur und werden in der datenschutzrechtlichen Diskussion in der Regel als

26 Vgl. dazu die Beiträge von *M. Hutter* und *Ch. Engel* in diesem Band; sowie *M. Froomkin,* Habermas@discourse.net: Towards a Critical Theory of Cyberspace, pp. 1-93, 16, http://www.discourse.net/ils.pdf.

27 Dazu aus neuerer Zeit etwa *F. Schoch*, Konvergenz der Medien – Sollte das Recht der Medien harmonisiert werden?, JZ 2002, 798 ff., 800 ff.

28 Zum Verhältnis BDSG/TDDSG vgl. nur *S. Engel-Flechsig*, Einleitung TDDSG, in: Roßnagel (Hrsg.), Recht der Multimediadienste, 2000, Rn. 58 ff.

„Systemdatenschutz“ bezeichnet.[29] In die Nähe solcher gesetzlicher Innovationen gehört auch der Rekurs auf die veränderten medialen Bedingungen der Kommunikation, wie sie etwa in der Ergänzung und Substitution der schriftlichen durch eine elektronische Einwilligung zum Ausdruck kommt. So ermöglichen beispielsweise § 12 Abs. 8 MDStV und § 5 TDDSG die von der Schriftform abweichende neuartige Form der elektronischen Einwilligung (per Mausklick), eine Abweichung, die im BDSG auch nach seiner letzten Änderung nur unter eng verstandenen Ausnahmebedingungen zugelassen ist.[30] Außerdem verfügt das Datenschutzrecht über „marktwirtschaftliche Elemente“, für die in der datenschutzrechtlichen Literatur immer wieder das Datenschutz-Audit als Beispiel genannt wird.[31]

Insgesamt fügen sich diese Neuerungen aber nicht zu einem neuen Leitbild des Datenschutzrechts oder gar zu einem neuen Ordnungsmodell (im oben, unter I, eingeführten Sinne des Wortes). Wie im Fall der Ausweitung des BDSG auf gesellschaftliche Beziehungen handelt es sich im Fall des internetbezogenen Datenschutzes vielmehr um Ergänzungen, die an das alte staatszentrierte Leitbild des Datenschutzes anzuknüpfen versuchen und den Kern dieses Modells, das Eingriffsabwehrkonzept samt Verbot mit Erlaubnisvorbehalt[32], nicht antasten. Die elektronische Eigenaufrüstung der Gesellschaft und die dadurch produzierten Gefahren und Risiken scheinen die Übertragung der Grundstrukturen des ursprünglich staatszentrierten Datenschutzes auf eine dienstepezifische Internetregulierung zu rechtfertigen. Jedenfalls hat die politische Datenschutzgesetzgebung die für den staatszentrierten Datenschutz unterstellte Asymmetrie zwischen „Überwachungsstaat“ und „gläsernem Bürger“ einfach in eine Asymmetrie zwischen „Überwachungsgesellschaft“ und „gläsernem Verbraucher“ umformuliert, ohne sich näher auf die Veränderungen, die das Internet für den Datenschutz bedeutet, einzulassen.

29 Vgl. nur *J. Bizer*, Kommentierung zu § 3 TDDSG, in: Roßnagel (Fn.28), Rn. 307; *Boehme-Neßler* (Fn. 1), S. 293.

30 *P. Schaar*, Datenschutzrechtliche Einwilligung im Internet, MMR 2001, 644 ff.

31 Vgl. dazu nur *H. Bäumler*, Marktwirtschaftlicher Datenschutz, DuD 2002, 325 ff.; *J. Bizer*, Datenschutzrechtliche Informationspflichten, in: Bäumler/v. Mutius (Hrsg.), Datenschutz als Wettbewerbsvorteil, 2002, S. 125 ff.

32 Dazu nur *A. Roßnagel*, Einleitung, in: ders. (Fn. 1), Rn. 53; *Bizer* (Fn. 29) Rn. 55 ff.

Das internetbezogene Datenschutzrecht ist heute in einem generellen Missbrauchsverdacht gegen Daten erhebende wirtschaftliche „Mächte“ fundiert, so wie das herkömmliche Datenschutzrecht in einem Missbrauchsverdacht gegen den Staat fundiert ist.

Schaut man jedoch genauer hin, zeigt sich, dass durch die Zunahme der Bedeutung der Internetkommunikation auch die stillschweigenden (kognitiven und normativen) Voraussetzungen des Datenschutzrechts unter Druck geraten. Vor allem die Verwandlung von Informationen in Wirtschaftsgüter, eine Bewegung, die durch die Möglichkeiten der Internetkommunikation weiter forciert wird, stellt das herkömmliche Leitbild des Datenschutzes auf eine harte Probe. Das gilt auch für die staatszentrierte Schutzpflichtkonstruktion des Bundesverfassungsgerichts und die in ihr enthaltene Annahme, dass sich die „informationelle Selbstbestimmung“ einer Verfügung der Privatrechtssubjekte entziehen könnte und als in der menschlichen Würde verankertes Persönlichkeitsrecht vom Staat „strukturell“ gesichert werden müsste. In all den eben erwähnten Beispielen, vom Bonus-Meilen Konto bis zu den Smart-Cards werden personenbezogene Daten nicht zwangsweise durch Polizei und öffentliche Verwaltung erhoben und dann für „Herrschaftszwecke“ missbraucht, sondern freiwillig durch Verträge und Einwilligungen der Betroffenen in Umlauf gebracht. Szenarien einer allgegenwärtigen Sammlung und Speicherung von Informationen (Stichwort: 1984)[33], sind also, wenn überhaupt, nicht auf der Seite des Staates, sondern auf der Seite der Gesellschaft Realität geworden. Und angesichts dieser Lage fragt sich doch, ob man den Datenschutz einfach aus der Bürger/Staat-Beziehung herauslösen und mit Hilfe einer Schutzpflichtkonstruktion in einen unspezifischen horizontalen Drittschutz umbauen kann, ohne genauer auf die Veränderungen der kognitiven Voraussetzungen des alten Leitbildes zu reagieren. Welche Auswirkungen eine solche „Strategie“ hat, wollen wir uns im nächsten Abschnitt anhand einiger neuerer Entwicklungen im Internet näher ansehen.

33 Dazu nur *F. Hufen*, Das Volkszählungsurteil des Bundesverfassungsgerichts und das Grundrecht auf informationelle Selbstbestimmung – eine juristische Antwort auf „1984“?, JZ 1984, 1072 ff.

E. Exemplarisch: Nutzerprofile, Data-Mining, Cookies

I. Personenbezogene Informationen als Güter der „Internetökonomie"

Der Trend, personenbezogene Informationen in Wirtschaftsgüter zu transformieren, lässt sich auch in Zusammenhängen beobachten, in denen das Internet inzwischen eine wichtige Wertschöpfungsquelle oder doch zumindest ein wichtiges Glied innerhalb einer Wertschöpfungskette darstellt. In ökonomischer Hinsicht wird der Vorteil des Internets u. a. darin gesehen, in Geschäftsbeziehungen zwischen Unternehmen (B2B) sowie zwischen Unternehmen und Kunden (B2C) einen besseren Informationsaustausch und damit eine in der herkömmlichen industriellen Massenproduktion nicht mögliche „Individualisierung" von Produkten und Dienstleistungen zuzulassen. Die kundenbezogene Individualisierung läuft in der Internet-Branche auch unter dem Stichwort „Customization"[34], ein Begriff, der primär auf die durch das Internet mögliche Prozesskostenoptimierung zielt, also die Senkung von Transaktionskosten, etwa durch Einsparen von Portokosten und den vereinfachten elektronischen Zugriff auf „Endverbraucher". Damit eng verbunden sind neuartige Marketingmöglichkeiten, insbesondere das Direktmarketing als Element eines übergreifenden Customer-Relationship-Marketing (CRM). Im Begriff des Customer-*Relationship*-Marketing, der als Oberbegriff für die Erkennung, Gewinnung, Bindung und Entwicklung von Kunden dient, kommt bereits die Bedeutungszunahme relationaler, prozesshafter Momente zum Ausdruck. Den Hintergrund für diese Bedeutungszunahme von *Beziehungen* und deren längerfristiger Pflege (gegenüber einer Punktualisierung der Zeit z.B. durch die Akzentuierung von „Kauf*entscheidungen*") bildet ein innerhalb, aber auch außerhalb der Internetwirtschaft zu beobachtender Prozess des Anstiegs vielfältiger intra- und interorganisationaler Beziehungsnetzwerke. Vor allem in den neuen Formen des „interfirm networking" wer-

34 Vgl. dazu *Hoeren* (Fn. 1), S. 268; *Boehme-Neßler* (Fn. 1), S. 301 f.; aus der wirtschaftswissenschaftlichen Literatur vgl. nur *A. Zerdick* u.a., Die Internet-Ökonomie, 1999, S. 194 ff.; vgl. auch *K. Imhof*, One-to-One Marketing im Internet – Das TDDSG als Marketinghindernis, CR 2000, 110 ff.

den Markttransaktionen durch Markt und Organisation übergreifende Koordinations- und Kooperationsformen ergänzt und zum Teil auch ersetzt.[35]

Die Individualisierung von Produkten und (Marketing-)Dienstleistungen dürfte in Zukunft zu einem weiteren Anwachsen der Zirkulation und Speicherung personenbezogener Informationen führen. Zwar ermöglicht das Internet zugleich neue Formen der Anonymisierung und vor allem Pseudonymisierung, die von der Datenschutzgesetzgebung u. a. in § 4 Abs. 6 TDDSG und § 13 Abs. 1 MDStV aufgegriffen worden sind und für viele Dienste - z.B. in elektronischen Auktionshäusern - eine wichtige Funktion haben.[36] Die Bedeutung pseudonymer oder anonymer Nutzerdaten darf für unseren Zusammenhang aber nicht überschätzt werden, da unter Marketinggesichtspunkten vor allem die nicht-pseudonymisierten und nicht-anonymisierten Nutzerprofile von ökonomischem Interesse sind.[37] Je mehr Unternehmen individualisierte Produkte und (Marketing-)Dienstleistungen entwickeln und je stärker die Bedürfnisse der Nutzer und Kunden nach solchen Angeboten wachsen, desto größere Mengen personenbezogener Informationen müssen bei Anbietern oder Dritten gesammelt, miteinander abgeglichen, verarbeitet und systematisiert werden. Dabei wird die Pseudonymität von Nutzern auch dann, wenn sie in der Öffentlichkeit gewahrt bleibt, zumindest insofern durchbrochen, als Unternehmen Pseudonymen reale Namen, Geburtsdaten, Wohnorte, Kreditkarten, Bankverbindungen und e-Mail-Adressen zuordnen müssen, um die Daten wirtschaftlich verwerten zu können.

In der Praxis werden nicht-anonymisierte und nicht-pseudonymisierte Nutzer- und Kundenprofile einmal durch Internetunternehmen selbst gewonnen. Um ein netzwerkgerechtes Pendant zur Beratung in guten Buchhandlungen an-

35 Vgl. dazu allgemein *M. Castells*, The Rise of the Network Society, 1996, S. 151 ff., 167 ff.; aus der juristischen Literatur vgl. nur *G. Teubner*, Das Recht hybrider Netzwerke, ZHR 165 (2001), 550 ff.

36 Zur Funktion und Auslegung dieser Regeln vgl. nur *P. Schaar*, Neues Datenschutzrecht für das Internet, RDV 2002, 4 ff., 13 f.; *K.-H. Ladeur*, Datenverarbeitung und Datenschutz bei neuartigen Programmführern in „virtuellen Videotheken“, MMR 2000, 715 ff., 718 ff.

37 *Boehme-Neßler* (Fn. 1), S. 303.

bieten zu können, registrieren beispielsweise die Server von amazon.de, welche Bücher Webnutzer einkaufen, um daraus „persönliche Empfehlungen“ abzuleiten. Diese Empfehlungen werden dem Nutzer beim nächsten Aufruf der Web-Seite präsentiert. Die datentechnische Erzeugung solcher Nutzerprofile ist ohne das sich laufend verschiebende und damit verändernde Kauf- und Leseverhalten der Kunden von amazon.de undenkbar und an den Empfehlungen, ja vor allem an der Treffsicherheit der Empfehlungen, haben die Kunden selbst ein Interesse: So wie ein Leser in der Offline-Welt Interesse an gut informierten Buchhändlern hat, liefert die persönliche Empfehlung im Internet Informationen in einem schwer überschaubaren Markt und schützt Nutzer vor unspezifischem „spamming“, ohne zu einer Kaufentscheidung zu verpflichten. Das Eigeninteresse an einer ökonomischen Verwertung personenbezogener Daten wird gegenüber dem Interesse an Personalisierung und zielsicherem Direktmarketing noch gesteigert, wenn für die Verwertung personenbezogener Informationen Entgelte gezahlt werden und die kommerzielle Gewinnung und Distribution derartiger Informationen selbst zu einer Marktlücke wird. Dabei muss das Entgelt nicht unmittelbar ausgezahlt werden, sondern kann auch die Form von indirekten Entgelten z.B. als Rabatt oder Prämie annehmen, wie es Offline innerhalb der vielfältigen Kundenbindungssysteme längst üblich geworden ist.

Dieser Gedanke ist seit einiger Zeit auch im Internet angekommen. An der Vorstellung des Aufbaus eines möglichst weit verzweigten Kundenbindungssystems ist etwa die Geschäftsidee von webmiles.de orientiert. Webmiles.de ist ein Prämienprogramm, das mit verschiedenen anderen Unternehmen vernetzt ist und dabei auch die Grenze zwischen Online- und Offline-Welt überschreitet. Bei Nutzung der Angebote von Partnerunternehmen, zu denen etwa auch eine im Verbund mit Banken betriebene Kreditkarte gehört, sammeln Webmiles-Nutzer Bonusmeilen, die in Prämien eingelöst werden können. Der Geschäftszweck des Internetunternehmens selbst ist die Generierung von Nutzer- und Kundenprofilen und ihre Verwendung innerhalb des Netzwerks von online- und offline Partnerschaften. Das Interesse der Nutzer ist der Zugang zu möglichst attraktiven Prämien und Rabatten. Auch in diesem Fall werden also personenbezogene Informationen in Wirtschaftsgüter transformiert, an deren möglichst effizienter Verwertung ein gesteigertes Eigeninteresse aller Beteiligten besteht.

II. Das „umfassende Kundenprofil“ als Substitut des „vollständigen Persönlichkeitsbildes“

Wie wenig die kognitiven Voraussetzungen des herkömmlichen Leitbildes des Datenschutzrechts in der bereichs- und dienstespezifischen Datenschutzregulierung hinterfragt werden, zeigt sich im Zusammenhang mit den neuen Formen des Direktmarketings darin, dass diese in der datenschutzrechtlichen Literatur zumeist als „Gefährdungen“ oder „Bedrohung“ des Rechts auf informationelle Selbstbestimmung interpretiert werden.[38] Damit werden die grundlegenden Unterschiede zwischen dem staatszentrierten Datenschutz und dem Datenschutz im Internet von Anfang an verwischt: Während totalitäre politische Systeme in der Vergangenheit immer wieder ein Interesse an der Überwachung aller Seiten des Lebens von Menschen entwickelt haben[39] und die Sammlung personenbezogener Informationen auch in liberalen Staaten in bestimmten Bereichen nur schwer zu begrenzen ist, gibt es weder ein wirtschaftliches Interesse an der Erstellung vollständiger Persönlichkeitsbilder noch bietet das Internet die technologischen Möglichkeiten, „umfassende Kundenprofile“[40] zu erstellen. Kundenprofile sind nie umfassend, denn hier geht es immer um die Beobachtung eines Ausschnitts der Lebensrealität von Individuen, im Wesentlichen um Aspekte des Konsumverhaltens. Dabei geht es den Webunternehmen in der Regel um eine möglichst sichere Zurechnung von Zahlungsfähigkeit und Zahlungsbereitschaft auf Kundenprofile, also um eine Verknüpfung selektiver personenbezogener Informationen mit „Profilen“, d.h. mit schemenhaften Bildern oder auch „Masken“[41], die sich nach statistischen Methoden (und Erfahrungen) aus bestimmten Verhaltensweisen

38 Typisch z.B. *Bizer* (Fn. 29), Rn. 136; *Rasmussen*, Datenschutz im Internet, CR 2002, 36 ff., 37 mit Blick auf den Einsatz von Cookies; vgl. auch *Peters/Kersten*, Technisches Organisationsrecht im Datenschutz, CR 2001, 576 ff., 577. Dort heißt es: „Was den organisierten Handel mit hoch sensiblen personenbezogenen Daten betrifft, so stehen wir erst am Anfang. Doch ist bereits jene skrupellose Entschlossenheit zur Beherrschung eines riesigen Marktes festzustellen, von denen die Märkte mit zweifelhafter bzw. eindeutig negativer ethischer Zielsetzung stets gekennzeichnet sind.“

39 Vgl. nur *C. Vismann*, Akten, 2000, S. 306 ff.

40 So aber z.B. *Bizer* (Fn. 29), Rn. 136; ähnlich *Roßnagel/Pfitzmann/Garstka* (Fn. 1), S. 117.

41 Vgl. *K.-H. Ladeur*, Datenschutz – vom Abwehrrecht zur planerischen Optimierung von Wissensnetzwerken, DuD 2000, 12 ff.

herauslesen lassen. Aber selbst diese Verhaltensweisen werden nicht individuell, bis ins letzte personenbezogene Detail gespeichert. So geht es gerade beim Direktmarketing um gruppenförmige Typisierungen, deren weitere Auflösung und Auffächerung wirtschaftlich ineffizient wäre. Unternehmen mögen heute ein größeres Interesse an Informationen haben, die Individualisierungen und Personalisierungen von Produkten und Dienstleistungen ermöglichen, aber doch immer in Form der Paradoxie, als individualisierte Massenproduktion, nicht aber in der Form der handwerklichen Herstellung von Unikaten oder zur Erbringung von Einmaldienstleistungen.

Eine weitere stillschweigende Fortschreibung des alten Modells zeigt sich darin, dass die neuartige netzwerkförmige, konnexionistische Struktur des Internets mehr oder weniger übergangen wird.[42] Informationen werden in der Internetkommunikation nicht einmalig und einseitig, durch eine auf Zwang beruhende Erstellung gewonnen und dann in staatlich kontrollierten Großrechenanlagen als fixe Bilder für alle Ewigkeit gespeichert. Im Internet geht es um die dezentrale, prozessartige Gewinnung von Informationen aus einer laufenden netzwerkartigen Beziehung zwischen Unternehmen und Nutzern, in denen die wechselseitige Beobachtung in Mehrfachbeziehungen z.B. in Dreiecksverhältnissen zwischen zwei Unternehmen und einer Vielzahl von Nutzern eher die Regel als die Ausnahme ist. Diese Interaktionsformen erlauben Unternehmen zwar Rückschlüsse auf nutzer- und kundenspezifische Bedürfnisse, Konsumverhalten, Markenpräferenzen etc. und damit auch, einen ökonomischen Mehrwert hinter dem Rücken der Nutzer und Kunden zu produzieren. Aber dieser ökonomische Mehrwert kann nur durch eine *aktive* Rolle des Nutzers generiert werden, der durch Intervention in die Prozesse der wechselseitigen Fremd- und Selbstbeobachtung einen Einfluss auf die Entwicklung von Nutzer- und Kundenprofile behält. Das heißt umgekehrt, dass die neuen Formen der Produktindividualisierung und des Direktmarketings nur funktionieren, wenn Nutzer und Kunden selbst ein Interesse an der Sammlung und Speicherung von Daten haben oder Unternehmen Bedingungen schaffen, in denen ein solches Interesse erzeugt und auf längere Sicht stabil gehalten werden kann.

42 Zu dieser Struktur vgl. nur *S. Weber*, Medien – Systeme – Netze, 2001; *M. Faßler*, Netzwerke, 2001.

III. Reaktionen der politischen Datenschutzgesetzgebung

Wie wenig die bereichsspezifische Datenschutzgesetzgebung diesen technischen und ökonomischen Veränderungen gerecht wird, zeigt sich angesichts der Entstehung eines internetbasierten Marktes für den Handel mit Nutzerprofilen bereits daran, dass der Datenschutz noch immer von einem Verbot mit Erlaubnisvorbehalt ausgeht (vgl. nur § 12 Abs. 3 MDStV, § 3 Abs. 1 TDDSG).[43] Welch zweifelhafte Ergebnisse diese Art staatlicher Datenschutzfürsorge impliziert, lässt sich zunächst im Bereich der Erstellung von Nutzerprofilen demonstrieren. Hier läuft die Datenschutzgesetzgebung tendenziell auf eine ökonomische Verhinderungsstrategie hinaus. Einerseits wird die Anfertigung von Nutzerprofilen von einer Einwilligung abhängig gemacht, andererseits wird aber selbst diese Einwilligung an ein nicht leicht verständliches Kopplungsverbot geknüpft (z.B. §§ 3 TDDSG, 12 MDStV). Danach darf ein Internetunternehmen, jedenfalls wenn es eine Monopolstellung hat, den Zugang zu seinen Leistungen nicht „von einer Einwilligung in eine Verarbeitung oder Nutzung seiner Daten für andere Zwecke abhängig machen" (§ 3 Abs. 4 TDDSG; § 12 Abs. 4 MDStV). Bei dieser Vorschrift ist vor allem unklar, was unter „anderen Zwecken" zu verstehen sein soll. Letztlich baut die Vorschrift auf der herkömmlichen Vorstellung eines punktuellen Eingriffs in die datenschutzrechtlich geschützte Persönlichkeitssphäre auf, der einmaligen Datenerhebung, die dann für „andere Zwecke" missbraucht wird.[44] Die Geschäftskonzepte von Internetunternehmen beruhen aber meistens auf einer Verknüpfung unterschiedlicher Zwecke, z.B. der Verknüpfung von E-Commerce und Direktmarketing. Und wenn die wirtschaftliche Praxis Formen der Kundenbindung ausbildet, in denen der Zweck der Nutzung eines Internetdienstes primär darin besteht, Nutzerdaten zu sammeln, besteht die ratio der Vorschrift nur noch darin, „Widerstand" gegen diese Formen von Geschäftstätigkeit zu leisten. Zumindest kann die in der Kommentarliteratur verbreitete Meinung nicht richtig sein, dass der Diensteanbieter sich die Einwilligung in die ansonsten gesetzlich untersagte oder nur einschränkend erlaubte Erstellung von Nutzer- und Kundenprofilen (z.B. § 6 Abs. 3 TDDSG) nicht „er-

43 Vgl. dazu und zur Rechtfertigung des Gesetzesvorbehalts z.B. *Bizer* (Fn. 29), Rn. 55 ff.

44 Davon gehen u. a. *Roßnagel/Pfitzmann/Garstka* (Fn. 1), S. 115 ff., ganz selbstverständlich aus.

kaufen“ können soll.[45] Damit würde die Dezentralität und Interaktivität des Internets ignoriert und das Moment der Privatautonomie des Webnutzers einkassiert. Das Internet weist dem Nutzer selbst eine zentrale Rolle bei der Erstellung und Pflege von Nutzerprofilen zu, jedenfalls macht es die Annahme unplausibel, dass hier einzelne Daten zu „Persönlichkeitsprofilen“ zusammengefügt werden, deren Richtigkeit und Verwendung sich der Kontrolle des Nutzers entziehen könnten.[46]

Nicht sehr viel anders geht die Datenschutzgesetzgebung mit dem kommerziellen Datentransfer zwischen Unternehmen um. Die Errichtung leistungsfähiger Datenpools, die aus der Verknüpfung unterschiedlicher Datenquellen hervorgehen, und der Verkauf solcher Datenbestände an Unternehmen, die diese Datenbestände ihrerseits mit Daten anreichern, die sie selbst gesammelt haben, wird heute in der (Internet-)Wirtschaft wohl noch nirgends in größerem Umfang praktiziert. Sollte der Trend zum Direktmarketing aber anhalten und die Erstellung von Kundenprofilen durch das Internet erst einmal eine gewisse Komplexität erreicht haben, ist leicht vorstellbar, dass sich ein ökonomisches Interesse an der Steigerung des wirtschaftlichen Verwendungsreichtums solcher Datenbestände entwickeln wird. Es dürfte dann sowohl innerhalb großer Konzerne als auch zwischen kooperierenden Unternehmen ein interner Druck entstehen, die Datengrundlagen für die Herstellung von Kundenprofilen quantitativ und qualitativ zu erweitern, ihre Genauigkeit und Treffsicherheit zu verbessern und die jeweils vorhandenen Datenbestände wechselseitig füreinander zugänglich zu machen. Das wird insbesondere solche Unternehmen betreffen, die auf das Erstellen von Kundenprofilen und das darüber hinaus gehende Sammeln von Datenbeständen mit Hilfe des Internets spezialisiert sind und diese Bestände für Zwecke des Direktmarketings innerhalb eines Konzerns und/oder an externe Unternehmen verkaufen (Data-Mining).

Darauf reagiert das deutsche Datenschutzrecht mit einem generellen Verbotsverdacht. Dabei handelt sich insofern um einen „Verdacht“, als es keine aus-

45 So z.B. *Bizer* (Fn. 29), S. 121.

46 So aber *Roßnagel/Pfitzmann/Garstka* (Fn. 1), S. 117 mit Hinweis auf BVerfGE 65, 1, 53 f.

drücklichen gesetzlichen Regelungen zum Data-Mining gibt. Der Handel mit verknüpften Kundendaten wird in der datenschutzrechtlichen Literatur aber als unvereinbar mit dem Grundsatz der Datensparsamkeit angesehen. Er widerspricht nach verbreiteter Ansicht außerdem dem Grundsatz der getrennten Generierung und Speicherung von Datenbeständen, wie er in § 4 Abs. 4 Nr. 4 TDDSG und § 13 Abs. 2 Nr. 4 MDSTV normiert ist. Danach müssen sich Unternehmen, die mit Hilfe des Internets Daten sammeln, intern so organisieren, dass die verschiedenen Unternehmensbereiche, in denen Daten gewonnen werden, voneinander getrennt operieren. Dadurch soll gesetzlich verhindert werden, dass Daten aus unterschiedlichen Abteilungen zusammengeführt werden und die Komplexität von Nutzerprofilen wächst.[47] Außerdem ist Data-Mining schwer mit den allgemeinen Grundsatz der Zweckbindung in Einklang zu bringen (§§ 3 Abs. 2 TDDSG, 12 Abs. 3 MDStV). Die Weitergabe einzelner Kundenprofile und der wirtschaftliche Handel mit Kundenprofilen werden in der datenschutzrechtlichen Literatur als Zweckänderung angesehen, die nur durch Unterrichtung und Einwilligung der Betroffenen gerechtfertigt werden kann. Praktisch gesehen muss ein Unternehmen den Umfang des geplanten Data-Mining mit dem Kunden von vornherein zum Thema der Geschäftsbeziehung machen, wenn es den generellen Verbotsverdacht neutralisieren will.[48]

Auch im Fall des Data-Mining fragt sich, was auf Dauer eine gesetzliche Regulierung bewirken soll, die sich nicht auf neue wirtschaftliche Praxisformen einstellt, sondern diese offensichtlich durch „Verbote“ zu traktieren geneigt ist. Das gesetzgeberische Instrument der punktuellen Einwilligung des Nutzers in eine Datenerhebung und deren Weiterverwendung, durch die ein an sich bestehendes „Verbot“ ausnahmsweise aufgehoben wird, passt nicht zu dem prozesshaften, relationalen konnexionistischen Charakter der Internetkommunikation. Es gibt vor allem keine adäquate Form vor, in der die privatautonome Verfügung über Daten und der Handel mit diesen Daten produktiv gestaltet werden könnte. Im Fall des Data-Mining mag das Moment der Interaktivität der Internetkommunikation durchaus anders zu bewerten sein als im Fall der unternehmensbezogenen Profilbildung, weil der Nutzen

47 Vgl. nur *P. Schaar/W. Schulz*, Kommentierung zu § 4 TDDSG, in: Rossnagel (Fn. 1), Rn. 98 ff, 101.

48 *Hoeren* (Fn. 1), S. 268.

komplexerer Profile erst aus einem kollektiven Effekt verschiedener Kausalitäten resultiert, ein Effekt, den der einzelne Nutzer nur sehr begrenzt beeinflussen kann. Aber eine zweckgebundene punktuelle Einwilligung und Unterrichtung ist ein zu inflexibles Mittel, da weder das Unternehmen noch der Nutzer die Zweckbindungen zum Zeitpunkt des Vertragsschlusses überblicken können.[49]

Ein letzter Fall, auf den hier noch kurz eingegangen werden soll, ist die Regulierung von Cookies. Cookies kommen meist dort zum Einsatz, wo Webnutzer anonym operieren. Da beim Internetsurfen im Normalfall dynamische IP-Adressen verwendet werden[50], dem Nutzer also beim Log-In in das Netz vom Access-Provider eine temporäre Adresse zugewiesen wird (und beim nächsten Besuch eine andere), können Internet-Unternehmen normalerweise nicht erkennen, von wem ihre Seiten genutzt werden. Um die systembedingten Nachteile der IP-Adressierung zu umgehen und auch unter den technologischen Bedingungen eines dezentral und netzwerkartig aufgebauten Internets das Nutzerverhalten beobachten zu können, ist es mit Hilfe der marktüblichen Internetbrowser (Microsoft Explorer, Netscape) möglich, kleine Datenpakete beim jeweiligen Nutzer abzulegen. Daraus entsteht eine Datenspur, die es Webunternehmen innerhalb kürzerer Zeiträume ermöglicht, Nutzer wiederzuerkennen und aus ihrem individuellen Verhalten beispielsweise Daten über bestimmte Gewohnheiten oder Vorlieben zu generieren. Diese Daten können dann als Basis für die Erstellung von Datenbeständen in höheren Aggregationen verwendet werden.

Auch auf den Einsatz von Cookies ist das Datenschutzrecht nicht abgestimmt. Zwar fallen Cookies nur dann unter das Datenschutzrecht, sofern die durch die kleinen Textdateien gesammelten Informationen als personenbezogene Daten qualifiziert werden können. Dann aber greift erneut das präventive Verbot mit Erlaubnisvorbehalt i. S. der §§ 3 Abs. 1 TDDSG, § 12 Abs. 2 MDStV. Es kommt dann auf die Einwilligung des Betroffenen an. Eine sol-

49 Zu diesen Schwierigkeiten vgl. nur *A. Büllesbach*, Datenschutz bei Data Warehouses und Data Mining, CR 2000, 11 ff., 17.

50 IP-Adressen sind nach richtiger Ansicht keine personenbezogenen Daten. Vgl. *W. Schulz*, Kommentierung zu § 1 TDDSG, in: Roßnagel (Fn. 1), Rn. 35.

che Einwilligung könnte innerhalb der Möglichkeiten der Netzwerkarchitektur bereitgestellt werden. Die Browsersoftware erfüllt aber die Voraussetzungen der elektronischen Einwilligung nach §§ 3 Abs. 3, 4 Abs. 2 TDDSG nicht.[51] Es ist deshalb momentan nicht möglich, eine wirksame elektronische Bewilligung als Erlaubnistatbestand für die Verwendung von Cookies abzugeben, was nichts anderes heißt, als dass die derzeitige Praxis des Einsatzes von Cookies in der datenschutzrechtlichen Literatur mehrheitlich als rechtswidrig angesehen wird, ein Urteil, das dort um so leichter fällt, als ein wesentliches Problem dieser Literatur auch im Fall der Cookies darin besteht, dass diese mit grob verzerrten kognitiven Beschreibungen operiert und vor allem sehr undifferenzierte Behauptungen über die Leistungsfähigkeit von Cookies aufgestellt werden.[52] Zusammengefasst und wiederum thesenartig zugespitzt kann man daher sagen, dass das eigentliche Problem der neuen Formen der Datenaggregierung in der „Internetökonomie“ nicht in der „skrupellosen Entschlossenheit zur Beherrschung [eines] riesigen Marktes“ gesucht werden muss, wie es in einem durchaus repräsentativen Beitrag aus der datenschutzrechtlichen Literatur heißt[53], sondern in der unspezifischen Ausdehnung des herkömmlichen Datenschutzrechts und des ihm zugrunde liegenden Leitbildes auf neue internetbasierte Formen des Direktmarketings.[54]

51 Vgl. *R. Selk*, Datenschutz und Internet, Dissertation Augsburg 2002, im Erscheinen; *R. Ihde*, Cookies – Datenschutz als Rahmenbedingung der Internetökonomie, CR 2000, 413 ff., 419 f.

52 So ist z.B. das wiederholt vorgetragene Argument, dass sich mit Hilfe von Cookies „umfassende Kundenprofile“ erstellen lassen, nicht zutreffend. Selbst wenn man ein solches Interesse unterstellen würde, gibt es kein größeres Internet-Unternehmen, das technisch in der Lage wäre, Nutzer über Cookies zu identifizieren. Das scheitert schon an der Menge der täglichen Zugriffe, die selbst bei weniger bekannten Webseiten schnell 30.000 Besucher erreicht. Wenn überhaupt können Unternehmen diese Daten nur im Hinblick auf ihre eignen Seiten beobachten, aber kein Unternehmen kann die Spur von Nutzern auch dann noch verfolgen, wenn der Nutzer die Webseite verlässt und zu anderen Inhalten wechselt. Dies wird bereits durch die Zentrumslosigkeit des Internets verhindert, die per se ein hohes Maß an Anonymität der einzelnen Webnutzer sichert.

53 *Peters/Kerstens* (Fn. 38), S. 577.

54 Ähnlich *Imhof* (Fn. 34), S. 110 ff., 116.

F. Zur Kritik der Unbestimmtheit des Datenschutzrechts

I. Allgemeines Persönlichkeitsrecht und demokratisches Gemeinwesen

Die inadäquate Reaktion auf die Bedeutungszunahme des Handels mit personenbezogenen Informationen, wie sie u.a. in den neuen internetbasierten Formen der netzwerkartigen Kooperation zwischen Privaten erfolgt, ist ein Beleg dafür, dass sich das Datenschutzrecht nicht einfach aus der Bürger/Staat-Beziehung herauslösen und mit Hilfe einer staatszentrierten Schutzpflichtkonstruktion sowie einer darauf aufbauenden bereichs- und dienstespezifischen Regulierung in einen horizontalen Vertragsschutz umbauen lässt. Die Übertragung des herkömmlichen Datenschutzes auf das Internet erscheint eher eine wenig durchdachte Verlegenheitslösung zu sein. In einer systemtheoretischen Perspektive ist vor allem auffällig, dass weder dem Volkszählungsurteil des Bundesverfassungsgerichts noch der politischen Datenschutzgesetzgebung einigermaßen klare Unterscheidungen zwischen Politik, Staat, Regierung, öffentlicher Verwaltung und Gesellschaft zu entnehmen sind. Der Datenschutz wird in einem territorialen Staatsverständnis fundiert, dem „demokratischen Gemeinwesen“[55], in dessen Zentrum der handlungs- und wirkungsfähige Staat steht, der durch seine Staats-Bürger hervorgebracht wird. Diese Annahme ist auch jenseits der Effekte, die das weltumspannende Netzwerk des Internets auf das jeweilige nationale Datenschutzrecht hat[56], wenig überzeugend: In einer liberalen Gesellschaft sind den ganzheitlichen Verweisungen, die im Begriff des „demokratischen Gemeinwesens“ mitschwingen, die gesellschaftsstrukturellen Grundlagen entzogen.[57] Begriffe wie Staat und Demokratie können hier nicht länger holistisch gebraucht werden. Auch der Begriff des „demokratischen Gemeinwesens“ erfasst in einer liberalen Gesellschaft immer nur einen Ausschnitt gesellschaftlicher Kommunikation, vor allem die Beziehungen zwischen Regierenden und Regierten, nicht aber sämtliche Handlungskontexte, in die Individuen hier verstrickt sind.

55 BVerfGE 65, 1, 43.

56 Dazu etwa *J. R. Reidenberg*, E-Commerce and Trans-Atlantic Privacy, Houston Law Review 2001, 717 ff.; *Ch. Engel*, Organising Co-Existence in Cyberspace, Reprints MPI Projektgruppe Gemeinschaftgüter, 2002.

57 Vgl. dazu *N. Luhmann*, Die Politik der Gesellschaft, 2000.

Dies ist auch im Volkszählungsurteil nicht wirklich reflektiert worden. Anders ist es kaum zu erklären, dass die Vorstellung „informationeller Selbstbestimmung“ überhaupt jemals so stark mit der Rolle des Staats-Bürgers in der Demokratie assoziiert und verfassungsrechtlich im allgemeinen Persönlichkeitsrecht verankert werden konnte. Die weitaus größere Anzahl personenrelevanter Informationen zirkulieren in einer liberalen Gesellschaft ja gerade *nicht* in politischen Zusammenhängen. Schon lange vor dem Aufkommen und der Verbreitung des Computers war es äußerst einseitig, den Datenschutz an einer als vertikal gedachten Beziehung zwischen Bürger und Verwaltung zu orientieren. „Selbstbestimmung“ schließt in einer liberalen Gesellschaft ja nicht aus, sondern ein, dass laufend Informationen über Personen, ihre Herkunft, ihren Bildungsgang, ihren Beruf, ihren Gesundheitszustand, ihre Konsumgewohnheiten, ihre kulturellen Vorlieben etc. kommuniziert werden. Dafür gibt es ganz unterschiedliche Gründe und Ursachen, beispielsweise weil Alltagskonventionen es verlangen oder Einzelne sich davon in bestimmten Situationen ökonomische Vorteile versprechen. Insbesondere wenn Interaktionen einen Kontext voraussetzen, der erst durch die Weitergabe personenbezogener Informationen aufgebaut und stabilisiert werden kann, ist die Relativität der Bedeutung des „demokratischen Gemeinwesens“ evident. Man denke nur an Arzt/Patienten-Verhältnisse, Arbeitnehmer/Arbeitgeber-Beziehungen, an die Tätigkeiten von Banken, Personalberatern, Immobilienmaklern, an exklusive Kundenbeziehungen z. B. im Automobilhandel oder an den Versandhandel (Otto, Quelle, Neckermann etc.). In all diesen Bereichen wurden Informationen über persönliche und sachliche Verhältnisse von Individuen schon lange vor der Erfindung des Computers registriert und über Jahre archiviert, auch wenn die technischen Speichermedien andere waren als heute. Kurzum: Von der Kommunikation persönlicher Lebenssachverhalte dürfte in der liberalen Gesellschaft schon immer ein Großteil aller Kommunikationen bestimmt gewesen sein. Die unspezifische verfassungsrechtliche Verankerung des Datenschutzrechts in einem als allgemein gedachten „Persönlichkeitsrecht“ erweist sich somit nur als Kehrseite

einer unreflektierten Staats- und Demokratiezentrierung innerhalb des Leitbildes des herkömmlichen Datenschutzrechts.[58]

II. Unbestimmtheit des Datenbegriffs – Grenzen der Sphärentheorie

Wie folgenreich der staatszentrierte Ausgangspunkt ist, zeigt sich auch im Begriff des „Daten-Schutzes" selbst, sofern man diesen nur aus seiner Staatszentrierung herauslöst.[59] In der datenschutzrechtlichen Literatur werden „Daten" oft als relativ exakt fixierte Informationen bezeichnet, etwa als Einzelangaben über persönliche und sachliche Verhältnisse (§ 3 Abs. 1 BDSG). So findet man in der datenschutzrechtlichen Literatur etwa das Beispiel, dass die Reifenspur eines Autos kein Datum im Sinne des § 3 Abs. 1 BDSG sein könne, sehr wohl aber die in der Kommunikation erfolgende Zurechnung der eine Reifenspur betreffenden Mitteilung auf eine bestimme Person.[60] Damit wird der Akzent vom Datenbegriff auf die räumliche Vorstellung der Nähe oder Ferne einer Information zu einer Person verschoben, und das läuft letztlich darauf hinaus, dass die Unbestimmtheit des Datenbegriffs in eine unbestimmte Vorstellung des Merkmals des Personenbezugs transformiert wird (vgl. auch § 3 Abs. 9 BDSG), die dann ihrerseits nur durch die Unterscheidung von Persönlichem und Nicht-Persönlichem, d.h. nur durch die Unterscheidung von Privatem und Öffentlichem näher bestimmt werden kann.

Hier setzt auch die neuere Rechtsprechung des Bundesverfassungsgerichts ein. Um eine grenzenlose Ausweitung des Recht auf „informationelle Selbst-

58 Deshalb ist es auch nicht richtig, wenn der Ausgangspunkt für das Persönlichkeitsrecht in Hegels (und daran anschließende) Überlegungen zur „Anerkennung" durch wechselseitige Selbst- und Fremdbeobachtung gesucht wird. So z.B. bei *U. F. H. Rühl*, Das allgemeine Persönlichkeitsrecht – Versuch einer Annäherung an seine Strukturen und Prinzipien, in: Albers/ Heine/ Seyfarth (Hrsg.), Beobachten-Entscheiden-Gestalten, 2000, S. 79 ff., 87.

59 Zum Informationsbegriff vgl. *M. Albers*, Information als neue Dimension des Rechts, Rechtstheorie 33 (2002), 1 ff.; vgl. auch *T. Vesting*, Zur Entwicklung einer Informationsordnung, FS 50 Jahre Bundesverfassungsgericht, 2001, S. 219 ff., 225.

60 So bei *U. Dammann*, Kommentierung zu § 3 BDSG, in: Simitis (Fn. 12), Rn. 5. Eine Eingrenzung des Datenbegriffs erfolgt hier ausschließlich über die Merkmale „Vermittlung" und „Aufbewahrung".

bestimmung“ (bzw. Selbstdarstellung) zu vermeiden, hat das Bundesverfassungsgericht nach dem Volkszählungsurteil versucht, diese Grundrechte über eine an der Privat/Öffentlich-Unterscheidung orientierte Sphärentheorie einzugrenzen und dabei auch zu Recht einige missverständliche Formulierungen des Volkszählungsurteils korrigiert.[61] Ohne hier auf Einzelheiten eingehen zu können, kann man doch die These wagen, dass auch die neuere Rechtsprechung des Bundesverfassungsgerichts nur wenig zur Lösung der Unbestimmtheitsprobleme des Datenschutzrechts beiträgt: Die Staatszentrierung des Rechts auf „informationelle Selbstbestimmung“ wird lediglich in eine staatszentrierte Unterscheidung von Privatem und Öffentlichem verschoben.[62] Es wird aber nicht berücksichtigt, dass der Gegenstand des Grundrechts auf „informationelle Selbstbestimmung“ nur noch sehr bedingt über den Personenbezug und eine daran anknüpfende Sphärentheorie konturiert werden kann. Durch diese Verschiebung wird die gesamte Begründungslast auf die Möglichkeit einer Grenzziehung zwischen einer vom Individuum kontrollierten (selbstbestimmten) Zirkulation von Informationen einerseits und einer allgemein zugänglichen öffentlichen Sphäre andererseits verlagert. Die öffentlich/privat Unterscheidung wird aber gerade durch die oben näher beschriebene elektronische Eigenaufrüstung der Gesellschaft unter Druck gesetzt. Die neuen Typen von Kundenbindungssystemen, Kreditkarten, Kundenkarten und die neuen Formen der kundenbezogenen Individualisierung und Personalisierung von Produkten und Dienstleistungen mit Hilfe eines Internet basierten Direktmarketings sind nur einige Beispiele dafür, wie sehr die gesellschaftlichen Voraussetzungen der Unterscheidung von Öffentlichkeit und Privatsphäre durch die elektronischen Medien selbst unter Druck geraten.

In welchem Maße sich die auch in den neueren Urteilen des Bundesverfassungsgerichts mehr oder weniger vorausgesetzte Schärfe der Unterscheidung zwischen Privatem und Öffentlichem inzwischen abgeschliffen hat, wird schließlich auch durch den Aufstieg einer neuartigen Aufmerksamkeitsökonomie belegt.63 So ist die Publikation selbst intimster Informationen in der Ökonomie der Aufmerksamkeit alltäglich geworden, ja gerade Informa-

61 Vgl. insbesondere BVerfGE 101, 361, 380 ff.

62 Dazu *K.-H. Ladeur*, Schutz von Prominenz als Eigentum, ZUM 2000, 879 ff.

63 Vgl. *G. Frank*, Ökonomie der Aufmerksamkeit, 1998.

tionen aus der Intimsphäre werden hier laufend in exklusive Wirtschaftsgüter verwandelt. Dies lässt sich vor allem an der medialen Präsenz der Berühmten und Bekannten, der Prominenz, ablesen. Hier ist die geschickte Streuung von Informationen aus der Privat- und Intimsphäre Bestandteil des Tagesgeschäfts, das in der Regel durch professionell arbeitende PR-Berater strukturiert wird. Die Affäre mit einem Star wie Dieter Bohlen oder Boris Becker wird gerade wegen der dabei anfallenden Informationen aus der Intimsphäre zu einer wertvollen Nachricht. Sie trifft offensichtlich eine vorhandene Nachfrage und ermöglicht es Presse und Fernsehen u. a. mit der Doppeldeutigkeit von intimen Informationen zu spielen und selbst schlichten Ereignissen immer wieder neue Nuancen abgewinnen zu können („Sie ist intelligent, kann fließend französisch"). Damit werden die betroffenen Personen regelmäßig Gegenstand eines die Grenze zwischen Öffentlichkeit und Privatsphäre aufhebenden Medieninteresses, und auch diese Entwicklung zeigt, dass entgegen einer in der datenschutzrechtlichen Literatur weit verbreiteten Meinung die Grenze zwischen Privatem und Öffentlichem selbst unscharf geworden ist. Das bedeutet, dass sich die Unterscheidung öffentlich/privat, die hinter der Sphärentheorie steht, allenfalls noch auf einer abgeleiteten, sekundären Ebene für eine rechtliche Ordnungsbildung benutzen lässt.

III. Das Internet als Kommunikationssystem?

Aufgrund dieser hier nur skizzierten Entwicklungen bleibt im Ergebnis unklar, wie der Datenbegriff über die Sinnverschiebung zur Privat/Öffentlich-Unterscheidung nähere Konturen gewinnen und sich insbesondere vom Informationsbegriff unterscheiden soll. Aber gerade wenn man beide Begriffe synonym verwendet, wie es auch in der verfassungsrechtlichen Vorstellung der „informationellen Selbstbestimmung" zum Ausdruck kommt, zeigt sich das ganze Dilemma eines auf das Internet erweiterten Datenschutzes: Löst man den Zweck des Datenschutzes aus einer gegen den Staat gerichteten Funktion und überträgt seine personenbezogenen Grundsätze auf das Internet, ohne dessen Funktionsweise selbst näher zu beschreiben, erhält man ein weitgehend konturenloses Datenschutzrecht. Da Information ein elementarer Bestandteil der operativen Produktion und Reproduktion sozialer Kommunikation ist, schützt das Datenschutzrecht potentiell die gesamte Internetkommunikation, sofern in der Kommunikation nur Informationen mit Personenbezug im Sinne des § 3 Abs. 1 BDSG und den entsprechenden bereichsspezi-

fischen Normen transportiert werden (§ 1 Abs. 2 TDSG, § 12 Abs. 1 MDStV, § 47 Abs. 1 RStV).

Damit ist eine Unterscheidung von Datenschutzrecht und Kommunikationsschutzrecht nicht mehr möglich. Da der Bezug auf eine Person in der *sozialen* Kommunikation immer gegeben ist, ist der Personenbezug sogar ein notwendiger Bestandteil sozialer Kommunikation. Kommunikation setzt voraus, dass das, was mitgeteilt wird, vom Empfänger auf eine Mitteilungsabsicht zurückgeführt werden kann. Die Abgrenzung des Kommunikationsbegriffs von einem bloßen Behaviorismus, d.h. die Akzentuierung des Willensmoment innerhalb einer Kommunikationsbeziehung, ist vor allem ein essentielles Element des Kommunikationsbegriffs liberaler Rechtsordnungen, wie etwa die §§ 119 ff. BGB zeigen: Erst das Moment der absichtsvollen Erklärung ermöglicht die Zurechnung einer Äußerung auf eine Person, andernfalls liegen „Willensmängel" vor. Die Willenserklärung ist also ein Paradebeispiel für das Recht auf „informationelle Selbstbestimmung": Bestellt jemand bei amazon.com immer wieder einen bestimmten Typus von Büchern, und wird dieses Bestellverhalten vom Internetanbieter registriert, ist die Bestellung zugleich die Willenserklärung wie der datenschutzrechtlich relevante Vorgang. Das aber heißt nichts anderes, als dass das Recht auf „informationelle Selbstbestimmung" ungefähr mit dem Zivilrecht deckungsgleich ist – und so wird es im Datenschutzrecht von vielen auch gesehen. Diese Unbestimmtheit des Datenschutzrechts konnte früher nur deshalb übertüncht werden, weil das, was für ein datenschutzrechtlich relevantes Datum gehalten wurde, einerseits durch die technologische Struktur staatlich betriebener Datenverarbeitungsanlagen und andererseits durch die staatlichen Erhebungszwecke zumindest ein Stück weit vorstrukturiert war.

Wie wenig sinnvoll die Übertragung des personenbezogenen Datenschutzrechts auf das Internet ist, zeigt sich auch darin, dass mit der Verbreitung des Internets ganz neue Fragestellungen einhergehen. In ihrer Mehrzahl haben diese Fragen keinen allgemein persönlichkeitsbezogenen Charakter, sondern sind informationsökonomischer Natur. Das lässt sich relativ einfach veranschaulichen: So verändern beispielsweise Internet-Tauschbörsen die Zugangsmöglichkeiten zu ökonomisch wertvollen Informationen, und dadurch werden nicht persönlichkeitsrechtliche, sondern neue eigentumsrechtliche

und urheberrechtliche Fragestellungen des Schutzes von Informationen gegenüber vertraglich nicht genehmigten Drittnutzungen aufgeworfen. Indem das Internet Transaktionskosten senkt, verändert es außerdem etablierte Produktionsstrukturen in vielen wirtschaftlichen Bereichen. Das Internet ermöglicht u. a. neuartige peer-to-peer Produktionen z.B. im Bereich der opensource Software, eine Entwicklung, die von manchen Internettheoretikern und Rechtswissenschaftlern als die eigentliche Neuerung des Internets angesehen wird.[64] Auch hier geht es nicht um personenbezogene Daten, sondern darum, dass das im herkömmlichen Eigentums- und Patentrecht angelegte und auf stabile Personen und Organisationen zugeschnittene Moment des Schutzes von „Erfindungen" und „Betriebsgeheimnissen", also von Informationen, neu überdacht werden muss.[65] In ganz anderer Weise wirft die Präsenz der Bundesregierung im Internet Fragen nach der Zulässigkeit neuer Formen der Regierungskommunikation auf.[66] Auch im Fall der Regierungskommunikation stellt sich aber keine persönlichkeitsrechtliche Frage, sondern das Problem, in welchem Maße der Staat das Internet als Medium der Informationspolitik benutzen darf und inwiefern und inwieweit Dritte vor der staatlichen Erzeugung und Verbreitung solcher Informationen rechtlich geschützt werden müssen.

Eine Eingrenzung des Gegenstandsbereichs des Datenschutzrechts lässt sich also auch nicht durch den Rekurs auf das Internet als „Kommunikationssystem" erreichen. Die eben erwähnten Beispiele zeigen vielmehr, dass das Internet offensichtlich in viele unterschiedliche, wirtschaftliche und politische Kommunikationsräume eindringt und laufend die Grenzen etablierter Kommunikationsräume, z.B. die Grenze von legaler und illegaler Informationsökonomie überschreitet. Das hat auch Folgen für die rechtliche Ordnungsbildung. In der juristischen Literatur wird das Internet oft als abgrenzbarer „Cyberspace", als nicht mehr auf territorialen Grenzen beruhender raumloser Kommunikationsraum jenseits der Nationalstaaten beschrieben. An diese Raumvorstellung wird dann regelmäßig die Notwendigkeit der Etablierung

64 Vgl. nur *Y. Benkler*, Coase's Pinguin, or, Linux and the Nature of the Form, 112 Yale Law Journal, im Erscheinen Winter 02/03.

65 *L. Lessig*, The Future of Ideas, New York 2001, S. 250 ff.; *T. Vesting*, Common Knowledge in the "Information Age", RCS Discussion papers, Florence 2001.

66 *K.-H. Ladeur*, Verfassungsrechtliche Fragen regierungsamtlicher Öffentlichkeitsarbeit und öffentlicher Wirtschaftstätigkeit im Internet, DÖV 2002, 1 ff.

eines neuen Rechtsgebietes, eines neuartigen „Cyberlaw“ oder „Internetrechts“, geknüpft, dem dann auch bestimmte datenschutzrechtliche Fragen zugeordnet werden.[67] Wer so ansetzt, übersieht jedoch, dass das Internet kein Kommunikations*system,* d.h. keine Form mit klaren Grenzen ist[68], sondern ein netzwerkförmiges, konnexionistisches Medium des Kommunizierens, das für unterschiedlichste Kommunikationsprozesse, von der dezentralen Produktion von Software, über das illegale Kopieren beliebiger Inhalte bis hin zur Regierungskommunikation genutzt werden kann.

G. Überlegungen zu einem alternativen datenschutzrechtlichen Ordnungsmodell

I. Der Computer als technisches Kommunikationsmedium

Das Internet basiert auf einer vollständigen Dezentralisierung seiner Elemente und Relationen, die das Netzwerk des Internets laufend neu zu einer „Einheit“ verweben, die im Moment ihres Entstehens schon wieder zerfällt. Diese Dynamik eines unaufhörlich in seinen Elementen und Relationen sich verändernden Netzwerks entzieht der Vorstellung der Dominanz relativ stabiler, hierarchisch verknüpfter und staatlich betriebener Großrechenanlagen seine Grundlage. Das ist in der datenschutzrechtlichen Literatur zwar schon relativ früh angemerkt[69], in seinen Konsequenzen aber nie wirklich zu Ende gedacht worden. Das Internet ist keine verkleinerte Datenverarbeitungsanlage, sondern ein hochflexibles Netzwerk, das als Schnittstelle zwischen sich und den Menschen den Computer setzt, ein neuartiges Kommunikationsmedium, das neben die bisherigen Kommunikationsmedien, Sprache, Schrift, Buchdruck und elektronische Medien, tritt. Der Computer verlängert die Sequenz der Kommunikationsmedien aber nicht nur um ein weiteres technisches Medium, er ist selbst ein andere Medien integrierendes Kommunikationsmedium, ein

67 Vgl. nur *Hoeren* (Fn. 1), S. 233 ff, *Boehme-Neßler* (Fn. 1), S. 283 ff.; im amerikanischen Schrifttum ähnlich z.B. *Lessig* (Fn. 1), S. 142 ff.

68 *Weber* (Fn. 42), S. 47 ff.; *D. Baecker*, Networking the Web, in: Ch. Engel/ K. H. Keller (eds.), Understanding the Impact of Global Networks and Local Social, Political and Cultural Values, 2000, S. 93 ff.

69 Dazu etwa *H. P. Bull*, Vom Datenschutz zum Informationsrecht, in: Hohmann (Fn. 7), S. 173 ff., 179 f.

Medium zweiter Ordnung, das quer laufende, schräge und überraschende Verbindungen zwischen früher getrennten Medien erzeugt. Das hängt vor allem damit zusammen, dass der Computer selbst auf der Grundlage eines neuartigen Universalmediums operiert, der digitalen Code*schrift*, die „alle anderen Medien – Sprache, phonetische Schrift, Bild, Musik, Audiovisionen – zu umgreifen, zu reproduzieren und miteinander zu verflechten erlaubt“[70]; man kann die Besonderheit des Computers deshalb gerade in seinen transmedialen Eigenschaften sehen und insofern auch von einem „Transmedium“ sprechen.[71] Der Computer eröffnet neue Kommunikationsmöglichkeiten, indem er die Vielfalt der Grenzüberschreitungen und Verknüpfungsmöglichkeiten steigert. Das bedeutet negativ gesehen, dass das Internet als dem diesem „Transmedium“ entsprechenden Netzwerk zu einer Unterwanderung, Destabilisierung oder auch Auflösung tradierter Grenzen und Grenzziehungen führt.

Diese Destabilisierung von Grenzen und Grenzziehungen gilt auch für den Begriff des Kommunikationsmediums selbst. Der Computer destabilisiert vor allem das Verhältnis von sinnhafter Kommunikation und technischer Umwelt des Kommunizierens, also auch die Unterscheidbarkeit zwischen dem Internet als einem technischen Phänomen und dem Internet als medialem und sozialem Kommunikationsnetzwerk.[72] Durch den Computer wird eine spezifisch technische Form der Sinnverarbeitung, die binäre Codierung, Bestandteil eines sozialen Kommunikationsnetzwerks, das als solches auch eng mit der maschinentechnischen physikalischen Umsetzung, der Hardware, gekoppelt ist. Der Schlüssel zum Verständnis der Besonderheit des Internets liegt deshalb im Begriff des *technischen* Mediums. Dieser hybride Begriff signalisiert, dass der Medienbegriff nicht länger von der natürlichen Sprache als dem grundlegenden Kommunikationsmedium her entwickelt werden kann, wie es z. B. in der Systemtheorie Luhmanns und in der späten Medientheorie

70 *M. Sandbothe*, Pragmatische Medienphilosophie, 2001, S. 184.

71 *Sandbothe* (Fn. 70), S. 124, 152.

72 Dazu ausführlicher *T. Vesting*, The Autonomy of Law and the Formation of Network Standards, Manuskript 2001, im Erscheinen.

McLuhans der Fall ist.[73] Der Computer verschiebt die traditionelle, in der westlich-abendländischen Kultur seit Platon bestehende Hierarchie von Sprache und Schrift zugunsten eines Vorrangs der digitalen Codeschrift und der darauf beruhenden Programmiersprachen, Benutzeroberflächen, Textformate, Webdesign etc. Das hat Derrida zu Recht in der Grammatologie angemerkt.[74] Die Differenz zwischen Materialität und Sinn, zwischen Laut und Zeichen, zwischen der Physis der Schrift einerseits und der Hermeneutik von Texten andererseits wird im Computer durch eine neuartige „Logik der Vernetzung" ersetzt, die m. E. weder in einer differenztheoretischen noch in einer identitätstheoretischen Sprache hinreichend erfasst werden kann. Entgegen der Auffassung Luhmanns, der den Computer in der Tradition der mathematisch-kybernetischen Kommunikationstheorie in eine Innen- und Außenseite aufspaltet, widersetzt sich der Computer gerade dieser Aufspaltung. Auf der einen Seite ist die Software nicht einfach nur „Umwelt" sinnhaften Kommunizierens, was sich etwa darin zeigt, dass sich der Schriftcode gerade *nicht* neutral zu den dadurch kommunizierten Inhalten verhält und auch nicht nur destruktiv auf den Computer einwirken könnte wie beispielsweise ein Feuer, durch das ein Buch verbrennen, aber nicht geschrieben werden kann. Die Software kann aber auch nicht auf die Ebene des Sinns, also des Geistes im Sinne des Deutschen Idealismus abgeschoben werden. Das aber macht Luhmann, wenn er die Computersoftware mit der Grammatik der Sprache, d.h. mit Formen sinnhafter gesellschaftlicher Kommunikation assoziiert.[75] Der Computer eröffnet gegenüber dieser Differenz eine „dritte Ebene":[76] Die Codeschrift wandert als technisch vergegenständlichte Schrift selbst in den Kern des Kommunikationsmediums ein.

73 *N. Luhmann*, Die Gesellschaft der Gesellschaft, Bd. 1, 1997, S. 190 ff., 205; zu McLuhan vgl. *R. Höltschl/? F. Böhler*, Ich bin mein eigener Computer, in: McLuhan (Hrsg.), Das Medium ist die Botschaft, 2001, S. 245 ff.

74 *J. Derrida*, Grammatologie (1974), 1983, S. 17 ff., 21; zu den Konsequenzen für den Kommunikationsbegriff vgl. *S. Krämer*, Sprache, Sprechakt, Kommunikation, 2001; vgl. auch *Vismann* (Fn. 39), S. 15 ff.

75 *Luhmann* (Fn. 73), S. 310; vgl. dazu auch die interessanten Überlegungen von *F. Balke*, Dichter, Denker und Niklas Luhmann, in: Koschorke/Vismann (Hrsg.), Widerstände der Systemtheorie, 1999, S. 135 ff.

76 Das legen insbesondere die Überlegungen von *G. Günther*, Das Bewußtsein der Maschinen, 1963, S. 19 ff., nahe.

Durch diese „dialektische“ Bewegung sprengt der Computer die enge Verknüpfung von Sinnverarbeitung, sozialer Kommunikation und Bewusstsein. Während die Sprache als Kommunikationsmedium von der Stimme unterschieden werden kann, die Schrift von Papier und Schreibwerkzeug und noch das analoge Fernsehen die Unterscheidung von technologischen Materialitäten einerseits und kommunikativen Inhalten zugelassen, ja sogar die Hierarchie des Inhalts gegenüber der Technik fortgesetzt hat[77], geht das Internet aus der Vernetzung eines Mediums hervor, dem Computer, dessen Code*schrift* selbst technischen Charakter hat. Die Programmiersprachen und digitalen Codes werden damit zu Bedingungen der Möglichkeit der Internetkommunikation – und nicht zu bloßen (Umwelt-)Voraussetzungen. Die weitreichende und heute noch nicht übersehbare Folge des Computers besteht also darin, dass der Computer selbst eine neue unsichtbare Form der sinnhaften und zugleich technischen Kommunikation jenseits der Verwendungskontexte sozialer Kommunikation etabliert. Dadurch verändert sich auch der Begriff des Zeichens bzw. des Symbols. Zeichen verweisen in Computernetzwerken nicht mehr auf die Differenz von Bezeichnendem und Bezeichnetem, sondern erzeugen selbst andere Zeichen. Mit der Software löst sich die Einheit des Zeichengebrauchs auf in einen Zeichengebrauch innerhalb der wechselnden Verwendungsbedingungen sozialer Kommunikation einerseits und eine digital codierte Symbolik andererseits, die die Symbole, die für den Zeichengebrauch in der sozialen Kommunikation notwendig sind, laufend maschinell produziert und reproduziert. Die digitalisierte Information führt also fortan ein Eigenleben in der Sinn verarbeitenden Maschine des Computers. Und das ist neu. Auch in Bibliotheken können Informationen, fernab von ihren möglichen Lesern, in Büchern und Dokumenten über Jahrhunderte erhalten und bewahrt werden. Der elektronische Speicher des Computers unterscheidet sich vom mechanischen Speicher des Buchs aber dadurch, dass er erst durch die digitale Codeschrift lesbar wird, also erst durch die Zwischenschaltung eines binären Sinn verarbeitenden und laufend binären Sinn transformierenden Computers.

77 Vgl. nur BVerfGE 12, 205, 227; 46, 120, 151, 155.

II. Vom Persönlichkeitsschutz zum technischen Designschutz

Die medientheoretischen Implikationen der voran stehenden Überlegungen können hier nicht weiter vertieft werden.[78] Überträgt man die gewonnenen Ergebnisse in den hier behandelten Kontext, könnte ein wichtiges Ergebnis für die datenschutzrechtliche Ordnungsbildung darin bestehen, den Datenbegriff über das Kriterium der Verkörperung von sinnhaften Informationen in digitalen Codes zu konturieren.[79] Der Datenschutz wäre dann nicht länger als primär personenbezogener Datenschutz zu konzipieren, sondern wäre seiner humanistischen Ableitungen zu entkleiden und in einen primär Software bezogenen Datenschutz umzubauen. Für den hier untersuchten Bereich der Internetkommunikation in Netzwerken privater Unternehmen und Nutzer wäre der Akzent auf die technischen Voraussetzungen der Internetkommunikation und erst sekundär auf die Informationsebene, die Ebene der sozialen Kommunikation, zu legen. Weil Daten Informationen sind, die sich im Medium der digitalen Codeschrift vergegenständlichen und dadurch zu maschinell mitlaufenden Komponenten der Internetkommunikation werden, käme es in einem alternativen datenschutzrechtlichen Ordnungsmodell darauf an, dieser technischen Anreicherung der Kommunikation zu folgen. Damit ist nicht nur der unsichtbare Code gemeint, den Computer verwenden, um sich selbst für sprechende, lesende und sehende Menschen verständlich zu machen, sondern auch und vor allem die Gestaltung der Standards, der Programmiersprachen sowie die Ebene der Sichtbarkeit, die Benutzeroberflächen (Webdesign) und

78 Der hybride Begriff des technischen Mediums läuft nicht auf den Ausschluss von Bewusstsein hinaus, aber umgekehrt kann die Destabilisierung der Unterscheidung von sinnhaften und materiellen Komponenten des Medienbegriffs auch nicht mehr als Ausnahmefall im System einer von der natürlichen Sprache abgeleiteten Kommunikationsbegriffs dargestellt – und durch ein Ergänzungskonzept wie „strukturelle Kopplung“ bewältigt werden. Eine höhere Flexibilität im Kommunikationsbegriff erscheint aufgrund der zunehmenden Bedeutung maschineller Zeichenverarbeitung sinnvoll zu sein.

79 Einen Vorschlag in diese Richtung macht *M. Albers*, Information als neue Dimension des Rechts, Rechtstheorie 33 (2002), 61 ff., 62, 68, 74, 84 f.; in den USA wird diese Richtung am konsequentesten von Joel Reidenberg vertreten; vgl. *Reidenberg*, Lex Informatica (Fn. 1), 553 ff.; *ders.*, Privacy Protection and the Interdependence of Law, Technology and Self-Regulation, 1999, http://reidenberg.home.sprynet.com/Publications. htm; *ders.*, The Movement toward Obligatory Standards for Fair Information Practices in the United States, http://reidenberg.home.sprynet.com/ Publications.htm.

sonstigen Schnittstellen, die die Verbindung zwischen dem weltumspannenden elektronischen Kommunikationsnetzwerk des Internets und den Nutzern herstellen. Wenn, wie oben thesenartig behauptet wurde, die Neuheit des Internets darin besteht, Begriffe wie Kommunikationsmedium und technisches Medium tendenziell ununterscheidbar zu machen, dann ist es nur folgerichtig, wenn der Datenschutz zu einem technischen Designschutz umgebaut wird.

Die Aufgabe des Datenschutzrechts würde sich dann auf die Beobachtung und ggf. Beeinflussung der Konfiguration der technischen Systeme verschieben. Seine Funktion wäre nicht länger die Verhinderung von Missbrauch, sondern die Erzeugung von Vertrauen in die Internetkommunikation und die dabei verwendete Medientechnologie. Das ist, wie oben schon festgestellt wurde, durchaus eine Tendenz in der datenschutzrechtlichen Literatur und der politische Datenschutzgesetzgebung[80], die dort unter Begriffen wie „Systemdatenschutz“ und „Selbstdatenschutz“ läuft. An manche Vorstellungen des „Systemdatenschutzes“ bzw. „Selbstdatenschutzes“ kann man in Zukunft durchaus anknüpfen, aber das Grundproblem dieser Überlegungen und vor allem ihrer gesetzlichen Umsetzungen besteht darin, dass das herkömmliche staatszentrierte Leitbild des Datenschutzrechts im Konzept des „Systemdatenschutzes“ bzw. „Selbstdatenschutzes“ erhalten bleibt, während der medienorientierte, technische Designschutz auf ein Ergänzungskonzept reduziert wird. Diese Strategie vermag auch deshalb nicht zu überzeugen, weil innerhalb des Ergänzungskonzepts des „Systemdatenschutzes“ bzw. „Selbstdatenschutzes“ primär mit Zweckprogrammen gearbeitet wird. So schreibt beispielsweise das TDDSG Daten erhebenden Internetunternehmen vor, mit Daten sparsam umzugehen, ohne sich näher mit den unternehmensinternen Implementationsbedingungen dieser Zweckprogramme zu beschäftigen. Mit dieser Teiltransformation des Datenschutzrechts zu einer symbolischen Rechtsmasse steht der Datenschutz natürlich nicht allein da, man denke nur an die Regulierung des Fernsehens.[81] Aber der Rückzug des Staates auf die Ebene des symbolischen Handelns ist kein Argument für die herkömmliche

80 Vgl. nur *Boehme-Neßler* (Fn. 1), S. 293; *Hoffmann-Riem* (Fn. 10), S. 513 ff., 534 ff.

81 Vgl. nur *T. Vesting,* Das Rundfunkrecht vor den Herausforderungen der Logik der Vernetzung, Medien & Kommunikationswissenschaft 49 (2001), S. 287 ff.

Form einer Datenschutzregulierung, die ihre Bindungseffekte, wenn überhaupt, nur noch durch mediales Rauschen erreicht, in der Medienberichte über „Datenschutzverstöße“ zum (mittelbaren) Substitut (unmittelbarer) gesetzlicher Bindungen werden.

Es muss also darum gehen, den Datenschutz an die technologischen Bedingungen des Computers und des Internets anzupassen. Deshalb muss die Regelungstechnik des Verbots mit Erlaubnisvorbehalt im internetbezogenen Datenschutzrecht aufgegeben werden. Diese Regelungstechnik widerspricht der dezentralen, nachbarschaftlichen Struktur des Internets, das aus einem Netzwerk verteilter Elemente und variierender Relationen produziert und reproduziert wird. Diese konnexionistische Struktur entspricht eher der Struktur privatautonomer Entscheidungsrechte, und darauf muss die öffentlich-rechtliche Regulierung eingestellt werden. So macht etwa das BGB die Möglichkeit zum Vertragsschluss nicht von einer gesetzlich vorgeschriebenen Einwilligung der Parteien in den Vertragsschluss abhängig, sondern schreibt gesetzlich eine *Form* vor, die autonome Willenserklärung, deren Produktivität im BGB vorausgesetzt wird. Nur wenn man diese Vermutung zugunsten der Produktivität einer konsensentlasteten Entscheidung aufgibt und umgekehrt davon ausgeht, dass die ökonomische Nutzung und Verwertung personenbezogener Daten aufgrund ihrer „Gefährlichkeit“ und „Bedrohlichkeit“ eigentlich verhindert werden muss, macht die datenschutzrechtliche Regelungstechnik des Verbots mit Erlaubnisvorbehalt überhaupt Sinn. Die Gleichsetzung einer vertraglichen Einwilligung in den Gebrauch personenbezogener Daten mit einer staatlich-gesetzlichen eingeräumten Verwendungserlaubnis negiert das in der Dezentralität enthaltene Produktivität auf kollektiver Ebene, die Generierung des Neuen, zugunsten einer in ihrer Produktivität selbst nicht weiter hinterfragten staatlichen Datenschutzfürsorge.

An die Stelle des staatlichen Verbots mit Erlaubnisvorbehalt und einer daran anknüpfenden Detailgesetzgebung hätte deshalb eine neue Datenschutzgesetzgebung für die Internetkommunikation zu treten. Es müssen also auch die gesetzlichen Formen und Instrumente der Datenschutzregulierung verändert werden. Dabei käme es angesichts der hohen Ungewissheit der Entwicklung des Internets vor allem darauf an, die Gesetzgebung radikal zu vereinfachen und auf wenige abstrakte Meta-Regeln zu beschränken. Kern dieser

alternativen Regulierungsstrategie hätte die Meta-Regel zu sein, für Internetnutzer Schnittstellenbedingungen zu schaffen, die es diesen ermöglichen, die Zirkulation von für sie empfindlichen Informationen aus der Privatsphäre so weit wie möglich selbst zu steuern und zu verantworten. Das liefe zunächst auf eine weitgehende „Deregulierung" des Datenschutzrechts im Internet hinaus. Angesichts der oben geschilderten elektronischen Eigenaufrüstung der Gesellschaft und der Instabilität der Unterscheidung von Privatsphäre und Öffentlichkeit müsste der politische Gesetzgeber sogar darauf verzichten, die in der Internetkommunikation sich jeweils situativ einstellende und von Person zu Person unterschiedliche Empfindsamkeit gegenüber der Weitergabe privater Daten abstrakt in einem materiellen Standard vorzugeben. Das hier vorgeschlagene Ordnungsmodell steht aber nicht einfach für eine „Rückkehr zum Markt". Es insistiert darauf, durch staatliche (und suprastaatliche) Regelungen technologische Bedingungen zu ermöglichen, in denen sich Konventionen des Privatsphärenschutzes in einem Netzwerk verteilter Entscheidungsrechte bilden und die Unterscheidung des Öffentlichen und Privaten sich im neuen Kommunikationsmedium des Computers restabilisieren kann. Im Fall der Cookies wäre es beispielsweise vorstellbar, gesetzliche Anforderungen zur Einstellung des Browsers zu formulieren. Die u. a. in § 12 Abs. 8 MDStV und § 5 TDDSG verankerte Regelung einer von der Schriftform des § 3 BDSG abweichenden neuartigen Form der elektronischen Einwilligung wäre also aufzunehmen. Sie müsste dann aber auch konsequent aus der Verankerung der Schriftkultur gelöst und vollständig den Funktionsbedingungen des neuen Kommunikationsmediums angepasst werden.[82] Die Regelung müsste also stärker auf die Gestaltung der Benutzeroberfläche zielen und darüber eine nutzerabhängige Steuerung des Einsatzes von Cookies möglich machen.

Auch bei einem technischen Designschutz ginge es letztlich um die pragmatischen Verwendungsmöglichkeiten des Computers und des Internets. Die Regulierungsstrategie, die hier vorgeschlagen wird, würde aber primär an die Strukturen der Hard- und Software anknüpfen, die jeder pragmatischen Verwendung vorgegeben sind. Daraus folgt auch, dass die bereichsspezifische Ausdifferenzierung des internetbezogenen Datenschutzrechts, die Unter-

82 Das Gegenteil vertritt z. B. *Ihde* (Fn. 51), S. 413 ff., 419, der am „Willensbegriff" festhalten will.

scheidung nach unterschiedlichen Diensten, insbesondere nach dem Charakter als Telekommunikation (§§ 85 ff. TKG), Rundfunk (§§ 47a ff. RStV), Mediendienst (§§ 12 ff. MDStV) und Teledienst (TDDSG), aufgegeben werden muss. Gerade weil das Internet ein „Transmedium" ist, das die Vielfalt der Verknüpfungsmöglichkeiten steigert bzw. negativ gesehen, zu einer Unterwanderung, Destabilisierung oder auch Auflösung tradierter Grenzen und Grenzziehungen führt, ist es wahrscheinlich, dass das Internet die zentralen Anknüpfungspunkte der dienstepezifischen Regulierung des Datenschutzes destabilisieren wird. Der Sinn dieser Bereichsdifferenzierung im Datenschutzrecht ist ohnehin relativ[83]: Die bereichsspezifischen Regelungen zum Datenschutz werden durch z. T. fragwürdige gesetzliche Typisierungen von Diensten erkauft, deren Halbwertzeit angesichts des schnellen technologischen Wandels äußerst kurz ist. Überdies wird die Handhabbarkeit dieses Mehrbereichsmodells noch dadurch verkompliziert, dass die Datenschutzbeauftragen in ihrer Praxis ein Schichtenmodell zu Grunde legen[84], dessen Kapazität zur Diskriminierung angesichts des hybriden Charakters vieler Internetdienste eher als bescheiden eingestuft werden muss. Für die betroffenen Unternehmen und Nutzer wirft diese Regelungstechnik schließlich überhaupt keine Vorteile ab.

Mit diesen Überlegungen ist keine Integration der datenschutzspezifischen Regelungen, die die Internetkommunikation betreffen, in das BDSG verbunden. Ob die wenigen Meta-Regeln, die gesetzlich normiert werden könnten, in einem besonderen Gesetz zusammengefasst oder als Sondervorschriften in einem besonderen Teil des BDSG integriert werden, ist eine eher gesetzestechnische Frage, die sich prinzipiell in beide Richtungen auflösen lässt. Entscheidend ist nur, dass es zu einer Deregulierung des Datenschutzrechts im Fall der Internetkommunikation zwischen Privaten kommt. Außerdem geht mit den voran stehenden Überlegungen keine kompetenzrechtliche Vorentscheidung zugunsten einer datenschutzrechtlichen Regelungsbefugnis des Bundes einher. Angesichts der Bedeutungszunahme der technologischen Bedingungen der Internetkommunikation und der wachsenden wirtschaftlichen Bedeutung derselben spricht allerdings viel dafür, dass die Kompetenz für ei-

83 Kritisch dazu etwa *W. Hoffmann-Riem* (Fn. 10), S. 513 ff.

84 Vgl. *P. Schaar*, Neues Datenschutzrecht für das Internet, RDV 2002, S. 4 ff., 6.

ne einheitliche Internetdatenschutzgesetzgebung beim Bund und nicht bei den Ländern liegt.

III. Staatliche Beobachtung transnationaler Konventionsbildung

Wenn das Datenschutzrecht primär auf die technische Seite der Internetkommunikation verlagert wird, müssen auch die neuartigen Formen der transnationalen Bildung von technischen Netzwerkstandards einer genaueren Beobachtung durch staatliche oder supranationale politische Organisationen unterstellt werden.[85] So haben sich auch im Bereich des Datenschutzes Formen der Selbstregulierung wie etwa der „Platform for Privacy Preferences" (P3P) innerhalb des „World Wide Web Consortium" (W3C) etabliert. P3P hat z.B. einen gemeinsamen Standard zum Schutz der Privatsphäre erarbeitet, auf den auch der neue Internet Explorer 6.0 von Microsoft eingestellt ist. Der Explorer blockiert Cookies von Unternehmen, die das technische Protokoll, das P3P erarbeitet hat, nicht akzeptieren. Diese und andere Formen der Netiquette im Bereich des Privatsphärenschutzes müssen künftig als autonome transnationale Regeln von der nationalen Datenschutzgesetzgebung zur Kenntnis genommen werden. Das schließt nicht aus, dass Staaten oder supranationale Organisationen wie die EG diese Konventionsbildung auf einer sekundären Ebene produktiv zu modellieren versuchen. Im Fall der Cookies könnte man sich etwa vorstellen, dass staatliche oder suprastaatliche Organisationen zu einer Optimierung solcher Selbstverpflichtungen beitragen.[86]

Neben die Pflicht zur Beobachtung der Selbstorganisation im Bereich technischer Netzwerkstandards wäre auch eine staatliche Pflicht zur Beobachtung der Entwicklung der Vertragsformen denkbar, über die der Datenaustausch zwischen Nutzern und Unternehmen geregelt werden. Es ist allerdings sehr

85 Dazu allg. *Reidenberg*, Lex Informatica (Fn. 1), S. 553 ff.; *Vesting* (Fn. 72); vgl. auch *S. Delfs*, Innovation – Standardisierung – Recht (Das Beispiel Internet), in: Eifert/Hoffmann-Riem (Fn. 2), S. 171 ff., 199 ff.; und *P. Mayer*, Das Internet im öffentlichen Recht, 1999, S. 58 ff., 239 ff. Darin bewahrheitet sich die These von Hase (oben Fn. 12), „dass sich das Recht nicht mehr umstandslos im Gesetz zentrieren läßt."

86 Vgl. dazu die Überlegungen bei *Reidenberg* (Fn. 79), Privacy Protection und The Movement.

fraglich, ob dies Gegenstand eines besonderen öffentlich-rechtlichen Datenschutzrechts sein sollte. Zwar hat das gemeinsame Interesse aller Beteiligten an Formen des Direktmarketings einen anderen kollektiven Effekt als in der Offline-Welt: Während beispielsweise Kundenprofile in der Welt des realen Buchhandels zwischen vielen Buchhändlern lokal zerstreut existieren, kann ein Internet-Unternehmen wie amazon.com aufgrund seiner raumunabhängigen, weltweiten Präsenz in einem sehr viel umfangreicheren Maße Nutzer- und Kundenprofile anlegen, die ab einer bestimmten Komplexität selbst einen erheblichen ökonomischen Wert darstellen. Das gilt insbesondere dann, wenn, wie so oft in der Internet-Ökonomie, langfristig nur ein Unternehmen erfolgreich ist und im Zuge seiner Expansion seine Produktpalette erweitert und Verknüpfungen zu andere Medien und daran angrenzenden Produkten aufbauen kann, von Büchern beispielsweise zu CD' s, DVD' s und Videos. Es ist dennoch äußerst fraglich, ob die von Internetunternehmen verwendeten Vertragsformen und allgemeinen Geschäftsbedingungen einer unstrukturierten Überprüfung durch Datenschutzbehörden ausgesetzt werden sollten. Sofern man die Entwicklung adäquater Vertragsformen nicht ganz dem Privatrecht und seinen Beobachtungsinstanzen überlässt (Zivilgerichte, Privatrechtswissenschaft etc.), müsste der Datenschutz sich aber auch hier von der Vorstellung des Eingriffsabwehrschutzes lösen und erst einmal beobachten, inwiefern die Interessen des Nutzers gegenüber den Interessen der Daten verarbeitenden Unternehmen in der Praxis zu kurz kommen. Es wären also beispielsweise gesetzliche Voraussetzungen notwendig, die dafür sorgen, dass sich Interventionen staatlicher Datenschutzbehörden in Formen des Data-Mining auf Fälle evidenter Fehlentwicklungen beschränken.

IV. Folgen für den staatszentrierten Datenschutz

Die hier vorgestellten Überlegungen gelten für den Bereich der Datenerhebung und Datenaggregation zwischen Privaten mit Hilfe des Internets. Sie setzen also mit dem Gedanken ein, dass die im BDSG vorgenommene Gleichsetzung zwischen öffentlichen und nicht-öffentlichen Stellen, die die Grundlage der Übertragung des herkömmlichen Datenschutzes in eine bereichspezifische Datenschutzregulierung für elektronische Medien (TKG, TDDSG, MDStV etc.) bildet, aufgegeben, jedenfalls aber stark relativiert werden muss. Wie der Datenschutz gegenüber staatlichen Stellen künftig zu regulieren wäre, ist nicht Gegenstand dieses Beitrags, aber es soll noch kurz darauf hingewiesen werden, dass die elektronische Speicherung großer Da-

tenbestände in Wirtschaftsunternehmen neuartige Fragen des Schutzes dieser Datenbestände gegenüber einer unbefugten Weitergabe an Dritte aufwirft. Zu diesen Dritten dürfte in Zukunft auch der Staat selbst gehören. So ist etwa nach den Terroranschlägen vom 11. September 2001 ein verstärktes Interesse an den Verbindungsdaten von Mobilfunkunternehmen entstanden, und zur Zeit plant die EG eine Verschärfung der Möglichkeiten polizeilicher Behörden, sich in bestimmten Fällen Verbindungsinformationen von Festnetz- und Mobilfunkanbietern zu holen. Hier mögen die traditionellen Vorstellungen der Zweckentfremdung von Daten für staatliche Kontrollzwecke durchaus ihre Gültigkeit behalten, ja angesichts der (oben beschriebenen) elektronischen Eigenaufrüstung der Gesellschaft könnte hier das eigentliche datenschutzrechtliche Problem der Zukunft liegen.

H. Zur verfassungsrechtlichen Verankerung des Datenschutzes in Art. 14 GG

In der Internetkommunikation und insbesondere im Bereich der hier untersuchten neuartigen Erscheinungen des E-Commerce, der Erstellung von Nutzerprofilen, des Data-Mining und des Einsatzes von Cookies, sind Fragen des Datenschutzes solche, die primär einen ökonomischen Charakter haben. Personenbezogene Informationen werden in der Internetkommunikation selbst Bestandteil wirtschaftlicher Wertschöpfungsketten, und deshalb kann diese Entwicklung nur noch schwerlich einem personenbezogenen Datenschutzrecht im Sinne des herkömmlichen Leitbildes unterstellt werden – zumal der Personenbezug in diesem Leitbild auf eine allgemein menschenrechtlich-persönlichkeitsrechtliche Komponente (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) und ein daraus abgeleitetes Recht auf „informationelle Selbstbestimmung“ zurückgeführt wird. Der Begriff des Personenbezugs bleibt in diesem Leitbild ähnlich allgemein wie sein Gegenpart, das „demokratische Gemeinwesen“, während es in Wirklichkeit um einen ganz bestimmten Typus von Kommunikation geht, nämlich um wirtschaftliche Kommunikation oder doch um die Zirkulation kommunikativer Inhalte, die eine Nähe zu wirtschaftlichen Handlungen aufweisen. Das muss dann auch im Verfassungsrecht adäquat abgebildet werden. Der Ansatz des Bundesdatenschutzgesetzes, „den einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird“ (§ 1 Abs. 1 BDSG), der auch für die dienste- und bereichsspezifische Regulierung gilt,

muss daher für die (hier untersuchten Bereiche der) Internetkommunikation aufgegeben werden. Ein umfassendes menschenrechtlich-persönlichkeitsrechtlich verankertes Grundrecht auf „informationelle Selbstbestimmung" kann es in der „Informationsgesellschaft" nicht geben.[87] Das Recht auf Datenschutz ist ein verteiltes Entscheidungsrecht, und wenn dieses Entscheidungsrecht in wirtschaftlichen Kommunikationen benutzt wird, dann muss der Datenschutz auch rechtlich den entsprechenden Grundrechtskontexten zugeordnet werden. Der internetbezogene Datenschutz gehört also primär in den wirtschaftlichen Kontext der Eigentums- und Berufsfreiheit, nicht aber in den menschenrechtlich-demokratietheoretischen Kontext des allgemeinen Persönlichkeitsrechts, das hier allenfalls sekundär, als Auffangrecht für wenige Fallkonstellationen, zur Geltung kommen kann.[88]

Auch ein Datenschutzrecht, das primär als technischer Designschutz ausgestaltet wäre, kann an die Wirtschaftsgrundrechte des Grundgesetzes anknüpfen. Das hier vorgestellte Ordnungsmodell zielt zwar in seinen regulierungstheoretischen Konsequenzen primär auf die rechtliche Strukturierung der Computersoftware, des Codes, der Standards, der Benutzeroberflächen etc., das schließt aber nicht aus, dass dieses Ordnungsmodell eine verfassungsrechtliche Verankerung in Grundrechten findet. Dieses, auf den ersten Blick möglicherweise überraschende Ergebnis wird plausibel, wenn man in Rechnung stellt, dass das öffentliche Interesse, um das es in dem hier skizzierten datenschutzrechtlichen Ordnungsmodell geht, nicht mehr dem Leitbild der persönlichkeitszentrierten Missbrauchsabwehr folgt, sondern einen Beitrag zur Erzeugung von Vertrauen in das technische Kommunikationsnetzwerk des Internets und damit verknüpfte Formen der (wirtschaftlichen) Kommunikation leisten will. Damit bleibt die Kontinuität zur liberalen Rechtstruktur gewahrt. Die Funktion des liberalen Rechts ist es seit jeher, die Bildung und Stabilisierung von Regeln und Ordnungsmustern abzustützen und damit

87 Dazu auch Albers, (Fn. 59), S. 78 ff., 81.

88 Deshalb ist auch den Stimmen in der US-amerikanischen Literatur nicht zu folgen, die das „europäische Modell" der „Demokratie" und „Selbstbestimmung" im Datenschutz gegen das US-amerikanische Modell des „Marktes" auszuspielen versuchen. So etwa Shapiro (Fn. 1), S. 158 ff.; abwägender Reidenberg (Fn. 56), S. 717 ff., 730 ff.

Erwartungssicherheiten zu erzeugen.[89] Gerade der Schutz von Institutionen ist Aufgabe des modernen Rechts. Wenn sich dieser Institutionenschutz aufgrund der Evolution des Internets von der Ebene der Beziehungen zwischen Personen, sei es des Marktes oder der Organisation, auf die Ebene technischer Kommunikationsnetzwerke verschiebt, an deren laufender Produktion und Reproduktion Personen als Webnutzer beteiligt sind (so wie sie als Verbraucher am Marktgeschehen und als Mitglieder an Organisationen beteiligt sind), dann kann es in Zukunft durchaus eine neue Aufgabe des Verfassungsrechts und der Grundrechte sein, einen eigenständigen Beitrag zur Sicherung der technischen Funktionsbedingungen des Internets durch die Erzeugung von technischem Systemvertrauen zu leisten.

Damit soll angedeutet werden, dass das hier vorgestellte Ordnungsmodell an die objektiv-rechtliche Komponente der Wirtschaftsfreiheiten und insbesondere der Eigentumsfreiheit anzuknüpfen versucht. Die Vorstellung objektiv-rechtlicher Grundrechtsfunktionen setzt voraus, dass Grundrechte ein kollektives Moment besitzen, das seinerseits nicht in der privatautonomen Verfügbarkeit der subjektiv-rechtlichen Komponente der Grundrechte aufgeht. Die Logik des Arguments lautet hier, dass erst durch die objektiv-rechtliche Sicherung der Grundrechte die Voraussetzungen für ihre individuelle Ausübung geschaffen werden. Dieses Moment der individuellen Unverfügbarkeit der kollektiven Komponente der Grundrechte kann durchaus Friktionen mit einem liberalen Grundrechtsverständnis erzeugen, insbesondere wenn die Funktion der Realisierung der kollektiven Grundrechtskomponente in erster Linie dem Staat bzw. dem „demokratischen Gesetzgeber“ zugewiesen wird, wie es das Bundesverfassungsgerichts in der Vergangenheit nicht selten getan hat.[90] Eine solche Verknüpfung ist deshalb so ambivalent, weil dabei unterstellt werden muss, dass der Staat ein über der Gesellschaft stehendes autonomes, „souveränes“ Handlungssubjekt ist, der gesellschaftliche Beziehungen durch deliberative Entscheidungen „von oben“ strukturieren könnte. Daraus resultiert jedoch im Ergebnis eine staatliche Kompetenzerweiterung

89 Vgl. nur *N. Luhmann*, Das Recht der Gesellschaft, 1995, S. 124 ff.

90 Eine gewisse Ausnahme wäre die Betonung von Organisation und Verfahren z.B. im Rundfunkrecht, aber auch im Datenschutzrecht (Datenschutzbeauftragter) selbst.

zur „Freiheitssicherung“[91], die zu Lasten des verteilten, subjektiven Entscheidungsrechts geht und ihrerseits nicht mehr kontrolliert werden kann; und das ist gerade dort, wo es um die rechtliche Strukturierung privatautonomer Beziehungsnetzwerke von hoher Komplexität geht, nicht mit einer liberalen Vorstellung in Einklang zu bringen. Sofern man die Unverfügbarkeit des kollektiven Moments der Grundrechte aber in den laufenden dezentralen Such- und Kreationsprozessen der Individuen, Gruppen und Organisationen (der Wirtschaft) der Gesellschaft lokalisiert und die Emergenz von Ordnungsmustern und Regeln akzentuiert, die sich aus dieser Suche und Kreation neuer Märkte ergeben, eröffnet sich eine innovative Perspektive auf die objektivrechtliche Grundrechtskomponente, die auch für die netzwerkförmige konnexionistische Struktur des Internets und ein darauf abgestimmtes Datenschutzrecht fruchtbar gemacht werden kann.[92]

Deshalb ist die hier vorgeschlagene Zuordnung des Datenschutzes zu den Wirtschaftsgrundrechten und insbesondere zu Art. 14 GG kein Plädoyer für die Übernahme eines „privatistischen“ Eigentumsmodells in den Datenschutz. Es geht hier nicht darum, die Zuordnung exklusiver Entscheidungsrechte an einer Sache, also einem Ding oder Körper, in ein eigentumsanaloges Recht am „eigenen Datum“ umzuformulieren. Ob das Modell exklusiver Entscheidungsrechte die Struktur des Eigentumsrechts hinreichend erfasst oder seine auf Kooperation angelegte Komponente, wie sie insbesondere in der dem Eigentum komplementären Institution, dem Vertrag, zum Ausdruck kommt, nicht zu stark vernachlässigt, braucht hier nicht entschieden zu werden. Jedenfalls führt eine am materiellen Sacheigentum orientierte Begriffsbildung zu einer verkehrten räumlichen Analogiebildung, die nicht nur für das Datenschutzrecht irreführend ist;[93] sondern auch für die neuen Formen des immateriellen, „geistigen“ Eigentum inadäquat ist. Gerade das immaterielle Eigentum in Form von Patenten, Copyrights usw. gewinnt in der Informations- und Netzwerkökonomie an Bedeutung, und damit vollzieht sich auch im Eigentumsbegriff eine Annäherung an einen von vornherein auf Verknüpfung angelegten Informationsbegriff. Weil das Eigentum selbst immateriellen Cha-

91 Kritisch dazu *R. Wahl/J. Masing*, Schutz durch Eingriff, JZ 1990, S. 553.

92 Für andere Aspekte wie das „sematic web“ vgl. *K.-H. Ladeur* in diesem Band.

93 Kritisch dazu *Simitis* (Fn. 12); *Hoffmann-Riem* (Fn. 10), S. 520 ff.; Trute (Fn. 2), S. 825; *Albers* (Fn. 59), S. 81; *Hase* (Fn. 12), S. 40.

rakter annimmt und Information und Wissen zur wichtigsten ökonomischen Ressource aufsteigen, kann das Eigentum nicht länger auf Exklusion angelegt sein, sondern muss selbst auf die Logik der Vernetzung umgestellt werden.[94] Deshalb können Rechte der privatautonomen Verwendung von „personenbezogenen Daten“ durchaus einem in diesem Sinne erneuerten Art. 14 GG zugeordnet werden, ohne damit Gefahr zu laufen, Informationsrechte als „widerstreitende absolute Herrschaftsrechte“ fassen zu müssen.[95]

Eine Verlagerung und Verankerung des Datenschutzes in der objektivrechtlichen Komponente der Eigentumsfreiheit des Art. 14 Abs. 1 GG schließt eine sekundäre Modellierung privatautonomer Regelbildung durch ein staatliches oder suprastaatliches Datenschutzrecht nicht aus. Anders als bei der Rundfunkfreiheit nach Art. 5 Abs. 1 Satz 2 GG formuliert Art. 14 GG jedoch einen Primat des dezentralen Entscheidungsrechts, so dass staatliche Maßnahmen nur in Abstimmung mit den Selbstorganisationsprozessen der betroffenen Industrien und Dienstleistungsunternehmen erfolgen können. Darin ist auch eine Vermutung für den Vorrang von Selbstregulierung angelegt[96], die die staatliche Datenschutzgesetzgebung als „Vorgabe“ akzeptieren muss, also nicht ihrerseits durch „souveräne Entscheidungen“ übergehen darf. Erst wenn durch die Erfahrungen einer längeren Praxis erkennbar wird, dass sich innerhalb privatautonomer Austauschverhältnisse, etwa bei der Erstellung von Nutzerprofilen, Ordnungsmuster herausbilden, die negative kollektive Effekte erzeugen, Effekte, die zur Selbstblockierung einer technologischen und wirtschaftlichen Entwicklung führen können, dürfen staatliche oder andere politische Organisationen wie die EG in diese Prozesse der Selbstorganisation eingreifen.

94 Vgl. dazu nur *K.-H. Ladeur*, in: Hoffmann-Riem/Eifert (Fn. 2), S. 339 ff., 355 ff.; *T. Vesting*, Subjektive Freiheitsrechte als Elemente von Selbstorganisations- und Selbstregulierungsprozessen in der liberalen Gesellschaft - dargestellt am Beispiel der Bedeutung der Intellectual Property Rights in der neuen Netzwerkökonomie, in: "Regulierte Selbstregulierung", Die Verwaltung, Beiheft aus Anlass des 60. Geburtstags von Wolfgang Hoffmann-Riem, 2000, S. 21–57.

95 *Hoffmann-Riem* (Fn. 10), S. 520.

96 Vgl. dazu nur *Trute* (Fn. 2), S. 822 ff., 828 ff.; *Hoffmann-Riem* (Fn. 10), S. 537 ff.