11.09.2009

Grundrechts- und Funktionsschutz für elektronisch vernetzte Kommunikation

Wolfgang Hoffmann-Riem*

A. Zur Vorsorgeaufgabe des Staates

In der heutigen Wissens- und Informationsgesellschaft sind die Kommunikationsinfrastrukturen und die mit ihrer Hilfe möglichen Kommunikationsdienste mindestens so wichtig wie klassische Infrastrukturen und die darüber abgewickelten Leistungen, etwa die Straßen- und Schieneninfrastruktur. Im Bereich der für die gesellschaftliche Entwicklung aktuell besonders wichtigen elektronisch gestützten Information und Kommunikation hat der Staat allerdings die für frühere Infrastrukturen in weiten Teilen typische Regelungs- und Durchführungsverantwortung weitgehend eingebüßt. Er baut und betreibt die Infrastrukturen nicht (oder wenn, allenfalls begrenzt) selbst und sichert ihre laufende Funktionsfähigkeit nur begrenzt als Teil einer staatlichen Aufgabe: Die Erfüllungsverantwortung[1] trägt er insofern weitgehend nicht mehr. Auch die in Zeiten der Privatisierung und Deregulierung immer bestimmender gewordene – in Art. 87 f. Abs. 1 GG für einen Teilaspekt der Telekommunikation sogar ausdrücklich normierte – Gewährleistungsverantwortung[2] nimmt er bisher nur zurückhaltend wahr, so etwa im TKG und im TMG.[3]

Allerdings: Gegenwärtig erlebt der Ruf nach dem Staat in einem anderen Feld eine unerwartete Renaissance. Die gigantische Banken- und Finanzkrise[4], die die Funktionsfähigkeit der internationalen und nationalen Finanzsysteme und die Leistungskraft aller Volkswirtschaften nachhaltig unterminiert, hat nunmehr zu Forderungen nach der Einstandspflicht des Staates sogar von

---

* Für wertvolle Anregungen danke ich Matthias Bäcker.

1 Zu ihr allgemein vgl. statt vieler *H. Schulze-Fielitz*, Grundmodi der Aufgabenwahrnehmung, in*: W. Hoffmann-Riem/E. Schmidt-Aßmann/A. Voßkuhle* (Hrsg.), Grundlagen des Verwaltungsrechts, Bd. I (im Folgenden: GVwR I), 2006, § 12, Rn. 150 ff.

2 Zur Gewährleistungsverantwortung s. *Schulze-Fielitz* (Fn. 1), Rn. 154 ff.

3 Zu den jeweiligen Anwendungsfällen dieser Gesetze und deren Abgrenzung s. statt vieler *M. Köhler/H.-W. Arndt/T. Fetzer*, Recht des Internet, 6. Aufl. 2008, Rn. 890 ff.; *D. Heckmann*, Juris Praxiskommentar Internetrecht, 2007, Kap. 1.1, Rn. 29 ff.

4 Vgl. *M. Bloss/J. Häcker*, Von der Subprime-Krise zur Finanzkrise, 2008; *H.-W. Sinn*, Der Kasino-Kapitalismus – wie es zur Finanzkrise kam und was jetzt zu tun ist, 2009. Vgl. statt vieler auch *L. Zeise*, Ende der Party – Die Explosion im Finanzsektor und die Krise der Weltwirtschaft, 2. Aufl., 2009, Bank für Internationalen Zahlungsausgleich, 78. Jahresbericht vom 30. Juni 2008. Zu den Governance-Strukturen des internationalen Finanzsystems s. *T. Strulik*, Cognitive Governance. Beobachtungen im Kontext der Risikosteuerung des globalen Finanzsystems, in: *G. F. Schuppert/A. Voßkuhle*, Governance von und durch Wissen, 2008, S. 87 ff. Zu Folgeproblemen im Föderalismus s. etwa *J. Wieland*, Finanzkrise und Bundesstaat, ZG 2009, S. 140 ff.

Seiten derjenigen geführt, die sich bisher meist um eine Zurückdrängung der Rolle des Staates bemüht haben. Die Krise verweist auf Defizite in einem weitestgehend privat gestalteten, international vernetzten Sektor. Hinreichende Sicherungen der Beherrschbarkeit von Risiken haben offenbar gefehlt. Von den Staaten werden jetzt nicht nur Garantien in Milliardenhöhen erwartet sowie die Sanierung und Übernahme von "maroden" Banken, sondern es wird auch gefordert, das System der internationalen und nationalen[5] Finanzaufsicht grundlegend neu zu gestalten. Damit wird eine verstärkte Wahrnehmung der Gewährleistungsverantwortung des Staates sowie der internationalen Gemeinschaft reklamiert.

Auch andere Großsysteme können potenziell grundlegenden Gefährdungen ausgesetzt sein. Das globale elektronisch gestützte Kommunikationssystem ist ein möglicher Kandidat. In ihm dominieren private Unternehmen, die staatliche Aufsicht ist marginalisiert und Zugriff hat jedermann. Im Bereich des Bankensektors hat es früher immerhin eine relativ gut funktionierende Finanzaufsicht gegeben und es gibt immer noch Aufsichtsstrukturen[6] und Kooperationsvorkehrungen[7] – etwa im Zusammenhang mit den Aufgaben von IMF, Weltbank, ESZB und BAFIN –, an die beim Wiedereinrichten einer funktionsfähigen Finanzaufsicht angeknüpft werden kann. Vergleichbares gibt es im Bereich der informationstechnischen Infrastrukturen und der über sie abgewickelten Dienste nicht.[8]

---

5 Zu den verfassungsrechtlichen Dimensionen s. *M. Ruffert*, Verfassungsrechtliche Überlegungen zur Finanzmarktkrise, NJW 2009, S. 2093 ff.

6 Zu den vielfältigen Rechtsgrundlagen des europäischen und deutschen Kapitalmarktrechts s. die Internet-Übersicht der juristischen Fakultät der Universität Augsburg, *Prof. Möllers*, abrufbar unter http://www.jura.uni-augsburg.de/prof/moellers/materialien/5_kapitalmarktrecht.

7 Dazu vgl. *A. von Aaken*, Transnationales Kooperationsrecht nationaler Aufsichtsbehörden als Antwort auf die Herausforderung globalisierter Finanzmärkte, in: *C. Möllers/A. Voßkuhle/C. Walter* (Hrsg.), Internationales Verwaltungsrecht, 2007, S. 219 ff.

8 Die internationale und die nationale Regulierung von Telekommunikation und Kommunikationsdiensten hat allenfalls teilweise eine hier einschlägige Zielrichtung; vgl. – zum nationalen Telekommunikationsrecht – statt vieler die Beiträge in Beck'scher TKG Kommentar, 2006 sowie *A. Picot*, Die Effektivität der Telekommunikationsregulierung in Europa, 2008. Das Datenschutzrecht betrifft nur personenbezogene Daten. Es zielt weder auf die Sicherung der Funktionsfähigkeit kommunikationstechnischer Infrastrukturen selbst noch auf eine Kontrolle der vielfältigen in ihnen abgewickelten Dienste. Zum Datenschutzrecht s. statt vieler *A. Roßnagel*, Handbuch Datenschutzrecht, 2003. Zum Telekommunikations- und Telemediendatenrecht s. etwa *C. Schnabel*, Datenschutz bei profilbasierten Location Based Services, 2009, S. 115 ff.

Die informationstechnischen Infrastrukturen sind für die Leistungsfähigkeit moderner Gesellschaften und die private Entfaltung aller – jedenfalls der nicht mehr unter vormodernen Bedingungen lebenden Menschen – ebenso unabdingbar wie das Finanzsystem. Die IT-gestützte Kommunikation ist schon in technischer Hinsicht anfällig, wie Angriffe durch Hacker oder durch Viren u. ä. zeigen – auch wenn Netzattacken bisher abgewehrt oder weitgehend schadlos gemacht werden konnten.[9] Maßnahmen digitaler Kriegsführung (Cyberwar) werden schon jetzt als bedrohlich wahrgenommen.[10] Übergriffe durch Ausspähung von Informationen durch wirtschaftliche Konkurrenten oder fremde Mächte sind nicht selten. Auch Missbräuche von Zugangsmöglichkeiten zur Netzkommunikation und bei der Verwendung der dort erfassbaren Informationen sind schon vielfach bekannt geworden, auch wenn sie sich allem Anschein nach noch ebenso in Grenzen halten wie die missbräuchliche Nutzung der bei der Inanspruchnahme von Kommunikationsdiensten anfallenden Nutzerinformationen.[11]

Selbst wenn Risiken des technischen Zusammenbruchs der IT-Systeme vermeidbar sein sollten, bleiben Risiken von Fehlentwicklungen in der Nutzung, die Auswirkungen in diversen gesellschaftlichen Bereichen haben können. Angesichts des schnellen und mit hoher Dynamik erfolgenden Ausbaus der Kommunikationstechnologien und ihrer Nutzung sowie angesichts der hier gegebenen Komplexität, der Intransparenz und der vielfältigen Vernetzungen wäre es naiv, von der Prämisse der steten Beherrschbarkeit der Leistungsfähigkeit der Infrastrukturen und von stets hinreichenden Möglichkeiten der Abwehr von Missbrauch auszugehen.

Wird in Rechnung gestellt, dass die Kommunikation über informationstechnische Infrastrukturen immer mehr die private Lebensführung – und damit

---

9 Beispiele dazu in http://de.wikipedia.org/wikiCyberwar.

10 Vgl. dazu etwa *E. Halpin/P. Trevorrow/D. Webb/S. Wright*, Cyberwar, Netwar and the Revolution in Military Affairs, 2006 sowie Fn. 9. In der zitierten Fundstelle finden sich auch Hinweise auf Gegenmaßnahmen von Regierungen, etwa der amerikanischen und deutschen. Vgl. zum Problem auch von *A. Kreye*, Angriff aus dem Nichts, Süddeutsche Zeitung Nr. 180 vom 7. August 2009, S. 11

11 Ein viel diskutiertes Beispiel für Missbrauch hat die Deutsche Telekom geliefert, die in großem Stil die ihr verfügbaren Verbindungsdaten für Ermittlungen gegen Mitarbeiter, Betriebsräte und sogar den Vorsitzenden einer großen Gewerkschaft eingesetzt hat. Vergleichbare Datenmissbräuche hat es auch in anderen Unternehmen gegeben. Zu Praktiken eines illegalen Handels mit Kontodaten vgl. etwa *J. Scherer*, MMR 2008, S. 433 ff.

auch die Grundrechtsausübung – bestimmt, dass fast kein Wirtschaftsunternehmen ohne sie auskommt, dass viele lebenswichtige Versorgungsfelder von ihnen abhängen und dass auch der Staat für die Erfüllung seiner Aufgaben auf derartige Kommunikationssysteme angewiesen ist, dann können Defizite in der Funktionsweise massive Folgen selbst dann haben, wenn sie sich nicht zu einer Globalkrise[12] ausweiten.[13] Die mögliche Anfälligkeit des internationalen Finanzsystems, z. B. aufgrund der Schaffung und Nutzung vieler, in ihren Vernetzungen nicht überschaubarer und nicht durch hinreichende Gegenwerte abgesicherter Derivate, war vor Ausbruch der Finanzkrise grundsätzlich bekannt. Und dennoch hat niemand die Dynamik vorhergesehen, etwa in Analogie zu den – in der Chaostheorie illustrativ metaphorisch beschriebenen – Wirkungen eines "Flügelschlags des Schmetterlings"[14], dem in der praktischen Verwirklichung die übergroßzügige Hypothekengewährung für ein kalifornisches Reihenhaus als möglicher Anlass der weltweiten Krise geglichen haben könnte. Durch Gegensteuerung an der richtigen Stelle – etwa bei den Konditionen der Kreditgewährung und deren Sicherung – hätte die Finanzkrise vermutlich vermieden werden können.

Im Hinblick auf die nationale und internationale Kommunikationsinfra-struktur und deren inhaltliche Nutzung stellt sich die Aufgabe rechtzeitiger Vorsorge gegen mögliche Defizite als Teil der Daseinsvorsorge. Allerdings ist nicht geklärt, wieweit die Regelungsaufgabe des Staates reicht und welche realistischen Möglichkeiten es für ihn gibt, auf die Schaffung jedenfalls eines hinreichenden Minimums an gemeinwohlorientierten Regeln hinzuwirken und gegebenenfalls staatliche oder überstaatliche Rahmensetzungen zur Sicherung der Funktionsfähigkeit und zur Vorsorge für den Fall von Funktionsdefiziten

---

12 Zu Globalrisiken und -krisen, auch als Vertrauenskrisen, s. *U. Beck*, Weltrisikogesellschaft – Auf der Suche nach der verlorenen Sicherheit, 2008.

13 Beispielsweise wird in technischer Hinsicht angenommen, dass die Architektur der dezentralen Struktur von Netzen wie des Internet Risiken vorbeugt. Zur Funktionsweise der "Architektur" insbesondere des Internet vgl. die "klassische" Untersuchung von *L. Lessig*, Code und andere Gesetze des Cyberspace, 2001.

14 Zum "Schmetterlingseffekt" s. statt vieler *J. Gleick*, Chaos – Die Ordnung des Universums, 1987, S. 20 ff.

solcher Infrastrukturen oder zur Vermeidung dysfunktionaler Folgeprobleme zu schaffen.[15]

Auf einen Teilausschnitt aus diesem Problemkreis zielt der vorliegende Beitrag. Gefragt wird nach der verfassungsrechtlichen Fundierung einer auf die Funktionsweise der elektronisch vernetzten Kommunikation gerichteten, deren aktuelle Gefährdungen und Chancen aufgreifenden staatlichen Aufgabe. Zunächst erfolgen terminologische Klarstellungen (B). Daran schließen sich eine Illustration der aktuellen Möglichkeiten der Nutzung elektronisch vernetzter Kommunikation und einzelner damit verbundener Chancen und Risiken (C I, II) sowie der Hinweis auf den zunehmenden Kontrollverlust Einzelner in informationstechnischen Infrastrukturen an (C III). Der Hauptteil (D) ist um normative Orientierungen bemüht. Die in der deutschen Diskussion bisher zentrale Perspektive der Sicherung von Selbstbestimmung und eines personenbezogenen Grundrechtsschutzes bei der Nutzung der IT-Infrastrukturen wird zunächst zum Ausgangspunkt genommen (D I, II). Die grundrechtliche Schutzaufgabe aber ist umfassender, da auch andere Grundrechte einbezogen werden müssen und Kommunikationsschutz auch als Schutz von Verhaltensfreiheit jenseits des Persönlichkeitsschutzes, etwa der Berufs- und Wirtschaftsfreiheit, zu verstehen ist (D III). Soll auch der Schutz der Kommunikationsnutzung durch den Staat in die rechtliche Betrachtung einbezogen werden, muss die grundrechtliche Dimension verlassen werden. Dies gilt auch, wenn es um den Schutz der Kommunikationsinfrastruktur als solcher, insbesondere ihrer allgemeinen Funktionsfähigkeit, geht (D III, IV). Den Abschluss bilden Überlegungen zur trans- und internationalen Dimension der Schutzaufgabe (D V).

B. Schutz von Information, Kommunikation und Diensten

Seit der Schaffung der Datenschutzgesetze in den siebziger Jahren[16] und dem Volkszählungsurteil des BVerfG[17] ist es üblich geworden, den Schutzbedarf um den Begriff "Daten" kreisen zu lassen. Dieser wird in der

---

15 Dazu s. auch unten D V.

16 Zur – noch älteren – Geschichte des Datenschutzes s. *K. von Lewinski*, Geschichte des Datenschutzrechts von 1600 bis 1977, in: *F. Arndt* u. a. (Hrsg.), Freiheit – Sicherheit – Öffentlichkeit, 2009, S. 196 ff.

17 BVerfGE 65, 1.

rechtswissenschaftlichen Diskussion meist ohne nähere Ankoppelung an das Begriffsverständnis in anderen wissenschaftlichen Disziplinen genutzt. Um die Vielfalt möglicher Schutzdimensionen zu erkennen, ist es hilfreich, die Begriffe Daten, Information, Kommunikation[18] und Dienste sowie Infrastrukturen zu unterscheiden.

Daten werden insbesondere in informationstheoretischen Kontexten als interpretationsfreie ("bloße") Zeichen oder Symbole verstanden. Sie werden insoweit von Informationen unterschieden, also von Mitteilungen, die den Bestand von Kenntnissen betreffen und gegebenenfalls verändern und dabei Sinngehalte vermitteln. Informationsaufnahme und -verarbeitung ist ein auf soziale Kognition und Prozesse des Verstehens der Bedeutung und des Inhalts von Mitteilungen ausgerichtetes Verhalten. Der Informationsbegriff ist sehr weit und umfasst Mitteilungen über Kenntnisse jedweder Art. Informationen werden über "Kommunikation" ausgetauscht. Dieser Begriff erfasst ein mehr oder minder flüchtiges Geschehen, das die Mitteilung von Informationen und deren Verstehen zu einer einheitlichen Operation verknüpft. Kommunikation in diesem Sinne ist ein auf Verständigungshandeln ausgelegter Austausch. Die Verständigungsleistung wird durch den jeweiligen Kontext beeinflusst. Kontextänderungen können daher auch erhebliche inhaltliche Auswirkungen haben. Werden Informationen Mittel und Gegenstand besonderer, etwa kommerzieller, Kommunikationsdienste, verlassen sie den Bereich einer bloßen Verständigungsleistung und schaffen "Mehrwert", gegebenenfalls entlang einer langen und höchst differenzierten, viele Akteure einbeziehenden Wertschöpfungskette[19] oder entsprechender -netzwerke. Sie werden Bestandteile einer für viele Lebensbereiche wichtigen, insbesondere auch kommerziell nutzbaren Leistung, die ein eigenständiges, auch ein marktfähiges, Gut werden kann.

---

[18] Zu entsprechenden Begriffsdifferenzierungen s. etwa *T. Vesting*, Die Bedeutung von Information und Kommunikation für die verwaltungsrechtliche Systembildung, in: *W. Hoffmann-Riem/E. Schmidt-Aßmann/A. Voßkuhle* (Hrsg.), Grundlagen des Verwaltungsrechts, Bd. II (im Folgenden: GVwR II), 2008, § 20, Rn. 11 ff. m.w.Nachw. und Differenzierungen; s. auch *M. Albers*, Umgang mit personenbezogenen Informationen und Daten, GVwR II, § 22, Rn. 7 ff.

[19] Dazu s. schon *A. Zerdick u. a.* (Hrsg.), Die Internet-Ökonomie: Strategie für die digitale Wirtschaft, 1999, S. 94 ff., 125 ff., 172 ff. (jetzt 3. Aufl.)

Alle mit diesen Begriffen gekennzeichneten Erscheinungen können schutzbedürftig sein und Schutz durch Recht erfahren. Bevorzugtes Schutzobjekt des bisherigen Datenschutzrechts sind die Speicherung, die Weitergabe oder die Verarbeitung von Daten. Der Datenbegriff ist dabei weiter gefasst als in der informationstheoretischen Literatur, wie schon der im BDSG typische Bezug auf "personenbezogenen" Daten (§ 3 BDSG) verdeutlicht, aber auch an Einzelregelungen, wie dem Gebot der Zweckbindung (z.B. § 14 BDSG), oder an den informationsbezogenen Erlaubnistatbeständen (z. B. § 13 ff., 25 ff. BDSG) deutlich wird: Daten werden rechtlich geschützt, weil sie Informationen betreffen und Grundlage von Kommunikation[20] sind.[21] Der Schutzbedarf kann sich auf den Zugang zu entsprechenden Inhalten beziehen, aber auch auf den Transport und die Weiterverarbeitung der Information und ihre Integration in weitere Kommunikationszusammenhänge und Kommunikationsdienste und er kann sich allgemein auf die Funktionsfähigkeit der dafür eingesetzten informationstechnischen Infrastrukturen erstrecken.

C. Zur Dynamik des Ausbaus und der Nutzung elektronisch gestützter Kommunikation

I. Ausbau des Computereinsatzes und Vernetzung

Ausgangspunkt der neuen kommunikationstechnischen Möglichkeiten sind insbesondere die Computerisierung und Vernetzung. Auch wenn Computer schon älter sind, lag die erste rechtlich eigenständig relevante Phase der Computerisierung um den Zeitraum der Erschaffung der ersten Datenschutzgesetze[22] und des Volkszählungsurteils.[23] In diese Zeit fallen auch die Anfänge des Internet.[24] Nutzbar für Datenverarbeitung waren seinerzeit allerdings weitgehend nur schwergewichtige und voluminöse Großcomputer

---

20 Die entsprechende Kommunikation ist allerdings durch Besonderheiten gekennzeichnet, auf die die in vielem "verdinglicht" konzipierte Rechtsordnung nicht ausgerichtet ist, so die Unkörperlichkeit, Zeitlosigkeit, Gleichzeitigkeit, Ortlosigkeit, Ubiquität, Flüchtigkeit, Manipulierbarkeit, Vervielfältigbarkeit u. a. der Information, so etwa *A. Roßnagel*, Recht und Technik in der globalen Informationsgesellschaft, in: *D. Klumpp/H. Kubicek/A. Roßnagel* (Hrsg.), next generation information society?, 2003, S. 423, 432.

21 S. dazu *Albers* (Fn. 18), Rn. 65.

22 S. o. Fn. 16.

23 BVerfG 65, 1.

24 Dazu s. knapp *Köhler/Arndt/Fetzer* (Fn. 3), Rn. 1 ff.

mit geringer Speicher- und Verarbeitungskapazität und nur selten mit Vernetzung. Auch sonstige Mittel der Elektronik waren „gewichtig“ und aufwändig in der Bedienung. Bundeskanzler Adenauer, der als einer der ersten "Handynutzer" bekannt geworden ist, benutzte dienstlich ein mobiles Telefon, das 16 kg wog.[25] Die "zweite Ära" der Computer, die Nutzung und Verfügbarkeit leistungsfähiger, kleiner und preiswerter Computer für jedermann – wie jetzt PC oder Laptop – war im Zeitpunkt des Volkszählungsurteils erst im Entstehen und an Kommunikationsleistungen, wie sie z.B. das Smartphone heute ermöglicht, wurde noch gar nicht gedacht, erst recht nicht an die heute gegebene immense Leistungsfähigkeit des Internet und technologisch gestützter Dienste, wie UMTS oder E-Commerce. Staatliche Überwachungen durch Kfz-Scanning oder im Wege der Online-Durchsuchung sowie die vielen neuen Kommunikationsdienste, wie sie heute in sozialen Netzwerken möglich sind, waren allenfalls Gegenstand von Science Fiction. Für die nunmehr dritte Phase, die all dies und vieles mehr ermöglicht, ist die praktisch allgegenwärtige Computerisierung kennzeichnend – Schlagworte lauten ubiquitous[26] oder pervasive computing.[27] Auch wird die Vernetzung zur bestimmenden Größe ("von der Computerzentrierung zur Netzzentrierung"). Darauf aufbauend werden laufend neue Kommunikationsleistungen entwickelt und auf vielfältige Art zu ökonomisch verwertbaren Diensten ausgebaut.

II. Beispiele praktischer Nutzung

Im Folgenden werden illustrationshalber – und damit selektiv und nicht systematisch – einzelne in schneller Entwicklung befindliche Felder benannt, die die Vielfalt neuer Möglichkeiten ebenso erkennen lassen wie Gefährdungspotenziale.

---

25 S. acatech BEZIEHT POSITION Nr. 5, Intelligente Objekte – klein, vernetzt, sensitiv. Eine neue Technologie verändert die Gesellschaft und fordert zur Gestaltung heraus, 2009, S. 12.

26 Dazu vgl. *F. Mattern* (Hrsg.), Die Informatisierung des Alltags – Leben in smarten Umgebungen, 2007; *J. Kühling*, Datenschutz in einer künftigen Welt allgegenwärtiger Datenverarbeitung – Aufgabe des Rechts?, Die Verwaltung 40 (2007), S. 153 f.; *A. Roßnagel/T. Sommerlatte/U. Wienand* (Hrsg.), Digitale Visionen – Zur Gestaltung allgegenwärtiger Informationstechnologien, 2008.

27 Vgl. auch Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD) sowie Institut für Wirtschaftsinformatik der Humboldt-Universität zu Berlin (HU), TAUCIS. Technikfolgenabschätzung. Ubiquitäres Computing und Informationelle Selbstbestimmung, Juli 2006.

1. Soziale Netzwerke

Das Internet hat viele neue "Geschäftsmodelle" stimuliert. Besonders expandieren zur Zeit – vor allem bei Jugendlichen – die sog. sozialen Netzwerke[28] im Web 2.0[29] (Beispiele: Facebook, MySpace, Xing oder Studi-VZ). Sie ermöglichen eine ungeheure Fülle und Vielfalt von Kommunikation – mit immer neuen Innovationen –, führen zum Anfall vieler personenbezogener Daten und verändern nachhaltig die "Kommunikationswelt", auch infolge der dort möglichen und für viele besonders attraktiven Interaktivität.

2. Kollektive Wissensgenerierung

Die Potenziale des Internet werden vermehrt zur kollektiven Wissensgenerierung genutzt. In diesen Prozess können auch eine Reihe personenbezogener Informationen einfließen. Bekannte Beispiele kollektiver Wissensgenerierung sind die über das Internet "organisierten" Kreationen der "Free and Open Source Software" (FOSS)[30] oder des open content (Wikis).[31] Weitere Formen der netzwerkorganisierten Wissensgenerierung[32] entstehen, so das sog. crowdsourcing[33] – die Nutzung großer Netz-Communities als Kreativitätsquelle – oder die Animierung von Anwendern/Konsumenten eines Produkts zur elektronisch vernetzten Mitarbeit an seiner Konzeption, Konfiguration und Entwicklung, beim Marketing oder bei der Evaluation (als

---

28 Solche Netzwerke sollen gegenwärtig weltweit von 734 Millionen Menschen genutzt werden, s. FAZ Nr. 154 vom 7.7.2009, S. 15.

29 Dazu vgl. statt vieler *T. Alby*, Web 2.0, Konzepte, Anwendungen, Technologien, 3. Aufl. 2008; *J.-H. Schmidt/I. Paus-Hasebrink/U. Hasebrink* (Hrsg.), Heranwachsen mit dem Social Web. Zur Rolle von Web 2.0-Angeboten im Alltag von Jugendlichen und jungen Erwachsenen, 2009.

30 S. statt vieler *M. Osterloh/R. Luethi*, Commons without Tragedy: Das Beispiel Open Source Software, in*: M. Eifert/W. Hoffmann-Riem* (Hrsg.), Geistiges Eigentum und Innovation, 2008, S. 145 ff.

31 Etwa Wikipedia, dazu s.etwa *C. Kohl/W.A. Liebert*, Selbstorganisation in der Wissensvermittlung, in: Fachsprache, Bd.26 (2004), S. 133 ff.

32 Vgl. etwa die Beiträge in *O. Drossou/S. Krempl/A. Poltermann* (Hrsg.), Die wunderbare Wissensvermehrung. Wie Open Innovation unsere Welt revolutioniert, 2006; *R. Reichwald/F. T. Piller*, Interaktive Wertschöpfung. Open Innovation, Individualisierung und neue Formen der Arbeitsteilung, 2006; *A. Rolf*, Mikropolis 2010. Menschen, Computer, Internet in der globalen Gesellschaft, 2008, S. 46 ff., 69 ff., 89 ff.

33 Vgl. etwa *F. Kleemann/G. G. Voß/K. Rieder*, Crowdsourcing und der arbeitende Konsument, Arbeits- und industriesoziologische Studien 2008, Heft 1, S. 29 ff. mit Beispielen S. 35 f.

Beispiel von "prosuming": dem Zusammenfallen von Produzent und Konsument). Hier geht es meist – anders als bei den nicht kommerziell konzipierten Open Content-/Software-Projekten – um die gezielte Nutzung und direkte ökonomische Verwertung von kreativen Ideen und Arbeitsleistungen der Nutzer/Konsumenten.

3. Aufbau von Service-Plattformen[34]

Die Zunahme der Zahl und der Arten von Diensten hat u. a. zur Schaffung von Plattformen durch private Anbieter geführt, mit deren Hilfe die Grundfunktionen verschiedener Kommunikationsdienste und die Verwaltung der darauf bezogenen Daten wahrgenommen werden. So können über solche Plattformen z. B. Vertragsbeziehungen zwischen Lieferanten und Endkunden abgewickelt, der Zugang zu Diensten ermöglicht (etwa ein auf die persönlichen Bedürfnisse abgestimmter Restaurantfinder) oder Qualitätsmanagementsysteme aufgebaut und genutzt werden. Auf solchen Plattformen werden Systemdaten und -dienste bereitgestellt und es kann auch mehreren Anbietern ermöglicht werden, einen einheitlichen Katalog von Dienstleistungen über dieselbe Plattform bereitzustellen. Auf den Plattformen können zu dem Zweck gegebenenfalls auch detaillierte Informationen über den Nutzer, seine persönliche Situation, die Art und den Kontext der Dienstenutzung, seine Einstellungen und Präferenzen, Lebensgewohnheiten u. a. erhoben und gezielt ausgewertet werden, etwa um "maßgeschneiderte" Dienste anbieten zu können und die Benutzung zu erleichtern. Dafür werden üblicherweise durch Kombination verschiedener Daten auch Profile[35] gebildet, die in unterschiedlichen Kontexten einsetzbar sind.

---

[34] Zu deren Technik s. *Schnabel* (Fn. 8), S. 143 ff.

[35] § 15 Abs. 3 TMG begrenzt allerdings die Bildung von Nutzungsprofilen zum Zwecke der Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung der Telemedien auf die Verwendung von Pseudonymen und erlaubt dies nur, wenn der Nutzer dem nicht widerspricht. Dieser Schutz ist aber nicht umfassend. Zu der Frage, ob auch pseudonymisierte Daten Persönlichkeitsbezug haben können, s. *Schnabel* (Fn. 8), S. 198 ff. Soweit dies der Fall ist, ist § 15 Abs. 3 TMG nicht maßgebend (*Schnabel* (Fn. 8), S. 206 f.). Der Begriff der Nutzungsprofile ist nicht gesetzesdefiniert. Ob und wieweit Nutzungsprofile in anderen Kontexten geschaffen und genutzt werden dürfen, ist rechtlich nicht geregelt, s. *Schnabel* (Fn. 8), S. 169 f. Zur Technik der Profilbildung s. *Schnabel* (Fn. 8), S. 180 ff.

4. Internet der Dinge

Ein Feld mit vielen unterschiedlichen Nutzungsdimensionen ist das sog. "Internet der Dinge"[36], das Informationsleistungen in zum Teil kleinen Kommunikationsräumen erbringt und dabei auch auf das "große" Internet zugreifen kann.

Die Vielfalt der Anlassbeispiele ist groß. Ein noch relativ harmloses Beispiel ist die vermehrt mögliche Steuerung und insbesondere Fernsteuerung haushaltswirtschaftlicher Steuerungssysteme in sog. intelligenten Haushalten.[37] Ein anderes Beispiel ist der von der EU forcierte Ausbau "sicherer, sauberer und effizienter Mobilität" durch die Einrichtung intelligenter Verkehrssysteme, die einerseits die Verkehrssicherheit, aber auch die Energieeffizienz erhöhen sollen.[38] Ermöglicht werden soll eine (laufende) Informationsübertragung (und vielfach auch Standortkennung) von Fahrzeug zu Fahrzeug, zwischen Fahrzeug und Infrastruktur sowie von Fahrzeug zu Notrufsystemen.[39] Ferner: Informationstechnisch basierte Energiesysteme ("e-energy") sollen die umfassende digitale Vernetzung sowie eine computergestützte Kontrolle und Steuerung des Gesamtsystems der Energieversorgung ermöglichen – von der Quelle der Energieerzeugung bis zum Energieverbrauch – mit weitreichenden Zielen, etwa auch der Verbesserung des Umweltschutzes.[40] Dass auch andere lebenswichtige Leistungen – wie etwa der Luft- und Schienenverkehr oder die Regulierung von Schifffahrtsstrassen etwa durch Schleusen – computergestützt und vernetzt verlaufen, sei ergänzend erwähnt.

---

36 *H.-J. Bullinger/M. ten Hompel* (Hrsg.), Internet der Dinge, 2007; *E. Fleisch/F. Mattern* (Hrsg.), Das Internet der Dinge, Ubiquitous Computing und RFID in der Praxis, 2005; s. zum Folgenden auch *O. Herzog/T. Schildhauer* (Hrsg.), Intelligente Objekte. Technische Gestaltung – wirtschaftliche Verwertung – gesellschaftliche Wirkung, 2009.

37 Dazu s. etwa *M. Bayerlein-Hoppe*, Haushaltsgeräte vernetzen keine Spielerei, elektrobörse Handel 02/2004, S. 12 ff.

38 Vgl. dazu Mitteilung der *EU-Kommission* "Für eine europaweit sichere, saubere und effizientere Mobilität: 1. Bericht über die Initiative "Intelligentes Fahrzeug", KOM (2007), 541 endg.

39 Befürchtet wird, dass sie Ansatzpunkte für einen "gläsernen Kraftfahrer"schaffen. S. dazu *F. Dencker*, Der gläserne Kraftfahrer, Zfs 2008, S. 423; *K. Vieweg*, Die Auswertung von Fahrzeugdaten bei der Unfallanalyse, 45. VGT 2007, S. 292 ff. S. auch *Weyl*, Privacy und schützenswerte Daten im Kraftfahrzeug heute und morgen, Manuskript 2009 (erscheint in *Gerhäuser/Vieweg* (Hrsg.), Digitale Daten in Geräten und Systemen (i. E.).

40 Vgl. dazu Bundesministerium für Wirtschaft und Technologie, E-Energy. IKT-basiertes System der Zukunft, April 2000 und dazu *M. Zinke/L. Karg*, Energieeffizienz braucht IKT. IKT braucht Energieeffizienz, in: *A. Brandi-Dohrn/D. Heckmann* (Hrsg.), Informationstechnik und Recht, Jahrbuch 2008, 2009, S. 41 ff.

In vielen Lebensbereichen werden vermehrt kleine und intelligente Chips eingesetzt. Sie ermöglichen das kontaktlose Speichern und Auslesen von Daten, die auf sog. RFID-Tags (Radio Frequency Identification Tags) gespeichert sind, die ihrerseits nahezu überall und gegebenenfalls sogar (fast) unbemerkbar befestigt werden können und die Kommunikation zwischen den mit solchen Objekten versehenen Gegenständen sichern. Solche sog. smart objects können beispielsweise ein Produkt von seiner Produktion über den Transport bis hin zum Ge- und Verbrauch begleiten[41] und die dafür genutzten Daten können über das Internet kommuniziert werden. Einsetzbar ist auch "smart dust"; dies sind winzige Chips, die in großen Mengen eingesetzt sich miteinander vernetzen, ihre Umgebung in bestimmter Hinsicht überwachen und die dabei anfallenden Daten an eine Station übermitteln können. „Smart objects“ können die Zustände des Objekts und die Prozessabläufe erfassen und austauschen, in die das Objekt integriert ist. Sie können nicht nur für die Optimierung privaten Wirtschaftens genutzt werden, sondern auch für die Erfüllung staatlicher Aufgaben, etwa bei der Gewerbe-, Lebensmittel- und Veterinäraufsicht oder der Arzneimittelkontrolle. Sie sind aber auch einsetzbar als Mittel der polizeirechtlichen Gefahrenvorsorge und -abwehr sowie der Strafverfolgung, etwa durch deren Verbindung mit einem Gegenstand (wie einem Kraftfahrzeug), dessen Ortung für die Erfüllung staatlicher Aufgaben gewünscht wird, oder auch für die Erfassung des Aufenthalts von Personen.

Auch soweit Daten nur bezogen auf "Dinge " erhoben werden[42], können sie gleichwohl Persönlichkeits- und Vertrauensschutzrelevanz erlangen, etwa wenn die über die Chips markierten Gegenstände an Dritte weitergegeben, insbesondere der Umgang mit ihnen online kommuniziert und durch Vernetzung die Kombination mit anderen Daten an unterschiedlichen Stellen ermöglicht wird. Dabei können Kenntnisse sich von dem "Gegenstand" lösen und Teil von Kommunikationsvorgängen auch in personenbezogenen Kontexten werden. Wird nicht nach einer gewissen Zeit für eine – evtl.

---

41 Dazu s. auch *Kröner*, Digitales Produktgedächtnis, Manuskript 2009 (erscheint in *Gerhäuser/Vieweg* (Hrsg.), (Fn. 39).

42 Zu der Reichweite des verfassungsrechtlichen Schutzes s. *B. Holznagel/P. Schumacher*, Auswirkungen des Grundrechts auf Vertraulichkeit und Integrität informationstechnischer Systeme auf RFID-Chips, MMR 2009, S. 3 ff.

automatisch erfolgende – Zerstörung solcher smart objects gesorgt, können ihre Informationsleistungen gegebenenfalls unübersehbar lange genutzt werden.

Die technischen Möglichkeiten stimulieren die Diskussion um neue Anwendungsfelder – etwa darüber, ob Asylbewerbern solche Chips implantiert werden sollen, ob sie für die Bestimmung des Aufenthaltsorts von dementen Personen oder Kindern eingesetzt werden können oder ob die in Kfz-eigenen Computern gespeicherten Daten über Verkehrsverhalten (etwa bei Unfällen) auch von der Ordnungsbehörde oder von Dritten genutzt werden dürfen.

5. Cloud Computing

War die für die Nutzung der Kommunikationsnetze erforderliche Software früher weitgehend auf dem jeweiligen Computer installiert, kommt es zunehmend zu Auslagerungen. Ein aktueller Trend ist die Software-Nutzung im Rahmen des Cloud Computing.[43] Bei ihm sind die für internetbasierte Dienste eingesetzte Software und die generierten Daten nicht auf der Festplatte des eigenen Computers verfügbar, sondern werden außerhalb des Einflussbereichs des Nutzers von Dritten an externen, dem Nutzer meist unbekannten Rechnern verarbeitet und aufbewahrt. Technisch sind sie für eine Vielfalt von Kommunikationsvorgängen einsetzbar, ohne dass der Nutzer die Herrschaft darüber hat.

III. Das besondere Problem des Kontrollverlusts

Prägend für viele neue Entwicklungen ist der zunehmende Verlust an Kontrolle über die Daten und Kommunikation, die in der elektronisch vernetzten Kommunikation entstehen und verbreitet sowie in unterschiedlichen Kontexten verwendet werden. Dieser Kontrollverlust verstärkt den Bedarf nach staatlichen Sicherungen.

---

[43] Dazu vgl. *D. Chappell*, Associates, A Short Introduction to Cloud Platforms, August 2008, abrufbar unter: http://www.davidchappell.com/CloudPlatforms--Chappell.pdf. Neue Betriebssysteme – wie etwa Google Chrome OS – setzen verstärkt auf das Cloud Computing und sichern dem Unternehmen (wie etwa Google selbst) den Zugang zu vielfältigen Informationen und ermöglichen diesen auf deren Verfügbarkeit aufbauende Geschäftsmodelle, etwa vielfältiger und gezielt adressierter Werbung.

Bei Nutzung der modernen Kommunikationsinfrastrukturen wissen die Betroffenen häufig nicht, was mit ihren Daten geschieht, welche Möglichkeiten der Vernetzung über Internet und Intranet bestehen, welche Chancen und Risiken damit verbunden sind, etwa wann und wo die Daten in Zukunft folgenreich werden – das Internet vergisst bekanntlich nicht. Die Problemdimension ist auch dadurch geprägt, dass das Wissen um die Ge- und Missbrauchsmöglichkeiten durch Dritte begrenzt ist, wie auch das Wissen darüber, ob und gegebenenfalls wie der Einzelne sich davor schützen kann. Angesichts der Kompliziertheit vieler Benutzeroberflächen und erforderlicher Einzelschritte bei der Programmierung und Benutzung – etwa für den Einsatz der Software, die zum Selbstschutz erforderlich wäre – lässt sich nicht einmal sagen, dass die Computer- und Softwareindustrie dem Nutzer beim Selbstschutz nachhaltig behilflich ist und es lässt sich fragen, ob sie es überhaupt sein will, da er manchen Geschäftsmodellen zuwider läuft. Jedenfalls hat der Nutzer gegenwärtig wenig für ihn praktikable Möglichkeiten, die über die Daten vermittelten Informationen zu "beherrschen".

Die Frage nach dem Wissen über die und nach der Beherrschbarkeit möglicher Schutzinstrumente stellt sich nicht nur für den einzelnen Nutzer, der persönlich selbst dann, wenn er über ein gewisses Know-how verfügt, im Umgang mit ihm überfordert sein kann – insbesondere wenn er nicht zur Generation der mit dem Computer Aufgewachsenen gehört. Sie stellt sich vor allem für Wirtschaftsunternehmen – die Stichworte "Industriespionage" und "Industriesabotage"geben nur den Blick auf kleine Ausschnitte der Problemlage wieder. Die Frage betrifft auch den elektronisch kommunizierenden und vielfältig vernetzten Staat. So ist er hinsichtlich des Aufbaus der Netze und deren Nutzung in vielem von anderen abhängig, insbesondere auf Vorarbeiten und Unterstützung durch private Unternehmen angewiesen. Aber auch diese Unternehmen beherrschen die informationstechnischen Systeme nicht selbst, sondern sind regelmäßig auf Vorleistungen und Leistungen anderer angewiesen, deren Nutzung eine Auslagerung von Informationen auf diese erfordert.

Ein aktuelles Anschauungsbeispiel für die Auslagerung von Informationen ist das schon erwähnte, im schnellen Aufbau befindliche, insbesondere von Google und neuerdings auch von Microsoft vorangetriebene, cloud computing.[44] Mit diesem Schlagwort oder dem der "services in the cloud" wird zur Kennzeichnung internetbasierter Dienste eine Metapher genutzt, die auf die Undurchsichtigkeit und ständige Bewegung der komplexen Infrastruktur, insbesondere der Art der eingesetzten Software, hinweist, auf die eine netzbasierte Kommunikation zugreift. Die Nutzer können die konkret eingesetzten Dienste und den Ort und die Art der Verarbeitung der Daten (welcher Rechner, welches Rechenzentrum, für welche Zwecke?) sowie die eingesetzte Software nicht kennen und wissen nicht, welche konkreten Daten gegebenenfalls in andere Kontexte überführt werden. Selbst wenn sie solche Kenntnisse hätten, würden diese ihnen noch keine Zugriffsmöglichkeiten eröffnen. Die Unüberschaubarkeit für den Nutzer nimmt im Übrigen ständig zu und führt zu immer weiter reichendem Kontrollverlust.

Ein praktikables und zugleich hinreichendes Gegenmittel zum Erhalt von Selbstbestimmung liegt nicht etwa darin, die Akteure zur Datensparsamkeit und Datenvermeidung (vgl. z. B. § 3a BDSG) aufzurufen. Selbst bei Nutzung von auf Datensparsamkeit ausgerichteten Systemen und bei sparsamer persönlicher Datenverwendung ist nicht ausgeschlossen, dass die dennoch generierten Daten in einen vom Nutzer nicht (mehr) kontrollierbaren Kontext geraten. Angesichts der Grenzen der Beherrschbarkeit der Vorgänge durch den Nutzer kann auch nicht darauf abgestellt werden, dass er durchgängig eine Möglichkeit hat, sich selbst zu schützen. Vielmehr besteht häufig ein Bedarf nach Fremdschutz, d. h. letztlich auch nach staatlich gesichertem oder jedenfalls überwachtem Schutz.

D. Normative Orientierungen

I. Möglichkeiten und Grenzen, auf Autonomie abzustellen

---

[44] S. o. Fn. 43.

1. Autonomie als Ziel und Mittel

Ausgangspunkt zukünftiger Konkretisierungen muss in freiheitlichen Rechtsstaaten weiterhin die Idee informationeller Autonomie sein, die ihrerseits auf der allgemeinen Idee der Selbstbestimmung fußt, die für alle Entfaltungsgrundrechte bestimmend ist. In diesem Sinne hat das BVerfG dem von ihm formulierten Recht der informationellen Selbstbestimmung im Volkszählungsurteil[45] das Paradigma der Freiheitssicherung zugrunde gelegt. Diese soll in erster Linie durch die Möglichkeit autonomer Entscheidung über den Datenzugang und die Datenverwendung verwirklicht werden. Nur ausnahmsweise, wenn eine gesetzliche Eingriffsermächtigung besteht – etwa zur Telekommunikationsüberwachung im Bereich der Gefahrenabwehr oder der Strafverfolgung[46] – tritt der Autonomieschutz nach diesem Konzept zurück.

Das Paradigma der Autonomiesicherung gibt zunächst ein Ziel des Freiheitsschutzes an, das auch durch neue technologische Entwicklungen nicht entwertet ist. Selbstbestimmung und ein darauf aufbauendes Recht zum Selbstschutz sind Elemente des verfassungsrechtlichen Freiheitsregimes. Das BVerfG hat seine Formulierungen seinerzeit allerdings so gewählt, dass dieses Paradigma zugleich auf Wege der Zielerreichung verweist, nämlich auf solche, die letztlich auf Selbstbestimmung angewiesen sind. Dementsprechend ist das Datenschutzrecht vielfach auf Instrumente ausgerichtet, die vom Gedanken der Selbstbestimmung ausgehen. Dies zeigen etwa die zentrale Funktion der Einwilligung (§ 4 Abs. 1, § 4a BDSG, § 12 Abs. 1 TMG) oder die Möglichkeit der Anonymisierung und Pseudonymisierung (vgl. § 3a Satz 2 BDSG).

2. Praktische Grenzen

Aufgrund der Entwicklung der Computertechnologie, der Netzkonstellationen und vieler neuer Dienste sowie der dadurch bedingten, praktisch unausweichlichen Abhängigkeiten hat sich der Realbereich der Freiheitsentfaltung verändert. Er ist ausgeweitet worden, aber die

---

45 BVerfGE 65, 1, 41 ff.

46 Vgl. statt vieler die Darstellung bei *M. Kutscha*, Überwachungsmaßnahmen von Sicherheitsbehörden im Fokus der Grundrechte, LKV 2008, 481, 482 ff.

Möglichkeiten der selbstbestimmten Entscheidung über die Verfügbarmachung und den Umgang mit den Daten sind nicht entsprechend mitgewachsen.

Der einzelne Bürger kann das für die Freiheitsausübung allgemein und den Persönlichkeitsschutz speziell grundsätzlich zentrale Selbstbestimmungsrecht über den Umgang mit personenbezogenen Daten praktisch auch dann nur mit begrenzter Wirkungsreichweite ausüben, wenn ihm bekannt ist, dass und welche Daten anfallen. So entfällt eine Möglichkeit autonomer Disposition, wenn der Bürger für ihn wichtige Dienste nicht erhalten könnte, ohne in weitere Datenverwendungen einzuwilligen, oder wenn er – etwa zur Sicherung der Vertraulichkeit von Daten – durch Selbstschutz überfordert ist oder Selbstschutz zu unzumutbaren Funktionseinbußen führen würde.[47] Ließe sich Selbstbestimmung nur durch Verzicht auf die Nutzung der IT-Kommunikationssysteme und ihrer Dienste verwirklichen, reduzierte dies die praktische Bedeutung eines auf Selbstbestimmung bezogenen Grundrechts auf Ja-/Nein-Entscheidungen über Grundrechtsgebrauch und würde die für Freiheitsausübung wichtige Möglichkeit der Feinsteuerung nach je individuellen Interessen verfehlen.

Das Problem kann am Beispeil des Einwilligungserfordernisses illustriert werden. Für den, der nicht einmal übersehen kann, worin er einwilligt – etwa weil er nicht wissen kann, wer was wann und bei welcher Gelegenheit über wen weiß[48] und es wie verwenden kann –, erfüllt eine wichtige Voraussetzung einer wirkungsvollen Einwilligung nicht, nämlich das Informiertsein, und damit die Möglichkeit zu einer die Folgen übersehenen und insoweit selbstbestimmten Entscheidung. Insofern bedarf es einer Feinsteuerung der Ausgestaltung des Einwilligungserfordernisses – auch im Wege der AGB-Kontrolle –, die Anforderungen an die Wirksamkeit einer Einwilligung stellt, durch die das gebotene Minimum an Informiertsein gesichert wird. Soweit bei der Inanspruchnahme von Kommunikationsdiensten die Einwilligung zu

---

47 Vgl. etwa die Hinweise bei *W. Hoffmann-Riem*, Der grundrechtliche Schutz der Vertraulichkeit und Integrität eigengenutzter informationstechnischer Systeme, JZ 2008, 1009, 1016 f. S. auch BVerfG JZ 2007, 576: Dort verlangt das Gericht, dass informationeller Selbstschutz dem Einzelnen auch tatsächlich möglich und zumutbar sein muss.

48 Zu dieser Formulierung vgl. BVerfGE 65, 1, 43.

bestimmten Datennutzungen verweigert werden kann, ohne dass dadurch die Möglichkeit der Dienstenutzung entfällt, sind Selbstbestimmungsinteressen gewahrt. Führt eine Nichteinwilligung aber zum Verzicht auf die Nutzbarkeit eines Dienstes, werden die Betroffenen vor dieser Folgerung vielfach zurückschrecken. Die Versuchungen durch die Vorteile der Nutzung des jeweiligen Dienstes dürften angesichts des (für viele zunehmend ausnahmslosen) Angewiesenseins auf elektronische Dienste jedenfalls dann groß sein, wenn der Nutzer Zugang zu vergleichbaren Diensten ohne eine solche Einwilligung nicht oder nicht problemlos findet.[49] Eine durch die Umstände praktisch (wenn auch nicht rechtlich) "abgenötigte" Einwilligung kann eine hinreichende materielle Legitimationskraft vor dem Hintergrund des Autonomie-Paradigmas kaum schaffen.

3. Kein Abhängigmachen grundrechtlichen Schutzes vom Einsatz von Selbstschutzmaßnahmen

Die Ermöglichung von Selbstschutz ist in einer freiheitlichen Ordnung ein wichtiges Element des Grundrechtsschutzes. Unter heutigen Bedingungen kann modernes Schutzrecht im Bereich der Kommunikationstechnologie allerdings nicht allein darauf aufbauen, dass der Betroffene seine Interessen selbst wahrnehmen kann und wird. Soweit eine solche Möglichkeit nicht hinreichend ist, sieht der Staat es vielfach – etwa im Verbraucherschutzrecht – als seine Aufgabe an, möglichst für Vorkehrungen und Strukturen zu sorgen, die Schutz auch jenseits privatautonomer Schutzvorsorge ermöglichen. Dies hat auch das Datenschutzrecht in der Vergangenheit so eingeordnet, wie beispielsweise Bemühungen zeigen, Persönlichkeitsschutz durch System- und Technikgestaltung zu gewähren.[50]. Ist der Betroffene aber nur begrenzt Herr der System- und Technikgestaltung, ist effektiver Schutz darauf angewiesen, dass ergänzende Schutzmaßnahmen staatlicherseits geschaffen werden und gesichert ist, dass sie auch tatsächlich greifen.

---

[49] Das Koppelungsverbot der§ 28 III b BDSG, § 12 Abs. 3 TMG, § 95 Abs. 5 TKG – praktisch nur für Markt beherrschende Unternehmen – verringert das Problem, beseitigt es aber nicht.

[50] Dazu s. statt vieler *Albers* (Fn 18), Rn. 102 ff.; *A. Dix*, Konzepte des Systemdatenschutzes, in: *Roßnagel* (Fn. 8), Abschnitt 3.5.

Verfassungsrechtlich reicht es nicht, dass ein Schutz vor dem Zugreifen Dritter auf Daten oder vor Manipulationen der Software oder der Datenbestände durch technische Abwehr- und Schutzmaßnahmen gewährleistet werden kann, so durch Firewalls, Verschlüsselungstechniken, Antivirenprogramme oder sog. Anti-Forensik- und Antidetection-Werkzeuge.[51] Jedenfalls entfällt Grundrechtsschutz als solcher nicht dadurch, dass der Grundrechtsträger sich gegen Eingriffe auch technisch wehren kann. Der moderne Staat gewährt Schutz durch Recht und hat diese Schutzposition insbesondere mit dem Ziel der Ablösung von anderweitigem Selbstschutz (historisch etwa der Fehde) entwickelt. Dementsprechend werden Beschränkungen grundrechtlicher Freiheit grundsätzlich als rechtliche Eingriffe eingeordnet, so dass der Staat eine gesetzliche Eingriffsermächtigung auch braucht, wenn der Betroffene auf mögliche Selbstschutzvorkehrungen verzichtet. Beispielsweise entfällt der Schutz durch das Wohnungsgrundrecht des Art. 13 GG nicht deshalb, weil der Betroffene dem Polizeibeamten auf dessen Aufforderung hin ohne Gegenwehr die Durchsuchung der Wohnung ermöglicht oder weil der Wohnungsinhaber keine hohen Mauern um sein Haus baut und keine elektronischen Sicherheitsvorkehrungen vorgesehen hat. Der Schutz verringert sich auch nicht, wenn es Vorkehrungen gegen unerwünschtes Eindringen grundsätzlich gibt, der Grundrechtsträger sie aber nicht nutzt. So entfällt der Schutz des Art. 10 GG vor dem Abhören von Telekommunikation nicht dadurch, dass die Teilnehmer nicht mit schwer entschlüsselbaren Codewörtern kommunizieren oder nicht die VoIP-Software SKYPE nutzen, die den Zugriff auf die Gesprächsinhalte während der Kommunikation ausschließt. Auf die Möglichkeit solcher Schutzvorkehrungen reagiert der Staat etwa mit der Ermächtigung zur Informationserhebung in dem Zeitpunkt vor der Verschlüsselung oder nach der Entschlüsselung (an der "Quelle" oder beim Mitschnitt im Empfangscomputer[52]), Maßnahmen, die selbstverständlich ebenso einen Grundrechtseingriff darstellen wie staatliche Zugriffe auf die Kommunikation, denen solche Hürden nicht entgegenstehen.

---

51 Zu ihnen s. *A. Geschonneck*, Computer Forensik, 3. Aufl., 2008, S. 97 ff.

52 Vgl. BVerfGE 120, 274, 306 ff., 309 – zur Quellen-Telekommunikationsüberwachung.

4. Insbesondere: Autonomieschutz bei öffentlich zugänglichen Informationen

Soweit Nutzer Daten öffentlich machen – etwa in sozialen Netzwerken (s. o. D II 1) oder durch Mitarbeit an Prozessen kollektiver Wissensgenerierung im Internet (s. o. D II 2) – ist das Selbstbestimmungsrecht insoweit gewahrt, als dies auf einer freiwilligen Entscheidung beruht, bei der grundsätzlich erkennbar ist, dass die "Herrschaft" über die Daten aufgegeben wird. Eine berechtigte Vertraulichkeitserwartung besteht insoweit selbstverständlich nicht. Können Dritte – auch der Staat – Internetkommunikation auf dem technisch dafür vorgesehenen Weg einsehen, liegt in der Kenntnisnahme grundsätzlich kein Grundrechtseingriff.[53]

Anders kann aber die Bewertung ausfallen, wenn die aus Anlass dieser Kommunikation anfallenden Nutzungsdaten in andere Kontexte einfließen.[54] Insofern bedarf weiterer Abklärung, wie weit das Öffentlichmachen von Kommunikation Schutzbedarf auslöst oder ob es zugleich als eine Einwilligung gemeint ist oder gedeutet werden darf, dass diese Daten durch Dritte für Zwecke aller Art verarbeitet und in anderen Kontexte genutzt werden dürfen. dies liegt eher fern. Auf keinen Fall liegt eine Einwilligung zu Manipulationen und sonstigem Missbrauch vor. Rechtlicher Persönlichkeitsschutz bleibt daher relevant.

Soweit Internetnutzer sich an öffentlich zugänglichen Prozessen kollektiver Wissensgenerierung beteiligen (s. o. D II 2), bewirkt dies nicht automatisch den Verzicht auf Schutz der Ergebnisse der geistigen Leistung vor der Nutzung durch Dritte. So bedeutet die Mitwirkung an Prozessen kollektiver Intelligenz nicht selbstverständlich eine Einwilligung, dass die Wertschöpfung durch diese Leistung in rechtlicher und ökonomischer Hinsicht ausschließlich anderen zugute kommt, also in deren Wertschöpfungsnetzwerke integriert werden darf. Ist aber gerade eine offene Nutzung durch jedermann gewollt – wie bei Open Content und Open Software –, ist dem Anliegen Genüge getan, jedenfalls sofern – wie durch die

---

53 BVerfGE 120, 274, 344 f., s. auch *T. Böckenförde*, Auf dem Weg zur elektronischen Privatsphäre, JZ 2008, S. 925, 935 f.

54 S. dazu – allerdings nur bezogen auf den staatlichen Zugriff, nicht auf die Nutzung öffentlich zugänglicher Daten durch Private – BVerfGE 120, 274, 345.

Nutzung der Copyleft-Klausel[55] gesichert werden kann – ausgeschlossen ist, dass Dritte sich die Leistung rechtlich unter Ausschluss anderer aneignen können.

II. Verfassungsrechtlicher Persönlichkeitsschutz

Angesichts der Bedeutung der informationstechnischen Infrastrukturen und der dort abgewickelten Dienste ist der Persönlichkeitsschutz ein besonders wichtiger Aspekt effektiven Grundrechtsschutzes. Die neuen Gefahrendimensionen haben das BVerfG in seiner IT-Entscheidung[56] veranlasst, ergänzend zu dem Grundrecht auf informationelle Selbstbestimmung eine neue Konstruktion zu entwickeln und dabei als Schutzziel die Vertraulichkeit und Integrität komplexer eigengenutzter, aber nicht eigenbestimmbarer informationstechnischer Systeme[57] herauszuarbeiten. Die Vertraulichkeit der Kommunikation setzt den Schutz vor Einblicken Dritter und vor der Weiterverarbeitung von Daten durch Dritte voraus. Von entsprechenden Schutzerwartungen erfasst ist auch die Integrität[58] des eigengenutzten informationstechnischen Systems, also der Schutz vor der Überwindung von Hindernissen, die vor dem Eindringen schützen, sowie vor Störungen und Manipulationen, etwa vor Verfälschungen (und dabei auch vor Beeinträchtigungen der Authentizität), vor Ergänzungen durch weitere Daten oder vor dem Einsatz entsprechender Schad-Software (Malware)[59], die den durch Daten transportierten Sinngehalt manipuliert oder die Daten in unübersehbare Kontexte katapultiert. Schutzbedarf besteht auch hinsichtlich der Infiltration und Manipulation der Programme, die – wie das Betriebssystem oder die Anwender-Software – die Funktionsweise ermöglichen oder Dritten den Zugang zu diesem System eröffnen.

Allerdings wird in der neuen Konkretisierung der alten Grundrechtsverbürgung der Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG nur der

---

55 Zu ihr s. *T. Jäger/A. Metzger*, Open Source Software, 2. Aufl. 2006, S. 4.

56 BVerfGE 120, 274.

57 Dazu vgl. *M. Bäcker* , Die Vertraulichkeit der Internetkommunikation, in: *H. Rensen/S. Brink (Hrsg.)*, Linien der Rechtsprechung des Bundesverfassungsgerichts - erörtert von den wissenschaftlichen Mitarbeitern, S. 99, 126 ff.

58 Zum Integritätsschutz vgl. *Bäcker* (Fn. 57), S. 125.

59 Zu Techniken des Zugriffs auf Computer s. etwa *H. Federrath*, Technische Aspekte des neuen Computergrundrechts, in: *R. Uerpmann-Wittzack* (Hrsg.), Das neue Computergrundrecht, 2009, S. 53, 54 ff.

personenbezogene Schutz berücksichtigt. Sie zielt nicht auf ein apersonales technikbezogenes Grundrecht, denn der Schutz ist ja aus dem Persönlichkeitsschutzrecht abgeleitet und insofern darauf begrenzt.[60] Der gegen Infiltrationen oder die Durchsuchung von Speichermedien als solchen gerichtete Schutz des informationstechnischen Systems erstreckt sich allerdings auch auf die für die Abläufe wichtigen Daten[61], so die im Arbeitsspeicher gehaltenen und temporär oder dauerhaft auf den Speichermedien des Systems abgelegten sowie – etwa beim cloud computing[62] – ebenfalls auf die außerhalb des eigenen Herrschaftsbereichs in fremden (aber eigengenutzten) Rechnern gespeicherten und erarbeiteten Daten.

Das herkömmliche Grundrecht auf informationelle Selbstbestimmung hat daneben weiterhin eigenständige Bedeutung.[63] Es gewährt seinen Trägern Schutz gegen die Erhebung, Speicherung, Verwendung und Weitergabe der auf sie bezogenen individualisierten oder individualisierbaren Daten. Es wehrt solche Gefährdungen ab, einerlei, ob sie punktuell oder fortlaufend, im Einzelfall oder massenhaft erfolgen. Dieses Grundrecht ist in der Rechtsprechung und Wissenschaft zu Recht nicht dahingehend eingeengt worden, dass es nur Maßnahmen mit direktem Bezug auf den Vorgang der Datenerhebung und anschließender Speicherung, Verwendung oder Bearbeitung sowie Weitergabe betrifft. Vielmehr erstreckt es sich auch auf organisatorische, verfahrensmäßige oder systemische Voraussetzungen dafür, dass derartige Erhebungen und nachfolgende Maßnahmen den grundrechtlichen Vorgaben entsprechen – also gegebenenfalls durch gegenläufige Interessen gerechtfertigt sind –, oder aber mangels Erfüllung der gesetzlichen Tatbestandsvoraussetzungen für Eingriffe unterbleiben. Der

---

60 Anders aber etwa *M. Eifert*, Informationelle Selbstbestimmung im Internet – Das BVerfG und die Online-Durchsuchungen, NVwZ 2008, 521, 522. S. ferner – wenn auch außerhalb einer vertretbaren Auslegung der BVerfG-Entscheidung, aber mit Verständnis für die Notwendigkeit auch objektiv-rechtlichen Grundrechtsschutzes –, *O. Lepsius*, Das Computer-Grundrecht: Herleitung – Funktion – Überzeugungskraft, in: *F. Roggan* (Hrsg.), Online-Durchsuchung, 2008, S. 21 ff.

61 Die rechtlichen Begriffe hierzu sind nicht ganz eindeutig, so spricht das TKG etwa von Bestands- und Verkehrsdaten (§ 3 Nr. 3, 30 TKG), das TMG von Bestandsdaten, Nutzungsdaten und Abrechnungsdaten (§ 14 Abs. 1, 15 Abs. 1, 15 Abs. 4 TMG), zu den entsprechenden Begriffen s. statt vieler *Köhler/Arndt/Fetzer* (Fn. 3), Rn. 919 ff., 922 ff.

62 S. o. Fn. C II 5.

63 Vgl. BVerfGE 120, 274, 311 ff.

Schutz informationeller Selbstbestimmung setzt dann schon auf der Ebene der Grundrechtsgefährdung an und kann deswegen durch solche strukturellen Vorkehrungen auf Gefährdungspotenziale reagieren. Auch wo Schutzvorkehrungen – etwa Maßnahmen zum Systemdatenschutz[64] – der konkreten Datenerhebung vorgelagert sind, handelt es sich um Maßnahmen zur Vorbeugung gegen Datenbeeinträchtigungen.

Dieser Systemdatenschutz umfasst in seiner bisherigen Ausprägung aber nicht auch den Schutz des Vertrauens in die Funktionsweise des eigengenutzten informationstechnischen Systems selbst. Der schon bisher mögliche und praktizierte Datenschutz durch Systemgestaltung ist nicht identisch mit einem Schutz des (so gestalteten) informationstechnischen Systems vor dem Zugriff auf das System selbst und vor den dadurch ermöglichten Datenzugriffen. Das verkennt der Teil der Literatur, der meint, die neue Grundrechtsausprägung sei überflüssig[65], insbesondere weil es doch schon heute Datenschutz durch Systemgestaltung gebe.

Der besondere Schutz der Vertraulichkeit und Integrität eigengenutzter informationstechnischer Systeme ergänzt den Schutz des Rechts auf informationelle Selbstbestimmung und verschärft Schutz durch grundsätzlich strengere Anforderungen an entsprechende Grundrechtseingriffe als bei Eingriffen in die sonstigen Gewährleistungen des Persönlichkeitsschutzes.[66] Soll eine rechtliche Grundlage auch zu heimlichen Eingriffen ermächtigen[67], bedarf dies einer darauf ausgerichteten Rechtfertigung, die berücksichtigt, dass der bei Kenntnis der Maßnahme sonst mögliche Schutz durch Eigeninitiative des Betroffenen außer Kraft gesetzt wird. Der Autonomieschutz muss dann in dem Schutz des Vertrauens auf Wahrung der

---

64 S. o. Fn. 50.

65 Dies ist der Obertenor der meisten kritischen Stellungnahmen, die darüber hinaus natürlich auch Einzelkritik üben. S. dazu etwa *Eifert* (Fn. 60), 521 ff.; *M. Sachs/T. Krings*, Das neue "Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme", JuS 2008, S. 481, 482 ff.; *Lepsius* (Fn. 60), 21 ff.; sowie *U. Volkmann*, Urteilsanmerkung DVBl. 2008, S. 590 ff.; *G. Britz*, Vertraulichkeit und Integrität informationstechnischer Systeme, DÖV 2008, S. 411 ff. Grundlegende Kritik an der Neukonstruktion auch bei *G. Manssen*, Das "Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme" – ein gelungener Beitrag zur Findung unbenannter Freiheitsrechte?, in: *Uerpmann-Wittzack* (Fn.59), S. 61 ff.

66 S. BVerfGE 120, 274, 315 ff.

67 Das IT-bezogene Grundrecht schützt allerdings nicht nur vor heimlichen Zugriffen, s. *D. Hömig*, "Neues" Grundrecht, neue Fragen?, Jura 2009, S. 207, 210. S. ferner *Böckenförde* (Fn. 53), S. 931.

rechtsstaatlichen Voraussetzungen des Eingriffs aufgehoben sein, und zwar gegebenenfalls auch durch Kontrollvorkehrungen, die nicht auf Initiative des Betroffenen angewiesen sind.[68]

Soweit das Grundgesetz Persönlichkeitsschutz über das Recht auf informationelle Selbstbestimmung und den Schutz der Vertraulichkeit und Integrität eigengenutzter informationstechnischer Systeme gewährt, erschöpft er sich nicht in einer subjektiv-rechtlichen Garantie. Die Grundrechtsnorm strahlt vielmehr auf die gesamte Rechtsordnung ein. Die objektiv-rechtliche Dimension des betroffenen Grundrechts[69] betrifft insbesondere die Gestaltung der Rechtsordnung im Umgang mit Beeinträchtigungen durch Private[70], etwa durch privatwirtschaftliche Unternehmen.[71] Aus dieser programmatischen Orientierung können Handlungsaufträge und Handlungspflichten für den Staat und Auslegungsmaximen bei der konkreten Rechtsanwendung folgen. Auf diese Weise werden die Integrität und Vertraulichkeit von eigengenutzten komplexen informationstechnischen Systemen zu einer Aufgabe und zugleich zu einem Leitbild für Freiheitsschutz als Persönlichkeitsschutz.[72]

III. Schutzaufgabe und -aufträge

Angesichts der Angewiesenheit von individuellen und gesellschaftlichen sowie hoheitlichen Akteuren auf die informationstechnischen Infrastrukturen und die dort abgewickelten Dienste wäre es allerdings eine erhebliche Problemverkürzung, staatlichen Schutz auf personenbezogene Kommunikation zu begrenzen. Beeinträchtigungsverbote und Schutzaufträge

---

68 S. etwa zum Richtervorbehalt BVerfGE 120, 274, 331 ff.

69 Dazu vgl. *Bäcker* (Fn. 57), S. 118 ff. S. ferner *G. Hornung*, Ein neues Grundrecht? CR 2008, S. 299 ff., 305; *M. Kutscha*, Mehr Schutz vor Computerdaten durch ein neues Grundrecht?, NJW 2008, 1042, 1044; *T. Stögmüller*, Vertraulichkeit und Integrität informationstechnischer Systeme in Unternehmen, CR 2008, S. 435 ff.; zustimmend *P. Sick*, VBlBW 2009, 85 mit Fn. 6 und dort weiteren Nachw. S. ferner *Petri*, Das Urteil des Bundesverfassungsgerichts zur Online-Durchsuchung, DuD 2008, S. 446, 448; *Lepsius* (Fn. 60), S. 32 ff.; *D. Heckmann*, Staatliche Schutz- und Förderpflichten zur Gewährleistung von IT-Sicherheit, in: Festschrift für G. Käfer, 2009, S. 129 ff. *Hömig* (Fn. 67), S. 211; *Gusy/Worms*, Grundgesetz und Internet, APuz 18/19/2009, S. 26, 32.

70 Vgl. BVerfGE 120, 274, 312 (wenn auch ausdrücklich nur zum Recht auf informationelle Selbstbestimmung).

71 Beispiele sind der Zugriff auf Daten sog. data mining, die Datenauswertung zur Adressierung von Werbebotschaften (Erfassung von Informationen über persönliche Vorlieben und das Konsumverhalten u. ä.), das Scoring-Verfahren bei der Kreditgewährung u. ä.

72 Vgl. dazu *I. Härtel*, Altes im neuen Gewande?, NdsVBl. 2008, S. 276, 279.

folgen auch aus anderen Grundrechten. In Betracht kommen etwa das Telekommunikationsgeheimnis (Art. 10 GG)[73] und das Wohnungsgrundrecht (Art. 13 GG).[74] Einschlägig können auch die Berufsfreiheit (Art. 12 GG) und die Eigentumsfreiheit (Art. 14 GG) sein. Arbeitnehmerdatenschutz, der sich nicht in Persönlichkeitsschutz erschöpft, oder der Schutz geistigen Eigentums sind bekannte Anwendungsfelder. Stets ist zu klären, welches der Schutzbereich des betroffenen Grundrechts ist und unter welchen Voraussetzungen Eingriffe zulässig sind. Beispielsweise sind die Anforderungen an Eingriffe im Persönlichkeitsschutzbereich regelmäßig strenger als in anderen grundrechtlichen Bereichen. So besteht ein absolut geschützter Kernbereich privater Lebensgestaltung[75] nur beim Persönlichkeitsschutz, nicht etwa bei beruflichen Betätigungen. Allerdings gibt es auch hier, etwa durch den traditionellen Schutz von Berufs- und Geschäftsgeheimnissen, Schutzgüter, die auch Aspekte der Vertraulichkeit und Integrität von Kommunikation umfassen. Gleiches gilt für den für staatliche Aktivitäten anerkannten, aber auch durch Informationszugangsrechte – dazu siehe das Informationsfreiheitsgesetz[76] – relativierten Geheimnisschutz.

Die staatliche Schutzaufgabe ist nicht auf grundrechtlich geschützte Betätigungen begrenzt, sondern erfasst auch Bereiche, in denen der Staat zur Erfüllung öffentlicher Aufgaben selbst auf informationstechnische Systeme zugreift, etwa bei der Aufgabenerfüllung im Zuge des E-Government.[77] Zwar ist eine verfassungsrechtliche Fundierung entsprechender Schutzaufträge nur partiell ausdrücklich erfolgt, etwa in Regeln über die (Bundes)Verwaltung (s. z. B. Art. 87d, e, 89, 90 GG) oder die Gesetzgebungskompetenz (s. z. B. Art. 73 Abs. 1 Nr. 6, 6a; 74 Abs. 1 Nr. 21, 22, 23 GG), zum Teil gekoppelt mit inhaltlichen Anforderungen, so durch den Gewährleistungsauftrag aus Art. 87 f. Abs. 1 GG im Bereich der Telekommunition. Der Staat ist aber nicht nur berechtigt, sondern als sozialer Rechtsstaat auch programmatisch

---

73 Dazu vgl. BVerfGE 120, 274, 306 ff.; Beschluss vom 16. Juli 2006, 2 BvR 902/06, Rn. 42 ff. sowie *Bäcker* (Fn. 57), S. 102 ff.

74 S. etwa BVerfGE 120, 274, 309 ff.

75 Zu ihm s. etwa BVerfGE 120, 274, S. 335 ff. m.w.Hinw.

76 Dazu s. die Kommentierungen bei *F. Schoch*, IFG, 2009.

77 Dazu s. statt vieler *M. Eifert*, Electronic Government. Das Recht der elektronischen Verwaltung, 2006.

aufgefordert, Infrastrukturverantwortung zu übernehmen[78], und zwar für informationstechnische Infrastrukturen als Fortsetzung der Aufgabe, die sich früher nur auf das Post- und Fernmeldewesen bezog. Angesichts der Offenheit des Grundgesetzes für trans- und internationale Entfaltungsmöglichkeiten betrifft die staatliche Verantwortung auch außerhalb seiner räumlichen Grenzen den Schutz der Funktionsfähigkeit informationstechnischer Systeme und der darüber abgewickelten Dienste, soweit er dort auf sie einwirken kann. Je wichtiger die Leistungsfähigkeit globaler informationstechnischer Infrastrukturen für die Entfaltung in verschiedenen Lebensbereichen und für die Gesellschaft insgesamt ist, umso mehr wird die Wahrnehmung von Schutzaufgaben durch den Staat zu einem Wesenselement sozial- und rechtsstaatlicher Gestaltung der Lebensbedingungen.

Im Einzelnen bestehen selbstverständlich erhebliche rechtsdogmatische Unterschiede zwischen den verschiedenen Ableitungen der Schutzaufgabe und des Schutzauftrags, so zwischen der Verwirklichung grundrechtlichen Persönlichkeitsschutzes für die Bürger, der Sicherung der Verhaltensfreiheit von wirtschaftlichen Unternehmen, dem Erhalt der Fähigkeit des Staates zur Erfüllung seiner allgemeinen Aufgaben unter Nutzung informationstechnischer Systeme sowie der Sorge für deren Funktionsfähigkeit als solcher.

IV. Aufmerksamkeitsfelder staatlicher Regulierung

Werden die verschiedenen Schutzbedarfe nicht erkannt oder rechtlich nicht befriedigt, besteht das Risiko von Funktionsdefiziten, auch das des Verlustes von Vertrauen in die informationstechnischen Systeme, verbunden mit dem weiteren Risiko, dass die durch sie ermöglichten Chancen nicht genutzt werden können. Das für informationstechnische Systeme wichtige Vertrauen[79] bezieht sich nicht nur darauf, dass die informationstechnischen Kommunikationsinfrastrukturen technisch, sondern auch darauf, dass sie in

---

78 Auszugehen ist von der lange anerkannten Einsicht, dass die Sicherung der Leistungsfähigkeit von Infrastrukturen auch eine Staatsaufgabe ist, vgl. etwa *H. P. Bull*, Die Staatsaufgaben nach dem Grundgesetz, 1977, S. 266 ff.; *G. Hermes*, Staatliche Infrastrukturverantwortung, 1998, etwa S. 128 ff., 323 ff., 333 ff., 400 ff.

79 Zu ihm grundsätzlich die Beiträge in *Klumpp/Kubicek/Roßnagel/Schulz* (Hrsg.), Informationelles Vertrauen für die Informationsgesellschaft, 2008. S. auch *Boehme-Neßler*, Unscharfes Recht, 2008, S. 428, 435 ff.

den Anwendungskontexten –gewissermaßen sozial – so funktionieren, wie die Nutzer es erwarten dürfen. Die soziale Leistungsfähigkeit solcher Infrastrukturen beruht – aufbauend auf den vielen technologischen und dienstbezogenen Leistungen – auch darauf, dass ein entsprechendes Vertrauen bei den Nutzern als Basis für Kommunikation aufgebaut wird und bei der praktischen Nutzung der Infrastrukturen auch wirksam wird, also praktisch gerechtfertigt ist.

Bei einer durch Vertrauensverlust bedingten Erosion der Leistungsfähigkeit gehen die möglichen Folgen über die konkret Betroffenen hinaus und können beispielsweise den Nutzen der elektronisch gestützten Kommunikation für Wirtschaftsunternehmen oder auch für den Staat beeinträchtigen, die mit den Bürgern über informationstechnische Systeme kommunizieren oder die sie auf andere Weise zur Aufgabenerfüllung nutzen. Dies hätte ebenfalls Folgen für die Nutzung informationstechnischer Systeme für private Zwecke einzelner Bürger: dadurch könnten die Bedingungen der Grundrechtsausübung in unterschiedlichen gesellschaftlichen Bereichen erschüttert werden. Auch insofern hat die vom BVerfG konkretisierte Teilausprägung des Grundrechts aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG mittelbar eine paradigmatische, über den Schutz des Persönlichkeitsrechts hinausweisende Bedeutung. Die Voraussetzungen für das Vertrauen in die Funktionsfähigkeit der informationstechnischen Systeme sind insgesamt so zu schaffen, dass sie sich in den verschiedenen Anwendungskontexten als freiheitsfördernd erweisen und insbesondere die Erfüllung von Aufgaben erleichtern, die über elektronisch vernetzte Kommunikation wahrgenommen werden.[80]

Diese Betrachtung reagiert zugleich auf den "qualitativen Sprung" in der gesellschaftlichen Bedeutung der Gefährdungslage und des Schutzbedarfs im Vergleich der vom Volkszählungsurteil[81] erfassten Situation mit der heutigen. Die Funktionsfähigkeit informationstechnischer Systeme – auch die der seinerzeit eingesetzten Großrechner – war damals ebenso wenig Thema öffentlicher Diskussion wie der Schutz von Kommunikationsdiensten. Es ging

---

80 Vgl. auch *Heckmann* (Fn. 69), S. 135.
81 Dazu s. BVerfGE 65, 1.

seinerzeit um Schutz vor einem möglichen Missbrauch durch Re-Individualisierung von manuell erhobenen Daten und durch ihre elektronische Verknüpfung mit anderen. Heutige Gefährdungslagen sind u. a. in der Art der Datenerlangung, der Breite und Tiefe der davon betroffenen Informationen, der Vielfalt und Unüberschaubarkeit der Verwendungen, insbesondere der vernetzten Nutzung, aber auch der Möglichkeit zur Erstellung komplexer Persönlichkeits-, Bewegungs- oder Sozialprofile damit kaum vergleichbar. Erst recht ist die Gefährdung der Funktionsfähigkeit der (heute sogar globalen) Infrastruktur und der über sie abgewickelten Kommunikationsdienste eine seinerzeit nicht zu bearbeitende Dimension.

Heutiges Schutzrecht muss daher über den Schutz des Persönlichkeitsrechts und anderer Grundrechte hinausgehen. Schutzziel ist auch die Leistungsfähigkeit der informationstechnischen Infrastrukturen für den Austausch von Informationen und die Entwicklung sowie Bereitstellung von Kommunikationsdiensten aller Art. Wichtige Unterziele staatlicher Regulierung sind u. a.:

(1) Nutzungsermöglichung: Die Bürger müssen in der Lage sein, die neuen kommunikationstechnischen Möglichkeiten zu nutzen; dies sichert die Rechtsordnung einerseits durch Vorkehrungen über die Zugänglichkeit von Infrastrukturen für die dort verfügbaren Dienste, aber auch durch einen rechtlichen Rahmen der Nutzung, der die Wahrung der jeweils betroffenen Interessen und in Kollisionsfällen einen Interessenausgleich ermöglicht.

(2) Schutzermöglichung: Durch Ausbau von Selbstschutzmöglichkeiten und Schaffung der rechtlichen Voraussetzungen für selbstbestimmtes Handeln (etwa durch Anforderungen an die Einwilligung in die Fremdnutzung von Daten) müssen die Bürger in die Lage versetzt werden, ihre geschützten Interessen selbst zu wahren. Soweit entsprechender Selbstschutz zumutbar ist, dürfen staatliche Schutzvorkehrungen zurückgeschraubt werden.

(3) Abwehr von ungerechtfertigten Beeinträchtigungen: In grundrechtlich geschützten Bereichen sind die rechtsstaatlichen Sicherungen für staatliche Eingriffe umzusetzen und es ist im Rahmen mittelbarer Drittwirkung der Grundrechte dafür zu sorgen, dass Einwirkungen, insbesondere mögliche Beeinträchtigungen, durch Dritte die grundrechtlichen Ausstrahlungswirkungen respektieren.. Dies muss durch Möglichkeiten effektiven Rechtsschutzes ergänzend gesichert werden.

(4) Mitwirkung an der Sicherung der Funktionsfähigkeit der Kommunikationsinfrastruktur, und zwar auch hinsichtlich ihrer globalen Dimension: Hinzuwirken ist im Rahmen des rechtlich und praktisch Möglichen auch darauf, dass die globale Infrastruktur funktioniert und mit den in Deutschland maßgebenden normativen Orientierungen kompatibel eingerichtet und betrieben wird. Dazu gehören selbstverständlich auch, die Vertraulichkeit und Integrität der übermittelten und der bei den Nutzungsvorgängen anfallenden personenbezogenen Daten auch im globalen Kontext zu sichern und diese insbesondere vor Missbrauch zu schützen. Der Schutzbedarf ist allerdings nicht auf personenbezogene Daten begrenzt.

Der durch solche Regulierungen wahrzunehmende Schutzauftrag betrifft nicht nur die Ausgestaltung von Eingriffsermächtigungen des Staates und von Schutzanforderungen gegen Beeinträchtigungen durch Private. Er bezieht sich auf die Ausgestaltung von informationstechnischen Infrastrukturen auch insoweit, als der Staat sie für seine Aufgabenerfüllung und entsprechende Dienste nutzt[82] und dabei etwa Maßnahmen der IT-Sicherheit ergreift.[83] Der Staat kann auch durch Förderung – etwa F&E-Maßnahmen – auf das Design von Infrastrukturen oder die Art der abgewickelten Dienste so Einfluss zu nehmen suchen, dass Schutzziele verwirklicht werden. Richtet der Staat im

---

82 Zur Bedeutung des Umgangs mit (persönlichkeitsbezogenen) Daten und Informationen als Komponente des modernen Verwaltungsrechts s. *Albers* (Fn. 18), Rn. 169.

83 S. dazu *Heckmann* (Fn.69), insbesondere S. 143 ff. S. auch *T. Dreier/R. Vogel*, Software- und Computerrecht, 2008, S. 314 ff. S. auch (allgemein) *B. Holznagel*, Recht der IT-Sicherheit, 2003.

Bereich des E-Government Informations- und Entscheidungsstrukturen unter Nutzung elektronischer Kommunikation ein und stellt er entsprechende Dienste bereit, gehört es zu seinen Aufgaben, die Voraussetzungen auch dafür zu schaffen, dass das E-Government für die Aufgabenerfüllung leistungsfähig ist (etwa Vertrauen "verdient"), also nicht nur, dass es Persönlichkeitsschutz gewährleistet. Aber auch die sonstige vom Staat ausgehende elektronische Kommunikation, auch die Generierung und Verarbeitung sowie die Weitergabe von Daten an andere Stellen, muss von einem Schutzmantel umgeben sein.

Nur als Hinweis erwähnt sei, dass Anknüpfungsmöglichkeiten für die Wahrnehmung von Schutzaufgaben schon in vielen Teilen der Rechtsordnung bestehen. So führt die elektronisch vernetzte Kommunikation weiterhin zu vielen"alten Fragen". Diese können zum Teil mit traditionellen Konzepten bewältigt werden, so etwa mit dem Datenschutzrecht oder dem Rückgriff auf sonstige rechtsstaatliche Grenzen persönlichkeitserheblicher Eingriffe, etwa im präventiven oder repressiven Sicherheitsrecht. Traditionelle Konzepte werden zum Teil aber zu überdenken sein. So wird das Datenschutzrecht über die Orientierung am Persönlichkeitsschutz hinaus gehen müssen und dabei auch um Kommunikations- und Diensteschutzrecht zu ergänzen sein. Das Recht geistigen Eigentums wird im Hinblick auf Prozesse und Ergebnisse kollektiver Wissensgenerierung modifiziert werden müssen. Das Telemedienrecht wird angemessene Antworten auf die Risiken durch Service-Plattformen u. ä. entwickeln müssen usw.

V. Inter- und transnationale Schutzaufgaben

Die Aufgabe des Schutzes der für individuelles, gesellschaftliches und staatliches Verhalten konkret genutzten informationstechnischen Systeme ist nur ein Ausschnitt aus der Aufgabe, die Kommunikationsinfrastruktur auch in ihrer globalen Dimension funktionsfähig zu halten. Bei dieser Aufgabe zeigen sich zusätzliche praktische Grenzen effektiven Schutzes durch die territoriale Beschränkung der staatlichen Handlungsmacht. Erschwerend für Regulierung wirkt auch, dass die informationstechnischen Infrastrukturen und Kommunikationsdienste mit nur begrenzter staatlicher Beteiligung entstanden sind und weitgehend in privater Regie betrieben werden. Ihre Funktionsweise

beruht in weiten Teilen auf der Idee der gesellschaftlichen Selbstregulierung, die von einem Selbstverständnis der Akteure getragen ist, das staatliche Verantwortung möglichst zurückdrängt. Daher stellen sich Fragen effektiver hoheitlicher Regulierung von Selbstregulierung.[84]

Wegen der Dominanz privater global players bei der Gestaltung der Infrastrukturen und der Dienste und damit auch deren Potenzial zur Beeinflussung von Freiheitsausübung und von gesellschaftlichen Problemlösungen bedarf es des Einsatzes des Staates als eines Trägers von Gegenmacht, um die Berücksichtigung von Interessen zu ermöglichen, deren Schutz durch privatwirtschaftlich gesteuertes Kalkül nicht gesichert ist. Die miteinander konkurrierenden privaten Akteure mögen zwar im Einzelfall jeweils gegenläufige Interessen verfolgen und dadurch auch eine gewisse Austarierung unterschiedlicher Interessen befördern. Sie eint aber das Interesse an der größtmöglichen Nutzung der Ertragspotenziale der Netze und Dienste. Dies ist mit dem Risiko verbunden, dass gegenläufige Interessen zu kurz kommen. Aber auch im Übrigen ist staatlich verantwortetes Handeln wichtig, etwa zur Förderung der Rechtssicherheit bei der Inanspruchnahme IT-gestützter Dienste oder der Gewährleistung von Rechtsverbindlichkeit.

Der Aufgabe, in einem weitgehend gesellschaftlicher Selbstregulierung überlassenen Feld auch gegenläufigen Gemeinwohlinteressen Verwirklichungschancen zu ermöglichen, können die Staaten sich im jeweiligen nationalen Bereich stellen, hier etwa, indem sie ihre Nachfragemacht hinsichtlich informationstechnischer Leistungen oder ihre Regelungsmacht über Telekommunikationsnetze nutzen und gegebenenfalls weiter ausbauen sowie die hinsichtlich der Dienste gegebenen Ansatzmöglichkeiten – etwa bei der Providerverantwortlichkeit[85] oder der AGB-Kontrolle – aufgabenspezifisch ausgestalten und für Implementierung sorgen. Die Aufgabe kann und muss aber auch auf den trans- und internationalen Handlungsebenen bewältigt werden, etwa über völkerrechtliche Verträge sowie unter Nutzung der Handlungsmöglichkeiten

---

84 Einen knappen, auch auf transnationale Selbstregulierung bezogenen Überblick über Konzepte und Schwierigkeiten regulierter Selbstregulierung gibt *A. Büllesbach*, Transnationalität und Datenschutz, 2008, S. 95 ff. m.w.Hinw.

85 Zur gegenwärtigen Providerhaftung (insbesondere nach § 7 ff. TMG) s. statt vieler die Überblicke in *Köhler/Arndt/Fetzer* (Fn. 3), Rn. 742 ff.; *Dreier/Vogel* (Fn. 83), S. 299 ff.

in internationalen Organisationen und supranationalen Einrichtungen. In europarechtlichen[86] und internationalen Kontexten werden die Vertreter der Bundesrepublik daher darauf hinzuwirken haben, dass die verfassungsrechtlichen Anforderungen des Grundrechtsschutzes[87] und deren programmatische Orientierungen gewahrt sowie die übergreifenden Aufgaben des Infrastrukturschutzes wahrgenommen werden. Da die Sensibilität für die vorliegend behandelten Fragen nicht in allen Gesellschaften, auch nicht in allen Mitgliedsstaaten der EU, ähnlich ausgeprägt ist wie in Deutschland, sind hier allerdings schwierige praktische Abstimmungsfragen zu bewältigen und es ist Überzeugungsarbeit zu leisten.

Bei der Erfüllung der Gewährleistungsaufgabe wird zu klären sein, wieweit private ("transnationale") Normenordnungen[88] – bisher etwa die sog. lex informatica im Internetrecht oder speziell Verhaltenskodizes[89] - ausreichen und durch staatliches oder suprastaatliches Recht beeinflusst werden können.[90]

Einflussnahmen durch die in öffentlicher Verantwortung stehenden Handlungsträger sind insbesondere möglich, soweit die einschlägigen "privat verantworteten" Regelsysteme auch auf staatliches Recht angewiesen sind oder dieses jedenfalls ergänzend nutzen. Das scheint in erheblich größerem

---

86 Zu den inter- und europarechtlichen Dimensionen – hier des Datenschutzes allgemein – s. *Schnabel* (Fn. 8), S. 42 ff. sowie – speziell zum Europarecht – *Albers* (Fn. 18), Rn. 39 ff.; *G. Britz*, Europäisierung des grundrechtlichen Datenschutzes?, EuGRZ 2009, S. 1 ff.

87 Obwohl die Ausführungen einer einzelnen Entscheidung eines nationalen Gerichts auf die nationale und internationale Kommunikationsordnung begrenzt sind, kann die Herausarbeitung des neuen Leitbildes durch das BVerfG in E 120, 274 auch international gewisse Vorbildfunktion haben (auch im Rahmen von Art. 8 EMRK – dazu s. *R. Uerpmann-Wittzack*, Der Schutz informationstechnischer Systeme nach der Europäischen Menschenrechtskonvention, in: Uerpmann-Wittzack (Fn. 59), S. 99 ff. – und Art. 8 Abs. 1 Grundrechtecharta) – zumal die BVerfG-Entscheidung auch international starke Aufmerksamkeit fand.

88 Regeln oder gar Recht gibt es im transnationalen Bereich, aber vor allem aufgestellt und verwaltet in "privater" Verantwortung, etwa als sog. lex informatica. Zur Selbstproduktion von Regeln durch global players vgl. etwa die "klassische" Untersuchung von *G. Teubner*, Globale Bukowina, Rechtshistorisches Journal 15 (1996), 255 ff. sowie *G.-P. Calliess*, Systemtheorie: Luhmann/Teubner, in: *S. Buckel/R. Christensen/A. Fischer-Lescano* (Hrsg.), Neue Theorien des Rechts, 2006, 57, 71 ff.; *M. Neves*, Transversale Rechtsvernetzung und Asymmetrien der Rechtsform in der Weltgesellschaft, in: Festschrift für Teubner, 2009, S. 841 ff.; *H. Willke*, Das Recht der Weltgesellschaft, in: Festschrift für Teubner, S. 887 ff.; detailreich und – zu Recht – relativierend *N. C. Ipsen*, Private Normenordnungen als transnationales Recht?, 2009.

89 Zu Binding Corporate Rules speziell in Datenschutzbereich s. *Büllesbach* (Fn. 84), S. 131 ff.

90 Hierzu s. – mit vielen Nachw. – *Ipsen* (Fn. 88), S. 104 ff.

Maße der Fall zu sein als in der Literatur meist angenommen wird.[91] Auch in dem Feld sog. transnationalen Rechts stehen private und staatliche Regelungen nebeneinander.[92] Zum Teil sind private Normensysteme nur Platzhalter in einer Übergangsphase, bevor hoheitlich verantwortetes Recht bestimmend wird.[93] Vor allem aber bedürfen auch private Normen vielfältig der Verzahnung mit staatlichem Recht oder sie sind zumindest auf eine hoheitlich verantwortete Auffangordnung angewiesen. Auch werden aus staatlich verantworteten nationalen oder internationalen Ordnungen häufig Prinzipien privater Streitbewältigung abgeleitet, Rechtsinstitute entlehnt und in private Regelsysteme auf unterschiedlichen Wegen integriert[94] oder es wird die staatliche Rechtsordnung als eine Art "Ausfallbürge" zur Rechtsdurchsetzung genutzt. Das zunächst für das staatliche Recht entwickelte Konzept einer Gewährleistungsverantwortung des Staates bei der Erfüllung von gemeinwohlrelevanten Aufgaben durch Private[95] und Konzepte zum Wechselverhältnis von gesellschaftlicher Selbstregulierung und staatlicher Regulierung sowie insbesondere Überlegungen zur Zuordnung unterschiedlicher Regelsysteme als wechselseitig nutzbaren Auffangordnungen[96] finden auch im transnationalen Bereich ihre Rechtfertigung. Das Recht der Kommunikations-Infrastrukturen und -dienste kann Pionierfunktion bei der Verknüpfung nationaler, internationaler und transnationaler Regelsysteme Privater und solcher hoheitlicher Provenienz sowie bei der Entwicklung darauf ausgerichteter rechtlicher Handlungsformen übernehmen.

Der Schutz der Funktionsfähigkeit der elektronisch vernetzten Kommunikation ist eine Gemeinwohlaufgabe, für deren Erfüllung neben Privaten auch Akteure unverzichtbar sind, die strukturell darauf eingerichtet sind, die verschiedenen in den Gesellschaften relevanten Interessen wahrzunehmen und ihre angemessene Berücksichtigung ausgleichend zu

---

91 S. dazu – mit Belegen auch zur gegenläufigen Auffassung – *Ipsen* (Fn. 88), S. 104 ff., 108 ff., 126 f.

92 Zur Zunahme staatlicher Regulierung in der globalen Informationsgesellschaft s. *Roßnagel* (Fn. 20), S. 425 ff. Vgl. auch *Ipsen* (Fn. 88), S. 212 ff.

93 So die These von *Ipsen* (Fn. 88), S. 211 f.

94 Dazu s. *Ipsen* (Fn. 88), S. 232 ff.

95 S. o. Fn. 2.

96 Zu diesem Konzept s. die Beiträge in *W. Hoffmann-Riem/E. Schmidt-Aßmann* (Hrsg.), Öffentliches Recht und Privatrecht als wechselseitige Auffangordnungen, 1996.

gewährleisten. Aufgerufen sind die Staaten, auch im trans- und internationalen Handlungsverbund Vorsorge dafür zu schaffen, dass Dysfunktionalitäten im globalisierten Kommunikationssystem nicht entstehen und dadurch Defizite und Krisen vermieden werden, deren Bewältigung – wie die der Finanzkrise – erheblich mehr staatliche Intervention erfordern würde als die rechtzeitige Vorsorge.