Erster Teil: Die Rechte des Individuums

Freiheit und Freiheiten

Die einschlägigen Grundrechte

Die Rechtslage des Individuums in der „Informationsgesellschaft" wird heute regelmäßig zunächst unter dem Aspekt des Datenschutzes und seiner Bedrohung erörtert. Es ist aber angebracht, zuerst *alle* in Frage kommenden Rechte des Einzelnen zu behandeln; von ihnen aus können und müssen dann die Risiken und Bedrohungen angesprochen werden, und von ihnen aus sind auch Grenzen der Freiheit zu bestimmen. In diesem Sinne also als erste Feststellung: Der Einzelne hat *subjektive Rechte*, die ihm kraft Verfassung oder sogar kraft internationalen Rechts zustehen; diese Rechte gelten auch, wenn wir uns ins Internet begeben und dort an Informations- und Meinungsaustausch teilnehmen.

Im Prinzip gilt für die Kommunikationsvorgänge im Netz, was auch für den Austausch außerhalb des Netzes gilt: Die in Art. 5 Abs. 1 GG gewährleisteten Grundrechte der Meinungs-, Presse- und Rundfunkfreiheit sind hier wie dort die Bastionen der politischen Freiheit, aber auch die zensurfreien (Art. 5 Abs. 1 Satz 3 GG!) Tore für Spiel und Unterhaltung. Die Meinungsfreiheit umfasst nach der Rechtsprechung des Bundesverfassungsgerichts nicht nur „Werturteile", sondern auch die Freiheit, wahre (!) Tatsachenbehauptungen zu verbreiten.[52] Dem Internetnutzer, der sich nur informieren will, steht das ebenfalls in Art. 5 Abs. 1 GG garantierte Recht zur Seite, „sich aus allgemein zugänglichen Quellen ungehindert zu unterrichten". Die Pressefreiheit und „die Freiheit der Berichterstattung durch Rundfunk und Film" werden weit ausgelegt und von manchen Autoren schlicht als „Medienfreiheit" bezeichnet. Dagegen ist nichts einzuwenden. Soweit allerdings eine „Freiheit der Internetdienste" angenommen wird,[53] ist dies zumindest missverständlich, denn „die Dienste" sind keine Akteure wie die Zeitungsverlage und Fernsehunternehmen; hinter ihnen stehen zunächst einmal natürliche oder juristische Personen, die ihre unternehmerische Freiheit nutzen (und deren Schranken beachten müssen, die sich von denen der Medienunternehmen unterscheiden können). Überzeugender ist es, für allgemeine Aussagen die Grundform der einschlägigen Freiheitsrechte zugrunde zu legen, also auf das Recht zur unge-

52 Vgl. u.a. BVerfGE 54, 208 (219); 61, 1 (7 f.); 85, 1 (14 f.);
53 Spindler 2012, S. 28 mit Nachweisen in Fn. 127. Dagegen u.a. Dix, in: DJT 2012, S. 72 These 13.

hinderten Äußerung und Verbreitung von Meinungen und wahren Tatsachen abzustellen. Diese Rechte können als „Äußerungs- und Kommunikationsfreiheit" zusammengefasst werden.

Freiheit im Netz

Das Internet kann aber ebenso wenig ein „rechtsfreier Raum" sein wie die übrige Welt. Die Rechte des Art. 5 Abs. 1 GG „finden ihre Schranken in den Vorschriften der allgemeinen Gesetze, den gesetzlichen Bestimmungen zum Schutze der Jugend und in dem Recht der persönlichen Ehre" (Art. 5 Abs. 2 GG). „Allgemeine Gesetze" sind solche, die nicht gegen die Meinungsfreiheit als solche gerichtet sind, sondern ohne Rücksicht auf die Meinungsäußerung andere Rechtsgüter schützen sollen. Zu den „allgemeinen Gesetzen" zählen u.a. die Bestimmungen des Zivilrechts zum Schutze materieller und immaterieller Güter anderer und das Recht des „geistigen Eigentums". Meinungsfreiheit soll dazu beitragen, dass geistiger Austausch und Auseinandersetzung möglich sind; das Grundgesetz unterscheidet auch nicht zwischen „wertvollen" und „wertlosen" oder „richtigen" und „falschen" Meinungen. Aber Meinungsfreiheit rechtfertigt es nicht, andere zu belästigen, zu beschimpfen oder durch unwahre Behauptungen in ihrer beruflichen oder gewerblichen Betätigung zu schädigen. Die Meinungsfreiheit der einen kollidiert oft mit dem Anspruch der anderen auf Privatsphäre und Persönlichkeitsschutz; in zahllosen Fällen war eine schwierige Abwägung nötig – was zu vielen Gerichtsentscheidungen über heikle Einzelfälle geführt hat. Die bekanntesten sind die Urteile höchster Gerichte (bis hin zum Europäischen Gerichtshof für Menschenrechte) in Sachen Caroline von Monaco gegen die Boulevardpresse). Schon bevor der Gedanke des Datenschutzes aufkam, ist auf diese Weise ein liberales System des „Äußerungsrechts" entstanden.[54]

Ohne solche Schranken wäre das Miteinander der Menschen oft unerträglich. Gerichte und Rechtwissenschaft haben die Schranken ihrerseits so ausgestaltet, dass sie das Grundrecht nicht in seinem Kern beschädigen. Berühmt ist die Definition der „allgemeinen Gesetze" durch das Bundesverfassungsgericht: Das sind solche, „die sich nicht gegen die Äußerung einer Meinung als solche richten, die vielmehr dem Schutz eines schlechthin, ohne Rücksicht auf eine bestimmte Meinung, zu schützenden Rechtsgutes dienen". Die „allgemeinen Gesetze" müssen „im

54 S. unten S. 51 ff..

Lichte der besonderen Bedeutung des Grundrechts der freien Meinungsäußerung für den freiheitlichen demokratischen Staat ausgelegt werden".[55]

Eines besonderen Grundrechts für die Kommunikation bedarf es daher nicht, und wenn dieses als schrankenlos verstanden würde, wäre es mit dem Grundgesetz nicht vereinbar. Die Forderung nach „Freiheit im Netz" kann allenfalls als ein Argument dazu dienen, die Handlungs- und Äußerungsfreiheit des Individuums (und die unternehmerischen Grundrechte der Betreiber) nicht zu eng zu begrenzen. Schwer vorstellbar, aber immerhin möglich ist es freilich, dass sich eines Tages die Meinung durchsetzt, man dürfe im Internet Dinge sagen, die unter Anwesenden nicht geduldet werden – das wäre dann ein Beispiel für eine neue Freiheit *im Netz*, aber keines für die Freiheit *des Netzes* vom Recht.

Als „allgemeines Gesetz", das die Freiheitsrechte des Art. 5 Abs. 1 GG einschränkt, ist im Jahre 1977 das Bundesdatenschutzgesetz (BDSG) mit seinen Regelungen über den richtigen Umgang mit Informationen hinzugekommen. Es will die Meinungs- und Medienfreiheit nicht einschränken, aber es kann faktisch zu erheblichen Einschränkungen oder zumindest Erschwerungen führen. Wer personenbezogene Daten Dritter in das Netz einstellt – und das geschieht in den sozialen Netzwerken, aber auch in anderen Teilen des Internet ständig –, speichert und übermittelt diese Daten, was nach der Grundvorschrift des BDSG (§ 4 Abs. 1) nur zulässig ist, „soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat". Die Einwilligung fehlt in zahllosen Fällen, und nach einer passenden Rechtsvorschrift wird man vergeblich suchen: Es gibt keine ausdrückliche Norm, die eine solche Erlaubnis oder Anordnung enthält. (Und falls jemand meinen sollte, die Erlaubnis ergebe sich aus dem Äußerungs- und Kommunikationsgrundrecht, so läge daran ein Zirkelschluss; denn dieses Grundrecht ist eben keine Erlaubnisnorm, sondern der Maßstab, an dem das Datenschutzgesetz als „allgemeines Gesetz" im Sinne von Art. 5 Abs. 2 GG gemessen werden muss). Man könnte allenfalls erwägen, dass Art. 5 Abs. 1 GG es erforderlich mache, einen Erlaubnistatbestand für Veröffentlichungen im Internet zu beschließen. Denn die gegenwärtige Rechtslage ist geradezu peinlich: Während es jedem frei steht, offline (wahre) Behauptungen über andere zu verbreiten, muss derselbe Vorgang, wenn das Internet als Transportmedium genutzt wird, vor dem BDSG gerechtfertigt werden, und unter Umständen kann eine Datenschutzauf-

55 BVerfGE 7, 198 (209); 62, 230 (244); 71, 162 (175); 85, 1 (16 f.). Das erstgenannte Urteil erging in einem Aufsehen erregenden Fall: Der Leiter der Hamburger Staatlichen Pressestelle, Erich Lüth, hatte zum Boykott eines Filmes von Veit Harlan, dem Regisseur von „Jud Süß" und anderen Propagandafilmen der Nazis, aufgerufen; nach bisherigem Recht lag darin ein Verstoß gegen das „allgemeine Gesetz", das die Schädigung Dritter verbietet (§ 826 BGB). Das BVerfG legte Art. 5 Abs. 2 GG so aus, dass der Meinungsfreiheit im konkreten Fall der Vorrang vor dem Zivilrecht zukam.

sichtsbehörde ihn verbieten oder reglementieren; hinzu kommen Unterrichtungs- und Auskunftspflichten gegenüber den Betroffenen.

Um dergleichen „bürokratische" Hindernisse auszuräumen, ist der Journalismus von vornherein vom Datenschutz ausgenommen worden. Das BDSG schreibt den Ländern vor, in ihren Gesetzen dafür zu sorgen, dass die „Unternehmen und Hilfsunternehmen der Presse" bei journalistischer Betätigung vom Datenschutz weitgehend freigestellt sind: In diesem Bereich gelten nur einige wenige Vorschriften (über das „Datengeheimnis" und den technischen und organisatorischen Datenschutz) (§ 41 BDSG). Wer aber ohne „journalistisch-redaktionelle oder literarische Zwecke" Informationen sammelt und verwendet, soll sich dafür nach den Regeln des Datenschutzrechts rechtfertigen müssen? Um auch das zu verhindern, halten manche es für angebracht, neben dem „Medienprivileg" auch ein „Laienprivileg" zu behaupten, das die Veröffentlichung von Tatsachen und Meinungen durch Nicht-Journalisten gegen Forderungen des Datenschutzes abschirmt.[56] Dafür spricht, dass die Äußerungsfreiheit nicht auf die Medien beschränkt ist; sie steht jedem und jeder zu. Ob aber wirklich die rechtliche Gleichstellung von Journalismus und Laienkommunikation geboten ist, kann mit gutem Grund bezweifelt werden.

Die *passive* Freiheit im Netz, das Suchen nach Informationen und Unterhaltung, ist selbstverständlich ebenfalls erlaubt und muss erlaubt bleiben, und solange dadurch niemandes Rechte berührt werden, darf und sollte das Surfen im Netz unbeobachtet geschehen. Wer nur lesen oder hören will, braucht seinen Namen nicht anzugeben. Die Diensteanbieter müssen diesen Wunsch nach Anonymität beachten.[57] In diesem Zusammenhang fordert der Berliner Datenschutzbeauftragte Alexander Dix, ein „Mediennutzungsgeheimnis" ausdrücklich festzulegen[58]– aber nur für den passiven Nutzer. Mit Recht betont Dix die Verantwortlichkeit der aktiven Nutzer: „Wer … aktiv Informationen im Netz veröffentlicht, sollte dies in pseudonymer Form (oder unter Klarnamen) tun müssen. Nur so können Datenschutz- und andere Rechtsverstöße verfolgt werden".[59]

Übrigens darf auch der Staat durch seine Behörden die „Freiheit" des Internets nutzen und sich mit allgemein zugänglichen Informationen bedienen. Das hat das

56 Christoph Fiedler auf der Datenschutz-Konferenz des BMI und des Humboldt-Instituts für Internet und Gesellschaft, Berlin 17./18.10.2012 (unveröff.).

57 Vgl. Telemediengesetz (TMG) § 13 Abs. 6: „Der Diensteanbieter hat die Nutzung von Telemedien und ihre Bezahlung anonym oder unter Pseudonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist. Der Nutzer ist über diese Möglichkeit zu informieren".

58 DJT 2012, S. 71 These 8.

59 DJT 2012, S. 71 These 8. Diensteanbieter sind nach § 7 Abs. 1 TMG „für eigene Informationen, die sie zur Nutzung bereithalten, nach den allgemeinen Gesetzen verantwortlich", aber nach Abs. 2 dieser Vorschrift bei der Durchleitung oder Zwischenspeicherung fremder Informationen „nicht verpflichtet, die von ihnen übermittelten oder gespeicherten Informationen zu überwachen oder nach Umständen zu forschen, die auf eine rechtswidrige Tätigkeit hinweisen". Dazu auch §§ 8-10 TMG.

Bundesverfassungsgericht in dem Urteil über die Online-Durchsuchung privater Computer ausgesprochen, war also insofern weniger behördenkritisch.[60] Nicht erlaubt ist es danach aber, dass eine staatliche Stelle „sich unter einer Legende in eine Kommunikationsbeziehung zu einem Grundrechtsträger begibt" und dabei „ein schutzwürdiges Vertrauen des Betroffenen in die Identität und die Motivation seines Kommunikationspartners ausnutzt, um persönliche Informationen zu erheben, die sie sonst nicht erhalten würde".[61] Der behördliche Internetsurfer wird hier mit einem verdeckten Ermittler gleichgestellt, der sich das Vertrauen von Kriminellen erschlichen hat – ein Vergleich, der mit der üblichen Anonymität der Internetnutzung nicht ganz vereinbar ist. Das Gericht schickt selbst die Bemerkung nach, dass im Internet normalerweise kein Vertrauen aufgebaut wird, also auch nicht enttäuscht werden kann; man kennt ja die Identität der Partner meist nicht und kann sie nicht überprüfen.

Informationsfreiheit versus Geheimsphären

Die Computer-Ethik des CCC sagt: „Private Daten schützen, öffentliche Daten nützen!" Ein eingängiges Motto, nach dem sich der Gesetzgeber schon in der Vergangenheit gerichtet hat: Personenbezogene Daten werden geschützt, Daten der öffentlichen Verwaltung stehen – im Prinzip – jedem zur Verfügung. Leider sieht die Wirklichkeit etwas anders aus als dass die Zweiteilung zweifelsfrei umgesetzt werden könnte. Weder ist eindeutig, was „privat" ist, noch gehören alle vermeintlich „öffentlichen" Daten wirklich der Allgemeinheit. Es lohnt, sich mit diesem Thema näher zu beschäftigen.

Die Freiheit, sich aus allgemein zugänglichen Quellen ungehindert zu informieren, steht im Grundgesetz gleich nach der Meinungsfreiheit (Art. 5 Abs. 1 S. 1 GG). Sie folgt auch aus anderen Freiheitsrechten, z. B. der Berufsfreiheit: Wenn ich einen Beruf richtig ausüben will, muss ich zahllose Kontakte aufbauen und pflegen und deshalb auch Informationen über andere Menschen sammeln und verwerten. Die Informationstechnik hat gewaltige Chancen eröffnet, diese Freiheit tatsächlich zu nutzen, und die Gesetze fördern ihre Wahrnehmung. Denn es gelten

60 BVerfGE 120, 274 Leitsatz 6 und S. 344 ff. Eine Ausnahme macht das Gericht schon an dieser Stelle, indem es hinzufügt, dass „ein Eingriff in das Recht auf informationelle Selbstbestimmung" gegeben sein könne, wenn Informationen aus allgemein zugänglichen Inhalten (also z.B. Webseiten) „gezielt zusammengetragen, gespeichert und gegebenenfalls unter Hinzuziehung weiterer Daten ausgewertet werden und sich dadurch eine besondere Gefahrenlage für die Persönlichkeit des Betroffenen ergibt". Hierfür bedürfe es einer Ermächtigungsgrundlage. Eine salvatorische Klausel, die viele Fragen aufwirft! S. aber auch den BMI-Entwurf zum Persönlichkeitsschutz (unten S. 140); dort wird jedoch auf „Geschäftsmäßigkeit" abgestellt.

61 BVerfGE 120, 274 (345).

heute in vielen Staaten und jedenfalls in Europa Gesetze, die dem Einzelnen das Recht garantieren, sich umfassend zu informieren. Die Behörden sind fast überall verpflichtet, ohne weitere Voraussetzungen jedem, der es wünscht, Einsicht in amtliche Unterlagen zu gewähren. Und über die gesetzlichen Verpflichtungen hinaus stellen heute alle möglichen Unternehmen und Behörden praktische, werbende und schlicht hilfreiche Informationen ins Netz ein; wir profitieren täglich davon. Wenn aber der Informationswunsch des einen mit dem Geheimhaltungswunsch des anderen kollidiert, sind wir wieder bei der Aufgabe, durch Abwägung eine Lösung zu finden.

Freilich sind in den Informationsfreiheitsgesetzen einige Fallgruppen ausgenommen (bei etwas unterschiedlicher Formulierung in den verschiedenen Ländern). Dass personenbezogene Daten, die dem Datenschutz unterliegen, nicht auf diesem Wege offenbart werden dürfen, ist selbstverständlich. Umstritten sind – verständlicher Weise – „Staatsgeheimnisse" und „Geschäftsgeheimnisse". Aber auch diese Vorbehalte standen schon in dem berühmten Freedom of Information Act von 1966, der zur Aufdeckung des Watergate-Skandals beigetragen hat. Die Fans von WikiLeaks und anderen „Offenbarungs"-Plattformen halten diese Schranken für obsolet, weil sie Staaten (Regierungen) und Unternehmen (Managern) nur Schlechtes unterstellen und das Heil von einer vollständigen Transparenz erwarten.

Nach den Informationsfreiheitsgesetzen (IFG) des Bundes und von elf Ländern hat jeder Anspruch darauf, dass die Verwaltung ihm ihre Akten offenlegt und Kopien gestattet. Das widerspricht nur scheinbar dem Datenschutz; denn die personenbezogenen Daten, die in der Verwaltung gespeichert werden, sind von dem Informationsanspruch ausgenommen. Die große Forderung nach Transparenz der Verwaltung ist also im Grunde bereits erfüllt; nur in fünf Bundesländern fehlt noch ein solches Gesetz. Den Katalog der Ausnahmen, der in allen Informationsfreiheitsgesetzen (auch des Auslands) ähnlich ist, finden freilich die „Piraten" aller Art viel zu umfangreich. Wer wie WikiLeaks auch militärische und diplomatische Geheimnisse veröffentlichen oder wer keine Rücksicht auf laufende Gerichtsverfahren nehmen will, dem erscheinen die Grenzen des Informationsanspruchs natürlich als zu eng gezogen. Der Gesetzgeber kann aber gar nicht anders als abzuwägen, welche Interessen der Allgemeinheit den Vorrang vor dem Informationswunsch Einzelner haben, und sei dieser Wunsch noch so gut „demokratisch" begründet. So ist es rechtspolitisch (jedenfalls im Grundsatz) nicht zu beanstanden, dass der Informationsanspruch nach dem Bundesgesetz in einer ganzen Reihe von Fällen nicht besteht, nämlich

„1. wenn das Bekanntwerden der Information nachteilige Auswirkungen haben kann auf

a) internationale Beziehungen,
b) militärische und sonstige sicherheitsempfindliche Belange der Bundeswehr,
c) Belange der inneren oder der äußeren Sicherheit,
d) Kontroll- oder Aufsichtsaufgaben der Finanz-, Wettbewerbs- und Regulierungsbehörden,
e) Angelegenheiten der externen Finanzkontrolle,
f) Maßnahmen zum Schutz vor unerlaubtem Außenwirtschaftsverkehr,
g) die Durchführung eines laufenden Gerichtsverfahrens, den Anspruch einer Person auf ein faires Verfahren oder die Durchführung strafrechtlicher, ordnungswidrigkeitsrechtlicher oder disziplinarischer Ermittlungen,

2. wenn das Bekanntwerden der Information die öffentliche Sicherheit gefährden kann,
3. wenn und solange

a) die notwendige Vertraulichkeit internationaler Verhandlungen oder
b) die Beratungen von Behörden beeinträchtigt werden" usw. (§ 3 IFG).

Das IFG schützt darüber hinaus auch den „behördlichen Entscheidungsprozess" (§ 4), das geistige Eigentum sowie Betriebs- und Geschäftsgeheimnisse (§ 6). Die Beachtung schutzwürdiger Interessen Betroffener – also der Datenschutzaspekt – ist in § 5 IFG noch einmal ausdrücklich und differenziert geregelt

Über die Berechtigung einiger Spezialklauseln lässt sich streiten. Der Gesetzgeber wollte offensichtlich keine irgendwie „gefährliche" Lücke lassen und hat daher manche Ausnahmen doppelt und dreifach festgelegt.[62] Hier wird sich gewiss noch einiges ändern, wenn die Beauftragten für die Informationsfreiheit mehr Fälle untersucht und Korrekturen angemahnt haben. Andererseits sind mehrere dieser Ausnahmen recht aktuell: Man denke nur an den Kampf gegen die Steuerhinterziehung und verbotene Kartelle (Nr. 1 d)) oder gegen die Ausfuhr von Rüstungsgütern in Konfliktzonen (Nr. 1 f)). Transparenz für die „Gegenseite" wäre fatal für das Gemeinwohl. Dass strafrechtliche Ermittlungen oder die Abwehr von Gefahren bei voller Kenntnis der Beschuldigten und Verdächtigen nicht erfolgreich sein können, ist eigentlich selbstverständlich, aber auch in zivilrechtlichen Streitigkeiten und verwaltungsrechtlichen Planungen ist ein gewisses Maß an Beratungsgeheimnis zwingend erforderlich. Insiderwissen verführt in der Wirtschaft immer wieder zu Transaktionen zu Lasten Dritter; in der Verwaltung kann Ähnliches geschehen.

62 Vgl. etwa die Kommentierung von Schoch 2009, insbes. Vorb. zu §§ 3 bis 6, Rn. 29 ff. und Kommentar zu § 3 Rn. 206 ff.

Die Praxis tut sich mit den geltenden Gesetzen schwer; man versucht immer wieder, sie zu unterlaufen. Der Paradigmenwechsel vom Arkanprinzip – alles, was der Staat tut, wird zunächst einmal geheim gehalten – zum Öffentlichkeitsprinzip lässt sich nicht von einem Augenblick zum nächsten bewirken; es genügt nicht, den Hebel umzulegen, man muss auch Dampf machen, um das Schiff der Verwaltung auf den neuen Kurs zu bringen. Und das wird nur gelingen, wenn auch die Einzelheiten und die Ausnahmen klar und allgemein akzeptiert sind. Wer energisch genug nach bestimmten Unterlagen der Verwaltung sucht und notfalls die Gerichte um Hilfe ersucht, der hat durchaus eine Chance, sich gegen Verschleierungsversuche durchzusetzen. Die Gerichte sind zunehmend bereit, der Exekutive Grenzen zu setzen.

Grundrecht auf Internet?

Gibt es auch ein Grundrecht oder gar ein Menschenrecht auf Internet? So wie ein Grundrecht auf Datenschutz in verschiedene Länderverfassungen geschrieben wurde und auch immer wieder als Ergänzung des Grundgesetzes gefordert wird, werden auch Forderungen erhoben, dem Internet verfassungsrechtliche „Weihe" zu vermitteln. Die öffentliche Meinung neigt auch sonst dazu, einmal erreichte Rechtspositionen zu verfestigen und Reformvorschläge dadurch zu untermauern, dass sie als Konsequenz grundrechtlicher Freiheiten dargestellt werden. Daraus lässt sich dann wiederum ableiten, dass diese grundrechtliche Verankerung auch im Text der Verfassung ausdrücklich und speziell festgeschrieben werden müsse. Die Rechtswissenschaft stimmt solchen Forderungen häufig zu.

Das Bundesverfassungsgericht legt der Politik eine derartige Folgerungsweise nahe, indem es den Inhalt der Verfassung in „Leitsätzen" konkretisiert und insbesondere die Reichweite der Grundrechte genauer bestimmt. Seine verfassungsrechtlichen Argumentationen liefern immer wieder Munition für rechtspolitische Forderungen, die auf eine Verbesserung der Rechtsposition des Einzelnen hinauslaufen. Die politischen Kräfte, denen an einer bestimmten verfassungsrechtlichen Festlegung liegt, wollen damit verhindern, dass ein künftiges, anderes zusammengesetztes Parlament das Erreichte wieder rückgängig macht. Solange kein entsprechender Verfassungsrechtssatz gilt, so meinen viele, würde auch dem Verfassungsgericht die Macht zur Korrektur des Gesetzgebers genommen. (Tatsächlich würde das Gericht aber wohl zu entsprechenden Ableitungen aus anderen, allgemeineren Verfassungsnormen gelangen!).

Die populäre Methode der Verfassungspolitik weckt bei den meisten Menschen Vorstellungen und Erwartungen, die entweder schon wegen ihrer Einseitigkeit und Unausgewogenheit nicht realisiert werden können, oder aber solche, die bei ange-

messener Auslegung der Gesetze und der Verfassung auch ohne Verfassungsänderung begründet sind. Unrealistisch sind manche Forderungen, die Befugnisse von Polizei und Justiz so sehr zu reduzieren, dass sich jedermann in der Öffentlichkeit unerkannt bewegen kann.[63] Ein Beispiel für die andere Variante bildet die „Erfindung" des „Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme" durch das Bundesverfassungsgericht. In dem Urteil zur Unzulässigkeit der „Online-Durchsuchung" privater Computer[64] hat das Gericht dieses Recht als eine Ausprägung des allgemeinen Persönlichkeitsrechts bezeichnet, das seinerseits aus dem Grundrecht auf freie Entfaltung der Persönlichkeit (Art. 2 Abs. 1 GG) in Verbindung mit dem Gebot der Achtung der Menschenwürde (Art. 1 Abs. 1 GG) hergeleitet wird. Die „Gewährleistung der Vertraulichkeit und Integrität" wird vielfach als ein „neues" Grundrecht, als eine besondere Form des verfassungsrechtlichen Individualschutzes aufgefasst, obwohl das juristische Ergebnis – Verfassungswidrigkeit des entsprechenden Landesgesetzes – auch ohne den neuen Begriff anerkannt werden müsste.[65] Es ist gewiss zweckmäßig, die Vielfalt der Phänomene durch eine differenzierte Begrifflichkeit zu ordnen, aber für die Betroffenen würde sich nichts ändern, wenn das Gericht die alten, bewährten Vorstellungen vom Persönlichkeitsschutz zugrunde gelegt und weiterentwickelt hätte. Übrigens haben einige Bundesländer ein Grundrecht auf Datenschutz in ihre Verfassungen aufgenommen; es ist nicht erkennbar, dass dort eine höhere Qualität oder Intensität von Datenschutz praktiziert wird als in den anderen Ländern.

Verfassungen sollen eigentlich kurz und knapp formuliert sein; sie sollen nicht Einzelfälle regeln, sondern nur die Grundstrukturen der Staatsorganisation und die Kernpositionen des Verhältnisses zwischen Staat und Individuen. Tatsächlich gehen viele Verfassungen weit über diese Grenzen hinaus, geben der Politik inhaltliche Richtlinien und versprechen den Einzelnen auch Schutz gegen gesellschaftliche Mächte. Damit prägen sie die Identität des Gemeinwesens und fördern – jedenfalls potentiell – die Integration der Menschen in den gemeinsamen Verband.

Aber eine Verfassung soll auch entwicklungsoffen sein; „sie muss politischen und gesellschaftlichen Akteuren Freiräume zu ihrer Entfaltung lassen, um dadurch Vielfalt zu sichern".[66] Auch aus diesem Grunde enthalten die Verfassungen viele relativ unbestimmte Formulierungen, die auf politischen Kompromissen beruhen und unterschiedlichen Interpretationen Raum lassen. Das bekannteste Beispiel der verfassungsrechtlichen Fixierung eines politischen Kompromisses ist der heutige Artikel 16 a des Grundgesetzes, der das Recht auf politisches Asyl – ursprünglich

63 In diese Richtung geht die „Verteidigung der Privaten" durch den Soziologen Wolfgang Sofsky (Sofsky 2007).
64 Urteil vom 20. Februar 2008, BVerfGE 120, 274
65 Zur juristischen Debatte vgl. u.a. Hoffmann-Riem 2009, S. 530 ff.; anders Bull 2011 a S. 34 f.
66 Voßkuhle 2011, S. XI/XII.

ein kurzer Satz in Artikel 16: „Politisch Verfolgte genießen Asylrecht“ – in vier umfangreichen Absätzen durch ein kompliziertes System von Detailregelungen, Ausnahmen und Gegenausnahmen ergänzt. Die Absicht, das Asylrecht vor der Abschaffung zu bewahren, ist verwirklicht worden, aber ob der Geist des alten Asylrechtssatzes, der als Einleitungssatz in Art. 16 a GG fortbesteht, erhalten worden ist, erscheint durchaus fraglich.

Kurz: Man darf von Verfassungsänderungen nicht zu viel erhoffen. Sie stellen in aller Regel den Abschluss einer Entwicklung dar, nicht deren Anfang (ausgenommen vielleicht so explizit zukunftsgerichtete Normen wie der Umweltschutz-Artikel 20 a des Grundgesetzes). Wenn die parlamentarischen Mehrheiten nicht ausreichen, um eine progressive Politik zu betreiben, hilft zwar unter günstigen Umständen das Bundesverfassungsgericht, aber auch dieses kann keine wirklichen Kehrtwendungen erzwingen.

Unter diesen Aspekten sind auch die Überlegungen zur verfassungsrechtlichen Verstärkung des Internets zu beurteilen. Soweit bloß plakativ von der „Freiheit *des* Internets“ gesprochen wird, ist schon unklar, wer denn da „frei“ sein soll; das Internet ist kein Zurechnungssubjekt, das Rechte oder Pflichten haben kann. Das Netz ist „stets nur Mittel zum Zweck“ (der freien Kommunikation) und steht eben deshalb nicht mit dem Kommunikationsgrundrecht auf gleicher Ebene.[67] Ein Anspruch auf *Zugang zum* Internet ist immerhin vorstellbar, und es wird berichtet, dass bereits ein großer Teil der Bevölkerung diesen Zugang für ein Grundrecht hält.[68] Gemeint ist aber auch ein Recht auf „freie Entfaltung *im* Internet“ und vor allem auf Abwehr aller staatlichen Eingriffe in die Nutzung des Internets.[69] Ohne dass das Grundgesetz geändert werden müsste, ist schon jetzt ein starkes „Recht auf Internet“ gesichert – nicht als Anspruch eines jeden Menschen auf unentgeltlichen Zugang zum jeweils modernsten weltweiten Netz und nicht als Recht auf beliebige Äußerungen im Netz, wohl aber als eine Pflicht des Staates zur Gewährleistung einer ausreichenden Infrastruktur und – im Rahmen des Möglichen – als gesetzlicher Anspruch des Einzelnen auf diskriminierungsfreie *Teilhabe* an dieser Infrastruktur, vor allem aber als verfassungsrechtliches *Abwehrrecht* gegen Einschränkungen der Meinungs-, Medien-, Kunst- und Wissenschaftsfreiheit.[70] Kai von Lewinski hat in aller wünschenswerten Klarheit herausgearbeitet, dass es keiner verfassungsrechtlichen „Operation“ (in Gestalt einer Verfassungsänderung)

67 So Hofmann 2012 in einem Bericht über einen Meinungsstreit in der New York Times.
68 Lewinski 2011, S. 70 Fn. 1 m.w.N.
69 Der Gutachter des DJT versteht „Internetfreiheit“ als ein „Institutsgrundrecht“ ähnlich der Presse- und Rundfunkfreiheit: „Sich Äußernde im Internet und erst recht Intermediäre“ müssten „sich auf die Institutsgrundrechte, insbesondere das der ‚elektronischen‘ Presse berufen können“ (Spindler 2012, S. 27 und 133).
70 Weitergehend fordert z.B. Spindler eine „allgemeine Freiheit der Internetdienste“ (Spindler 2011, S. 28), während Dix für eine Erweiterung der Medienfreiheiten nach Art. 5 GG „keinen Anlass“ sieht (in: DJT 2012, S. 72 These 13.

bedarf, um die vermeintlichen Lücken im Grundgesetz zu schließen, sondern dass zur Korrektur der altersbedingten „Kurzsichtigkeit" unserer Verfassung eine „gesetzliche Sehhilfe" genügt: „Dem ‚Recht auf Internet' ist mittelfristig am besten gedient, wenn man die Interpretationsspielräume des Grundgesetzes nutzt".[71] „Das bloße textliche Einfügen eines ‚Rechts auf Internet" ist (politische) Geschmacksfrage".[72] Die Einführung einer *Universaldienstleistungspflicht* (also der von der Bundesnetzagentur festgelegten Pflicht eines Unternehmens, in einem bestimmten Gebiet für technisch hochwertige Verbindungen zu sorgen)[73], wie sie z.B. von der SPD vorgeschlagen wird, dürfte praktisch bedeutsamer und effektiver sein als die Diskussion über ein neues Grundrecht.

Wenn demgegenüber eingewandt wird, nur eine ausdrückliche verfassungsrechtliche Verankerung der Internet-Freiheit sei eine ausreichende Bastion gegen Unterdrückungsabsichten der Regierungen, so ist zu entgegnen: Gegen rechtsfeindliche Bestrebungen von Regierenden kommt kein Verfassungstext an. Die Geschichte liefert bis zum heutigen Tag genügend Beispiele dafür, wie rücksichtlos Machthaber mit Verfassungen umgehen, wenn sie ihren Absichten im Wege stehen.[74] Auch wenn das Bundesverfassungsgericht die politischen Mehrheiten in wichtigen Fällen mit Erfolg korrigiert hat – der Gesetzgeber könnte mit verfassungsändernder Mehrheit auch diese Urteile korrigieren. In wirklich entscheidenden Machtproben hängt die Verteidigung der rechtsstaatlichen Grundwerte ohnehin davon ab, dass das Volk selbst sich zur Wehr setzt und die Medien den Mut aufbringen, den Mächtigen zu widersprechen. Solange die Demokratie funktioniert, wird uns diese Probe erspart bleiben.

Das vermeintliche Ende der Privatheit

Niemand will für seine Umgebung ein „offenes Buch" sein, jeder und jede will seine und ihre Geheimnisse für sich behalten. Deshalb will auch niemand für andere „transparent" sein; kein anderer Mensch soll ihm oder ihr in die Seele schauen können. Wir sträuben uns instinktiv dagegen, anderen zu tiefen Einblick in unsere Gedanken und Wünsche zu geben; wir fürchten, zum „gläsernen" Menschen zu werden. So verteidigen wir unsere räumliche und ideelle „Privatsphäre" oder – in etwas umfassenderer Formulierung „Privatheit" (dieser Begriff wird meist synonym gebraucht). Geradezu abschreckend finden wir es, wenn sich Dritte daran machen, „Persönlichkeitsprofile" herzustellen, die zur Grundlage von Entschei-

71 Lewinski 2011, S. 92.
72 Lewinski 2011, S. 94.
73 Vgl. dazu §§ 78 ff. Telekommunikationsgesetz.
74 So auch Heller 2011, S. 160 (s. unten S. 63 ff.).

dungen werden können, ohne dass wir uns dazu äußern können. Auch wer „nichts zu verbergen hat“, empfindet Unbehagen, wenn andere versuchen, in fremde Seelen einzudringen.

Tatsächlich ist es mit dem Schutz vor diesem Eindringen schlecht bestellt – wenn man den Äußerungen von Experten und Journalisten folgt, die sich kritisch mit der Entwicklung der Informationstechnik und ihrer Anwendung befassen. Datenschützer haben Schreckensbilder vom drohenden oder bereits erreichten „Überwachungsstaat“ gemalt; auch ich habe während meiner Amtszeit als Bundesbeauftragter für den Datenschutz diese Gefahr betont und dafür geworben, dass Staat und Gesellschaft mit personenbezogenen Daten rücksichtsvoll umgehen. Das Bewusstsein für die Notwendigkeit von Datenschutz ist durch diese Öffentlichkeitsarbeit ständig gewachsen, aber die Öffentlichkeit hat nicht nachvollzogen, dass viele der Sorgen sich als unbegründet erwiesen haben. Das Scheitern der Volkszählung 1983 gilt als Nachweis der gewachsenen Einsicht in die Risiken der Informationstechnik (zu Unrecht, denn gerade bei dieser Massen-Datenverarbeitungsaktion war das Risiko extrem gering!).[75] Nach wie vor wird der vermeintlich mutige Boykott der harmlosen Volkszählung als demokratische Höchstleistung gefeiert, und man vermisst eine gleiche Fundamentalkritik gegenüber aktuellen informationstechnischen Neuerungen. Das Internet aber gilt als der stärkste Feind der Privatsphäre, und wegen seiner Allgegenwärtigkeit meinen inzwischen viele, ein wirksamer Schutz der Privatsphäre sei endgültig unmöglich geworden. Der Buchtitel „Das Ende der Privatsphäre“[76] wird als Tatsachenfeststellung verstanden; was der Autor – der amtierende Bundesbeauftragte für den Datenschutz und die Informationsfreiheit – als Mahnung zur Umkehr verstanden wissen will, wird als abgeschlossener Prozess angesehen. Romanschriftsteller beteiligen sich in der Nachfolge von George Orwell an der politischen Debatte mit Horrorszenarien über ein künftiges Alltagsleben unter allumfassender Überwachung.[77] „Die Privatsphäre ist ein Auslaufmodell“; „Wir treten ein in das Zeitalter der ‚Post-Privacy‘: in ein Leben nach der Privatsphäre“, heißt es in dem Buch eines Bloggers und Filmkritikers unter Bezugnahme auf die alarmistischen Titel anderer Bücher, wenn auch mit einer ganz anderen Schlussfolgerung (auf die ich zurückkommen werde).[78]

75 Mehr dazu: Bull 2012, S. 151 ff.
76 Schaar 2007.
77 S. etwa Trojanow/Zeh in Anknüpfung an Sofsky; dazu die kritische Rezension von Milos Vec, FAZ v. 14.9.2009, S. 8 .
78 Heller 2011.

Tatsachen und Legenden

Um die phantastische Erfindung des weltweiten Netzes ranken sich manche Legenden. Sie sind zum großen Teil durch tatsächlich bestehende Eigenschaften der verwendeten Technik, wirtschaftliche Strukturen und soziale (sozialpsychologische) Gesetzmäßigkeiten begründet. Aber sie werden in einem Maße verallgemeinert, dass sie schließlich mit der Realität nichts mehr zu tun haben. So ist es gewiss richtig, dass im Netz unendlich viele Informationen über einen großen Teil der Menschheit gespeichert sind, aber es ist falsch, dass „das Netz" „alles" „über jeden von uns" „weiß". Abgesehen davon, dass „das Netz" kein Subjekt ist, sondern dass in Wahrheit nur die großen Technikfirmen, Netzbetreiber und Diensteanbieter gemeint sind, also das Oligopol von Microsoft, Google, Facebook, Twitter und einigen weiteren Unternehmen – die irreführende Verallgemeinerung liegt in der Behauptung, dass die Herren des Netzes die gleiche Art von „Wissen" besäßen wie natürliche Personen. Es wird unterstellt, dass die Verfügung über die Speichermedien und Computer gleichzusetzen sei mit dem Bewusstsein von Individuen.

Die anthropomorphen Begriffe und Metaphern, die durch die Internet-Debatte geistern,[79] verschleiern den entscheidenden Unterschied: Der Computer hat kein Bewusstsein und kein Gedächtnis.[80] Er speichert Zeichen, die nach unseren Konventionen Inhalte repräsentieren, und verändert oder transportiert sie nach vorgegebenen Programmen. Aus den Zeichen entsteht Bedeutung erst durch das Bewusstsein, und dieses ist dem Menschen vorbehalten; der Maschine fehlt es. Es ist ein langer Weg, ehe aus den Zeichen und Datenträgern zunächst „Information" und im günstigen Fall „Wissen" wird – und noch länger ist der Weg zu der Macht, von der man annimmt, das Wissen vermittle sie. Zwar können die technischen Vorgänge, die aus den Zeichen etwas „Bedeutendes" machen, sehr schnell vor sich gehen, aber die Wahrnehmung durch menschliche Augen oder Ohren und die Verarbeitung im menschlichen Kopf können lange dauern; unter Umständen brechen diese Vorgänge ergebnislos ab.

Unser Unbehagen angesichts der undurchschaubaren Apparate, das „diffuse Gefühl des Ausgeliefertseins"[81] rührt zum guten Teil daher, dass wir uns dieser wesentlichen Eigenschaften des technischen Systems nicht bewusst sind. Wir fragen uns zum Beispiel im Hinblick auf Standortsuchsysteme: „Wer weiß eigentlich,

79 Kritisch zum Gebrauch von Metaphern auch Passig/Lobo 2012, S. 36 ff., 48.

80 Auch dies wird von einigen Autoren inzwischen bestritten, das Gegenteil zumindest als Zukunftsvision behauptet. Vgl. etwa Meckel 2012 („Hybridisierung des Menschen durch die Verbindung von Körper, Technik und Geist"); Metzinger 2012 („Erste Maschinen mit Bewusstsein werden unglücklich sein"). Der britische „Experte" David Levy soll „perfekte Sexroboter" angekündigt haben und mit der „ersten Heirat zwischen Mensch und Maschine" „so in 50 Jahren" rechnen (Weber 2012). Auf derartige Phantasien kann keine Politik gegründet werden.

81 Kurz/ Rieger 2011, S. 8.

wo ich mich gerade befinde? Und warum weiß er auch, wo meine Freunde gerade sind – sogar besser als ich?“[82] Die Antwort ist ganz einfach: „Er“ ist nicht irgendeine Person oder Personengruppe, sondern das dazu eingerichtete und programmierte Datenverarbeitungssystem. Dieses unpersönliche Konstrukt „weiß“ natürlich gar nichts; es hält nur die Daten bereit, aus denen jemand Informationen ableiten kann. Um das unheimliche Äußere der Technik zu überwinden, personalisieren wir den Computer, und diese metaphorische Ausdrucksweise lenkt uns von der einfachen Wahrheit ab, dass die Geräte im Kern so viel und so wenig leisten wie ihre Benutzer, nur schneller und zuverlässiger, und dass ihr „Wissen“ immer erst von einem Menschen aktiviert werden muss (z.B. weil jemand nach mir sucht – sei es aus gutem, sei es aus schlechtem Grunde, aber nie ohne Anlass).

Wenn das technische Gehirn „abschaltet“, zu langsam oder falsch reagiert, gehen die Zeichen und ihre Bedeutung vorzeitig ganz oder teilweise verloren. Im Übrigen können die gespeicherten Informationen zwar theoretisch noch lange aktiviert werden, aber solange das nicht geschieht, sind sie nicht Bestandteile „unseres“ Gedächtnisses. Wir sprechen zwar auch von Archiven und Aktensammlungen als „Gedächtnis“ der Gesellschaft, doch auch das ist bloß metaphorisch gemeint und in gewisser Hinsicht schief.

Das Gedächtnis der Computer und die Lücken im Netz

Eine andere Behauptung lautet: Das Internet vergisst nichts. Auch das ist in dieser Pauschalität falsch. „Auch wenn es Internetarchive gibt: Wer einmal versucht hat, eine bestimmte Webseite aus dem Jahr 1998 noch einmal aufzurufen, kann das bestätigen“.[83] Richtig ist, dass ein großer Teil der Speicherungen dauerhaft ist und auch verfügbar bleibt. Daten können tatsächlich eine Langzeitwirkung entfalten; man staunt oft, dass uralte, längst überholte Angaben in irgendeinem Speicher „überlebt“ haben, während die Welt darum herum sich verändert hat. „Jugendsünden“ können Greise einholen. Äußerungen, die ich selbst vergessen habe oder für gelöscht halte, werden aus den Tiefen des Netzes hervorgezogen und dem Betroffenen vorgehalten – ob es ihm lieb ist oder nicht.

Andererseits braucht man sich nur klar zu machen, wie viele Daten tagtäglich von den speichernden Stellen wieder gelöscht werden. Große Mengen personenbezogener Daten werden gelöscht, weil dies gesetzlich vorgeschrieben ist – man denke an die Überprüfungs- und Löschungspflichten der Sicherheitsbehörden (die bisweilen – offline, weil diese Daten gar nicht im Netz stehen – sogar übereifrig

82 Kurz/Rieger 2011, S. 8.
83 Drösser 2011. Ebenso Passig/Lobo 2012, S. 45 („ein Narrativ, das … wenig mit den Fakten zu tun hat“).

befolgt werden, wie im Fall einiger Unterlagen über den „Nationalsozialistischen Untergrund“). Unternehmen löschen ständig Daten, weil sie den Speicherplatz anders verwenden wollen, und die Kosten dauerhafter Aufbewahrung dürften auch die Betreiber der sozialen Netzwerke dazu veranlassen, die Daten ihrer „Mitglieder“ und Nutzer nach einiger Zeit zu vernichten. Die an den Daten interessierten werbenden Unternehmen wollen „frische Daten“; mit archivwürdigen Angaben können sie nicht viel anfangen. Wer an der Vergangenheit bestimmter Personen interessiert ist – z. B. als alter Freund oder Konkurrent, als Behörde oder als potentieller Arbeitgeber – kann zwar manches Relevante im Netz recherchieren, aber niemals sicher sein, dass er ein auch nur halbwegs vollständiges und aktuelles Persönlichkeitsbild des Betreffenden erhält. Polizei und Justiz recherchieren selbstverständlich auf vielerlei Wegen und möglichst gezielt, also unter Kriterien, die aus konkreten Verdachtsanlässen abgeleitet sind; sie verlassen sich nicht allein auf die Internetspuren.

Es gehört zu den allgemeinen Pflichten nach dem Datenschutzrecht, unrichtige Daten zu berichtigen, nicht mehr erforderliche und unzulässig gespeicherte Daten zu löschen und bestrittene Angaben zumindest zu sperren. Die Gesetze können zwar kein „Recht auf Vergessen“ begründen – denn das Vergessen kann nur in den Köpfen der Menschen stattfinden, auf die kein Gesetz Einfluss hat. Aber Löschungspflichten sollen dazu beitragen, dass Altes und Falsches nicht dauerhaft weitergetragen wird. Nach dem Entwurf einer Datenschutz-Grundverordnung der EU soll jeder Betroffene ein „Recht auf Vergessenwerden und auf Löschung“ haben (so die Überschrift des einschlägigen Artikels).[84] Die umfassende Umsetzung dieses Anspruchs wird allerdings schwierig sein.[85]

Der Einzelne hinterlässt bei jeder Suche im Internet Spuren und bei jeder Eingabe personenbezogene Daten, die zunächst gespeichert werden und vielfältig genutzt werden können; aus diesen Angaben kann ein Mosaik zusammengesetzt werden, das viel über Verhaltensweisen und Kaufpräferenzen, Aufenthalte und Lebensgewohnheiten verrät.[86] Dass damit „Persönlichkeitsprofile“ hergestellt würden, die für gute wie böse Zwecke nutzbar seien, ist eine der wesentlichen Ursachen für die Angst, die viele – wirklich oder angeblich – vor der Informationstechnik empfinden. Aber was auch immer Psychologen und Werbestrategen aus den Internetspuren der Nutzer herausholen, sie können nichts Zuverlässiges über die Absichten und Meinungen der Einzelnen aussagen. Zu einem wirklichen Persönlichkeitsprofil aber würde gerade das „forum internum“, die innere Bewusstseinsver-

84 Art. 17 des Entwurfs (Kommissions-Drucksache (2012) 11 v. 25.1.2012.
85 Die technische Lösung in Gestalt des „digitalen Radiergummis“ scheint nicht praktikabel zu sein, vgl. Drössel 2011.
86 Mehr dazu unten S. 65 f.

fassung des einzelnen Menschen gehören. Der „Datenschatten", die „digitale Identität"[87] unterscheidet sich von dem wirklichen Menschen.

Schließlich trifft auch die Behauptung nicht zu, der Staat und/oder die Wirtschaft wollten „alle" Informationen über „alle" Einwohner zur Kenntnis nehmen oder zur Verfügung haben.[88] Es kennzeichnet gerade das geltende Recht, dass die Befugnisse zur Speicherung, Verarbeitung und Verwendung persönlicher Daten durch eine Vielzahl spezieller Rechtsnormen geregelt sind, und es ist eine unbewiesene Behauptung, dass diese Normen ständig verletzt würden. Sie werden im Großen und Ganzen eingehalten. Dass damit immer noch eine riesige Zahl von Datenübermittlungen zulässig ist, kann keiner bestreiten, aber nur wer sich aus der Gesellschaft verabschieden will, kann den Austausch und die Nutzung von Informationen grundsätzlich ablehnen.

Zur Klarstellung: Mit der Kritik der Internetlegenden soll nicht etwa bestritten werden, dass es zahlreiche Risiken des Datenmissbrauchs gibt. Aber für die rechtliche Bewältigung der neuen Probleme ist es nicht hilfreich, sich an den Verallgemeinerungen auszurichten. Vielmehr muss es eine Rolle spielen, wie häufig ein Phänomen ist und wie viele Menschen es tatsächlich betrifft. Sonst werden die Normen, mit denen das Risiko bekämpft werden soll, zu weit geschnitten, und stiften dann mehr Schaden als Nutzen.

Ich räume ein: Diese Betrachtungsweise setzt ihrerseits die Gewissheit voraus, dass meine Gedanken trotz aller Computer und Netze letztlich frei sind und frei bleiben, selbst wenn andere versuchen, meine Lebensäußerungen auszudeuten. Wer dies bestreitet, kommt zu anderen Schlüssen. Die Politik muss und will auch auf diese andere Wahrnehmung eingehen und auch die Menschen „abholen" und zufrieden stellen, denen die Technik unheimlich bleibt.

Die Dimensionen des Persönlichkeitsschutzes

Damit sind wir bei der Frage, wie das Recht auf die Tatsachen, aber auch auf die Ängste der Menschen eingehen soll. Der übliche Ansatzpunkt ist das tradierte und verfassungsrechtlich geschützte Persönlichkeitsrecht. Kulturkritiker behaupten, das Zeitalter des Privatsphärenschutzes sei vergangen, und im günstigsten Fall plädieren sie dafür, aus der „Post-Privacy" das Beste zu machen.[89]

Über den Inhalt der Begriffe „Privatheit" und „Privatsphäre" besteht – entgegen dem ersten Anschein – kein Konsens. Seine Bedeutung schwankt zwischen „Robinson" und „My home is my castle", zwischen vollständiger Abschottung des

87 Diese Begriffe verwenden z.B. Worms/Gusy 2012, S. 95.
88 Auch diese Vorstellung wird vielfach verbreitet, vgl. etwa Sofsky 2007; Bolz 2010.
89 Heller 2011, S. 7 f.

Einzelnen von der Gesellschaft und dem Schutz eines räumlich abgegrenzten Bereichs. Privatheit ist Voraussetzung von Freiheit; sie ist Kraftquelle und Erholungsraum. Es ist trotzdem falsch, sie einfach mit Freiheit gleichzusetzen. Innere Freiheit, wie sie im privaten Bereich gewonnen und ausgeübt wird, reicht für die Entfaltung des Menschen nicht aus; Freiheit muss sich gerade in der Auseinandersetzung mit anderen bewähren.

Die Extremposition: Abschirmung von der Gesellschaft

Es ist zwar durchaus richtig, wenn gesagt wird, Privatheit sei „zuerst ‚Freiheit von' und nicht ‚Freiheit zu etwas'", und für die private Freiheit sei „primär" „die Abwesenheit von Zwang und äußerer Einwirkung". [90] Aber damit ist eben nur die eine Seite des Themas angesprochen und die andere, eigentlich unübersehbare ist ausgeblendet. So verschanzt sich der Soziologe Sofsky in seiner „Zitadelle der persönlichen Freiheit", die er als Schutz nicht nur vor „Enteignung und Entmündigung", sondern auch vor „Aufdringlichkeit und Bevormundung, vor Macht und Zwang" ansieht.[91] Er legt Wert auf „Abstand" und wittert „Einmischung" von der gesamten Umwelt: „Das Heer der Eindringlinge reicht von besorgten Eltern, misstrauischen Verwandten und neugierigen Nachbarn über selbsternannte Moralprediger, Toleranzprüfer, ehrgeizige Meinungsmacher und Gesinnungspädagogen bis zu den Steuereintreibern, Spitzeln und Wachposten der Fürsorge". „Sie alle", meint der Autor, „verstoßen gegen das Freiheitsrecht des einzelnen, in Ruhe gelassen zu werden".[92]

Nicht alle „Verteidiger des Privaten" gehen in ihrer Soziophobie so weit. Man darf vermuten, dass auch die „Robinsoniaer" gern an den Segnungen der Zivilisation teilhaben möchten, die Wirtschaft, Technik und Staat geschaffen haben, und dafür gewisse „Einmischungen" der sozialen Umwelt hinnehmen. Doch scheinen viele zu glauben, alle Leistungen anderer und der Gemeinschaft genießen zu können, ohne dafür selbst irgendetwas über sich selbst preiszugeben. Selbst Robinson auf seiner einsamen Insel hätte aber eine Hilfsbitte mit der Angabe seines Standortes verbunden (wenn er ihn denn bezeichnen konnte), und in der Flaschenpost hätte er zumindest seinen dringendsten Bedarf beschrieben. Und dass die gemeinsame Organisation zur Erfüllung öffentlicher Aufgaben, die wir Staat nennen, nicht ohne Steuern auskommt und soziale Wohltaten nicht anonym verteilt werden können, sollte zum soziologischen Grundwissen gehören. Es führt in die Sackgasse,

90 Sofsky 2007, S. 153.
91 Sofsky 2007, S. 37. Dieser Autor bestreitet die Friedensfunktion des Rechts und spricht in negativem Sinne von „totalem Rechtsstaat" (S. 24).
92 Sofsky 2007, S. 37 f.

wenn dem Staat, der die Konflikte mit seinen Mitteln lösen will, nur Unterdrückungsabsicht unterstellt wird.[93]

„Öffentlich“ gegen „privat“

Die Abgrenzung zwischen „privat“ und „öffentlich“ ist seit je ein zentrales Thema der politischen Theorie und der Rechtswissenschaft. Zu einer freiheitlichen Ordnung gehört sowohl Privatheit wie Öffentlichkeit: die Abschirmung einer privaten Sphäre und die Freiheit privater Betätigung wie auch die öffentliche Wahrnehmung und öffentliche Kritik des individuellen Handelns. Die Grenzen des Privatheitsschutzes und des Öffentlichkeitsanspruchs variieren im historischen und internationalen Vergleich. „Privatheit ist eine kulturelle Konstruktion“; „die Grenzen des Privaten gelten als konstitutiv für das normative Selbstverständnis moderner, liberal-demokratischer Gesellschaften und sind doch notorisch umstritten“.[94] Und die Bestimmung dieser Grenzen geschieht durch Rechtsnormen: „Es bedarf des Rechts“.[95]

Das geltende Recht erkennt den menschlichen Wunsch nach Intransparenz an, und zwar überall in der westlichen Welt und weit darüber hinaus, und so gelten in Deutschland wie in ganz Europa, in den USA und Kanada und in vielen anderen Staaten, auch auf anderen Kontinenten Rechtsnormen, die es anderen erschweren sollen, die geheimen Gefühle und Sehnsüchte der Menschen herauszufinden.[96] Sie sind teils Richterrecht, teils Gesetzesrecht, und über ihre richtige Anwendung wird lebhaft diskutiert. Die Europäische Menschenrechtskonvention hat schon 1952 das Recht jeder Person auf „Achtung ihres Privat- und Familienlebens, ihrer Wohnung und ihrer Korrespondenz“ statuiert,[97] und die Charta der Grundrechte der Europäischen Union hat diese Bestimmung fast wörtlich übernommen[98] und ein Recht auf Schutz der personenbezogenen Daten hinzugefügt.[99]

93 So aber Sofsky 2007, u.a. S. 38.
94 Seubert 2012, S. 101. S. a. die Beiträge in Seubert/Niesen (Hrsg.) 2010.
95 Worms/Gusy 2012, S. 96.
96 Die umfassende Literatur und Rechtsprechung zum Persönlichkeitsschutz kann hier nicht zitiert werden; das ist auch nicht nötig, weil die Grundlinien unumstritten sind. Die unterschiedlichen Formen des Persönlichkeitsschutzes werden im folgenden Text durchgesprochen.
97 Art. 8 EMRK.
98 In Art. 7 EU-Grundrechte-Charta heißt es nur statt „Korrespondenz“ „Kommunikation“.
99 Art. 8 EU-Grundrechte-Charta.

Würde, Freiheit, Selbstbestimmung

Während der Schutz der Privatheit bei uns – in Deutschland und seinen europäischen Nachbarstaaten – im Kern auf das Gebot der *Menschenwürde* zurückgeführt wird, betrachten amerikanische Juristen und Politiker den Gedanken des Datenschutzes als Konsequenz der *Freiheit* des Individuums.[100] Der Yale-Professor James Q. Whitman hat dies in einem materialreichen rechtsvergleichenden Aufsatz auf die Formel von den „Two Western Cultures of Privacy" gebracht, deren Grundvorstellungen „Dignity versus Liberty" sind.[101] Andreas Zielcke plädiert in seiner Besprechung dieses Ansatzes dafür, die beiden Ideale aufeinander zu beziehen und miteinander zu verbinden; sonst blieben zu große Lücken im Rechtsschutz,[102] und das hat viel für sich – auch wenn die amerikanische Nüchternheit in manchen Zusammenhängen deutlich mehr Klarheit schafft als der deutsche Griff zu den moralischen Sternen.

Zwischen Freiheitsrecht und Menschenwürde schlägt die Idee der *Selbstbestimmung* eine Brücke, und diese Idee spielt in der deutschen Literatur und Praxis eine wichtige Rolle. Selbstbestimmung über das, was ich anderen über mich mitteilen will, ist eine rechtliche Selbstverständlichkeit. Ich kann bestimmen, wem ich was über mich offenbare. Ich kann Schutz davor verlangen, genötigt, bedroht, getäuscht oder unter Drogen gesetzt zu werden. Vom Staat kann ich erwarten, dass er nur diejenigen Informationen über mich sammelt und verwertet, die er zur Erfüllung seiner Aufgaben benötigt. Als soziales Wesen kann ich allerdings nur begrenzt darüber bestimmen, was andere über mich wissen; ich kann nicht verhindern, dass andere sich ein (aus meiner Sicht) falsches Bild von mir machen. Das Recht, über meine Äußerungen selbst zu bestimmen, ist von Wissenschaft und Gerichten zum „informationellen Selbstbestimmungsrecht" weiterentwickelt worden. Vom Bundesverfassungsgericht zum Bestandteil des Grundgesetzes erklärt, bildet es seit drei Jahrzehnten den rechtstechnischen Rahmen für die richterliche Ausformung des Datenschutzes und wird von Verwaltung und Wirtschaft, aber auch von der Wissenschaft als Eckpfeiler der Informationsrechtsordnung immer neu beschworen.

Der Schritt von der Äußerungsfreiheit zur „informationellen Selbstbestimmung" ist freilich größer als man zunächst annehmen mag. Denn diese juristische Weiterentwicklung wird im Grunde den Besonderheiten gerade der Informationssammlung und des Kommunikationswesens nicht gerecht. Sie kann allenfalls eine Richtungsangabe darstellen („möglichst viel Selbstbestimmung beim Umgang mit den Daten"), ist aber zu formal, als dass sie eine Abgrenzung zwischen erlaubtem

100 Zielcke 2010 mit Hinweis auf Whitman 2004
101 Whitman 2004.
102 Zielcke 2010.

und verbotenem Verhalten ermöglichen und inhaltliche Ansätze zur Konfliktlösung liefern könnte.[103]

Die Selbstbestimmungsidee führt immerhin zur praktischen Lösung eines Teils der Probleme, indem sie die *Einwilligung* der Betroffenen zur Erlaubnisgrundlage macht. Wann eine Einwilligung sinnvoll ist (und wann das Gesetz eine allgemein verbindliche Lösung schaffen muss), und unter welchen Umständen die Einwilligung wirksam sein soll, kann und muss seinerseits rechtlich geregelt werden.[104] Wenn die Einwilligung vorab nicht erlangt werden kann – wie bei den Geodatendiensten (Google Street View u.a.) –, kann die Selbstbestimmung immerhin nachträglich durch ein möglichst leicht zugängliches Widerspruchsrecht gewährleistet werden.[105]

Die Geschichte des Persönlichkeitsrechts

„Entdeckt" wurde die „Privatheit" von US-amerikanischen Juristen; als Ursprung aller weiteren juristischen Überlegungen zu diesem Themenfeld gilt der Aufsatz der Bostoner Juristen Samuel D. Warren und Louis D. Brandeis „The Right to Privacy" aus dem Jahre 1890.[106] Die Autoren reagierten damit auf die in der Presse aufkommenden Sensationsgeschichten aus dem Privatleben Prominenter; sie folgerten den Schutz der Betroffenen aus dem ungeschriebenen Common Law, das sich „in seiner ewigen Jugend" immer weiter entwickle. Das Recht auf Leben werde nunmehr auch als das Recht verstanden, „sich des Lebens zu freuen – das Recht in Ruhe gelassen zu werden".[107] Trotz der etwas schwachen Begründung setzte sich nach längeren Schwankungen die Ansicht durch, dass es ein solches Recht auf Privatheit gebe und dass seine Verletzung zum Schadensersatz verpflichte. Die Presse war davon nicht gerade begeistert.

In Deutschland herrschte bis nach dem Zweiten Weltkrieg die Meinung vor, nur die Ehre und das Ansehen einer Person seien rechtlich geschützt. Ein *allgemeines Persönlichkeitsrecht* erkannte der Bundesgerichtshof erstmals 1958 an; es billigte einem Herrenreiter, dessen Foto zur Werbung für ein Stärkungsmittel missbraucht worden war, einen Schadensersatzanspruch wegen Verletzung dieses Rechts an.[108] Im Laufe der Zeit konstruierten die Gerichte ein ganzes System von Rechts-

103 Zur Kritik des „informationellen Selbstbestimmungsrechts" vgl. Bull 2011 a m.w.N.; s.a. Schoch 2012.
104 Vorschläge dazu zuletzt bei Spindler 2012. Zu den Rahmenbedingungen s.a. Wolf Osthaus, in: DJT 2012, S. 75, Thesen 8-10 (u.a.: Abnutzungs- und Gewöhnungsgefahr, falsche Anreize).
105 Spindler 2012, S. 134 These 21.
106 Warren/Brandeis 1890. Näheres bei Bull 1984, S. 77 ff.
107 Das Wort vom „right to be let alone" hatte bereits der Richter Cooley geprägt.
108 BGHZ 26, 349. Vgl. nochmals Bull 1984, S. 79 ff.

positionen – vom *Recht auf das eigene Bild*[109] über das *Recht an der eigenen Stimme* bzw. *am gesprochenen Wort*[110] bis zum *Recht an den „eigenen" Daten* (das freilich nur im übertragenen Sinne gemeint ist)[111]. Man knüpfte an den Schutz der *räumlichen* Privatsphäre an, die durch die Unverletzlichkeit der Wohnung (Art. 13 GG) besonders gesichert ist, und erweiterte den Privatsphärenschutz um den Bereich der privaten *Geheimnisse*; von da aus war der Schritt zu den sonstigen Informationen über die eigenen Verhältnisse nicht weit.

Klassisch ist etwa die Formulierung des Bundesverfassungsgerichts, dem Einzelnen müsse „um der freien und selbstverantwortlichen Entfaltung seiner Persönlichkeit willen ein ‚Innenraum' verbleiben", „in dem er ‚sich selbst besitzt' und ‚in den er sich zurückziehen kann, zu dem die Umwelt keinen Zutritt hat, in dem man in Ruhe gelassen wird und ein Recht auf Einsamkeit genießt'".[112] Im konkreten Fall ging es darum, ob die Bürger im Rahmen eines Mikrozensus nach ihren Urlaubsgewohnheiten gefragt werden durften. Das Verfassungsgericht hat das gebilligt, weil die Statistiker sich nur für „das Verhalten des Menschen in der Außenwelt" interessierten; der „unantastbare Bereich privater Lebensgestaltung" werde dadurch nicht erfasst. Zitiert wird aus diesem Urteil meist nur die über den eher harmlosen Gegenstand weit hinausgreifende Formulierung, dass es dem Staat verboten ist, „den Menschen in seiner ganzen Persönlichkeit zu registrieren und zu katalogisieren, sei es auch in der Anonymität einer statistischen Erhebung, und ihn damit wie eine Sache zu behandeln, die einer Bestandsaufnahme in jeder Beziehung zugänglich ist".

Heute wird „Privatheit" oder „Privatsphäre" fast schon allgemein mit „Datenschutz" gleichgesetzt, und die eine wie die andere Rechtsfigur wird zusätzlich mit der Achtung vor der Menschenwürde begründet. Wir sollten aber genauer unterscheiden; denn die Schutzrichtung ist nicht identisch, und es ist nicht selbstverständlich, dass etwa die Offenbarung von Geheimnissen aus der Privat- oder Intimsphäre nach den gleichen Rechtsnormen beurteilt wird wie die Veröffentlichung irgendwelcher Lebenssachverhalte im Netz. Die Menschenwürde ist verletzt, wenn ein Individuum erniedrigt, missachtet, wie eine Sache behandelt wird. Schwere Beleidigungen können diesen Tatbestand erfüllen, aber nicht jede Missachtung ei-

109 Vgl. § 22 Kunsturhebergesetz und § 201 a StGB sowie u. v. a. etwa die Entscheidungen des BVerfG und des EGMR in Auseinandersetzungen verschiedener illustrierter Blätter mit dem Ehepaar von Hannover („Caroline"-Entscheidungen), insbes. Beschluss des BVerfG v. 26.2.2008, BVerfGE 120, 180 und Urteil des EGMR v. 7.2.2012, Kommunikation & Recht 2012, S. 179.

110 Aus der Rspr.: BGHZ 27, 284 (290); BVerfGE 34, 238 (grundsätzliches Verbot heimlicher Tonbandaufnahmen) und 106, 28 (39ff.) (Verbot einer Mithöreinrichtung, die ohne Wissen des Gesprächspartners eingerichtet wurde).

111 BVerfGE 65, 1 (43).

112 BVerfGE 27, 6 (mit Zitaten aus: Wintrich, Die Problematik der Grundrechte, 1957, S. 15 f., und Dürig, in: Maunz/Dürig/Herzog/Scholz, Grundgesetz, 2. Aufl., Art. 1 Rdnr. 37).

ner Datenschutzvorschrift. Mit Datenschutznormen lässt sich die Verletzung individueller Rechte bekämpfen, aber nicht die Praxis, dass rechtmäßig gewonnene Daten über Individuen wie Waren gehandelt und ausgewertet werden. Ausufernde Datenverarbeitung, massenhafte Speicherung und technikgestützte Auswertung von Lebensäußerungen sind Phänomene, die viele beunruhigen – aber sind das wirklich Angriffe auf Grundrechte oder gar auf die Menschenwürde von Individuen? Doch allenfalls dann, wenn Menschen missachtet, respektlos behandelt, in ihrer Integrität verletzt werden. Das aber ist bei nüchterner Betrachtung der meisten Vorgänge von Massendatenverarbeitung nicht der Fall. Die „Täter“ interessieren sich nicht für die individuell Betroffenen, sie behandeln nicht die Personen, sondern die diese betreffenden Daten wie Sachen, und bilden Gruppen von Betroffenen, die nicht mehr als Individuen gemeint sind, sondern als Träger bestimmter Merkmale. Die Betroffenen haben kein „Eigentum“ an den „personenbezogenen“ Daten, und selbst wenn sie es hätten, würden wir den „Diebstahl“ von Daten nicht als Angriff auf die Würde der Eigentümer ansehen.

Von „Verwaltung“ zu „Verdatung“

Irgendwann im Laufe der frühen Diskussionen um die Risiken der Datenverarbeitung ist das Wort von der „Verdatung“ aufgekommen. So wie die Menschen „verwaltet“, „verkabelt“ und „vernetzt“ werden – was immer auch eine Form von Unterlegenheit ausdrückt –, werden die Individuen in Ansammlungen von Daten verwandelt, also zum *Objekt fremder Verfügung* gemacht. Das aber könnte in der Tat mit der Achtung vor der Menschenwürde unvereinbar sein.

Entscheidend dafür, ob die Verarbeitung persönlicher Informationen eine unzulässige „Verdatung“ bedeutet, ist die Situation, in die der Betroffene durch diesen Vorgang gerät.[113] Entweder wird nur etwas über ihn von einer Behörde oder einem Unternehmen zur Kenntnis genommen und es werden Schlüsse daraus gezogen – das ist bei jeder Form von „Verwaltung“ im weitesten Sinne unvermeidlich; es ist auch gewollt, weil ja aufgrund der Informationen etwas geschehen soll. Die typischen Fälle sind, dass der Betroffene einen Anspruch auf eine Leistung oder Zahlung hat – zu diesem Zweck werden im Geschäftsleben die meisten Daten erhoben und verwendet – oder dass andere oder der Staat eine Leistung von ihm verlangen können – seien es Steuern, Sozialabgaben, private Schadensersatz- oder Unterhaltszahlungen und was sonst noch an Gegenständen privaten oder staatlichen Interesses in Betracht kommt. Die unvermeidliche Folge aber ist die Unterwerfung des Einzelnen unter die Macht Dritter: Die Information kann im Streitfall gegen

113 In einem anderen Sinn benutzt Heller (2011, S. 54 ff.) den Begriff der Verdatung („die Verdatung der Welt, der Texte, der Menschen“).

den Einzelnen verwendet werden. Ist es also eine unerlaubte „Verdatung", ein Fall von Unterdrückung des Individuums, wenn dem Gläubiger zur Durchsetzung eines Anspruchs auf Schadensersatz das Recht zugesprochen wird, die dazu erforderlichen Daten über den Schuldner zu verwenden?

Betrachten wir ein paar Beispiele, bei denen von Unterwerfung des Individuums durch den Staat oder durch Private (insbesondere Unternehmen) gesprochen wird. Die schwersten Eingriffe in die Sphäre des Einzelnen gehen von den Behörden aus, die zur Verfolgung von Straftaten und zur Bekämpfung von Gefahren für die öffentlichen Sicherheit berufen sind: Polizei, Staatsanwaltschaften und Geheimdienste (Verfassungsschutzämter, Bundesnachrichtendienst und militärischer Abschirmdienst). Verfolgt die Justiz mit Hilfe der Polizei Straftäter, so darf sie aufgrund gesetzlicher Regelungen zahlreiche Informationen sammeln und auswerten, untereinander abgleichen und zur Überprüfung an weitere Behörden übermitteln. Die Beteiligten sind an die Strafprozessordnung und die Polizeigesetze gebunden (die übrigens deutlich weniger Befugnisse haben als die beliebten Fernsehkommissare in Anspruch nehmen, aber doch eine ganze Menge). Es ist unvermeidlich, dass einzelne Akteure versuchen, ihre Befugnisse zu überschreiten, sei es aus Übereifer, sei es aus Nachlässigkeit oder weil sie die Rechtsnormen falsch interpretieren. Den Betroffenen können daraus große Belastungen erwachsen; wer zu Unrecht strafrechtlich verfolgt wird, fürchtet aus gutem Grund, dass „immer etwas hängen bleibt". Und dabei ist es häufig ganz unerheblich, ob die Informationen in einem Computer gesammelt wurden oder ob jemand ein Gerücht verbreitet hat, das nur in einigen Köpfen existierte. Ja, die Beeinträchtigung kann viel größer sein, wenn ein Staatsanwalt ohne Benutzung einer Datensammlung jemanden einer Straftat bezichtigt, als wenn er im Zuge einer Rasterfahndung alle Angehörigen einer bestimmten Personengruppe überprüft. Man denke an einige Fälle öffentlichen „Prangers", etwa die Verhaftung eines Verdächtigen vor laufenden Fernsehkameras oder die vorzeitige Bekanntmachung eines Ermittlungsverfahrens.

Dennoch: Gefahren für das persönliche Ansehen, für die Ehre oder für die berufliche Entwicklung bestehen besonders da, wo große Mengen von Informationen automatisiert verarbeitet werden, und insbesondere da, wo sie zu Zwecken der öffentlichen Sicherheit verwendet werden. Man gerät eher in Verdacht – zu Recht oder zu Unrecht, man wird leichter übervorteilt oder übertölpelt, wenn andere einen besonders großen Bestand an Informationen nutzen können.

Klar ist: Die „Online-Durchsuchung" privat genutzter Computer durch eine Behörde beeinträchtigt die Privatsphäre noch mehr als eine Wohnungsdurchsuchung und Beschlagnahme von Akten. Von der Wirtschaft gehen solche Gefahren nicht aus; kein Unternehmen kann uns etwas vorschreiben. Aber wenn Unternehmen mehr Informationen besitzen als ihnen in einem ausgewogenen Verhältnis zustehen, droht den Unterlegenen Diskriminierung, vor allem durch Verweigerung von

Vertragsabschlüssen und Krediten. Es ist unbestritten, dass das Recht gegen solche Nachteile schützen muss.

Der Schutz der freien und unbefangenen Kommunikation

Über die Abwehr konkreter Schäden hinaus soll das Persönlichkeitsrecht aber auch dazu beitragen, dass wir weiterhin *frei* und *unbefangen* miteinander *kommunizieren* können. Die Freiheit und Unbefangenheit der Kommunikation ist von vielen Seiten bedroht, aber in höchst unterschiedlicher Intensität: von Seiten des Staates durch unmittelbare Eingriffe, Verbote und Sperren, von Privaten durch Ausspähung, durch Auswertung vorhandener Daten und durch unerwünschte Ansprache. Man tauscht sich nicht offen aus, wenn man befürchten muss, dass Fremde mithören oder mitlesen. Man will nicht mit Leuten in Verbindung stehen, die man nicht kennt, denen man nicht vertraut. So wird Datenschutz auch als Schutz vor unerwünschter Kommunikation verstanden – und sogar als Schutz davor, von Fremden angesprochen zu werden oder namentlich adressierte Sendungen zu erhalten.

Nach weitverbreiteter Ansicht liegt eine Beeinträchtigung der individuellen Freiheit schon dann vor, wenn die Menschen das *Gefühl* bekommen, sie würden ständig beobachtet, registriert, bewertet und kontrolliert. Wenn ich so frage, habe ich allerdings den Maßstab gewechselt; es geht dann nicht um die tatsächliche Wirkung der Informationsprozesse, sondern um deren subjektive, durch Vermutungen und Ängste verzerrte oder übersteigerte Wahrnehmung. Ist das ein hinreichend fester Boden dafür, die betreffende Form von Datenverarbeitung einzuschränken oder gar zu unterbinden? Habe ich ein *Grundrecht auf* den *Respekt* anderer – oder ist das nicht vielmehr nur eine *gesellschaftliche* Norm, eine Regel des anständigen Umgangs miteinander, die den Staat nichts angeht? Immerhin nehmen die nationalen und europäischen Gesetzgeber auch solche Ängste zum Anlass, regelnd auf die Entwicklung der Internet-Kommunikation einzuwirken. Ein Großteil der Auseinandersetzungen mit den sozialen Netzwerken dürfte gerade um die Frage kreisen, wie weit dieser „Gefühlsschutz" gehen soll oder darf. Praktikable Abgrenzungen können aber – wenn überhaupt – nur die Gesetzgeber formulieren; es ist unmöglich, solche Regeln aus den Grund- und Menschenrechten unmittelbar abzuleiten.

Das Grundmuster der Risikodiskussion

Möglichkeit und Wirklichkeit der Techniknutzung

Bei der Beschäftigung mit dem Themenkreis „Gesellschaft und Technik" fällt immer wieder auf, dass *technische Möglichkeiten* den Ausgangs- und Endpunkt von Diskussionen über *politische und soziale Probleme* bilden. Viele Probleme werden als Folge technischer Entwicklungen angesprochen, und neue Techniken werden als Lösung angeboten. Es ist zwar verständlich, wenn Unternehmen der Internetwirtschaft so vorgehen; sie brauchen Geschäftsmodelle und Marketingstrategien. Politik und Wissenschaft jedoch erfüllen ihre Aufgaben nicht ausreichend, wenn sie nur von dem ausgehen, was die Technik-Erfinder und Vermarkter versprechen, statt umgekehrt zunächst die wahrscheinliche Entwicklung zu erforschen, die Interessenlage zu klären und um politische, soziale, wirtschaftliche und rechtliche Lösungen zu ringen. Die Technik muss dabei einerseits als eine Bedingung der sozialen und ökonomischen Entwicklung bedacht werden, andererseits aber als (anzupassendes!) Hilfsmittel gestaltet werden. Ob z.B. die neuen Medien wirklich soziale Strukturen verändern, wie häufig behauptet wird, ist keineswegs sicher und hängt u.U. gerade umgekehrt von der rechtlichen Ausgestaltung ab, um die in den netzpolitischen Diskussionen gerade gestritten wird. Man sollte das Pferd nicht vom Schwanze her aufzäumen.

Regelmäßig läuft die Untersuchung der Gefahren der Informationstechnik in einer bestimmten Form ab.[114] Über welche neue Technik und welche Nutzungsart auch immer geredet und geschrieben wird – die Kontroverse ist immer gleichartig strukturiert. Den Befürwortern stehen die Kritiker gegenüber, und ihre Bedenken laufen immer auf dieselbe Begründung hinaus:

- Erstens: Es sei *möglich*, dass die Technik für unerwünschte Zwecke benutzt werde,
- es sei zweitens auch *wahrscheinlich*, dass tatsächlich in der Zukunft jemand (der Staat, ein Unternehmen, Private) versuchen werde, dies zu tun, so dass
- drittens ein ernstes Risiko bestehe, dass durch Fehlhandlungen und Fehlentwicklungen tatsächlich *Schäden* bei Betroffenen entstehen.

In allen drei Punkten wird regelmäßig zu pauschal und ohne ausreichende empirische Basis argumentiert. Staatliche Maßnahmen, insbesondere neue Gesetze müssen auf eine solidere Grundlage gestellt werden als auf nicht zu Ende gedachte Prognosen und gefühlte Bedrohungen.

114 Dass „fast alle Elemente der heutigen Datenschutzdiskussion" schon vor Jahrzehnten in Gebrauch waren, dokumentieren Passig/Lobo 2012 (S. 201 ff.) an alten Presseartikeln.

Es macht schon einen großen Unterschied aus, nach welchem *Maßstab* ein Handlungszweck unerwünscht ist. Der beliebte Begriff „Missbrauch" kann bedeuten, dass Daten unter *Verletzung von Rechtsnormen* gesammelt und genutzt werden – dann ist die Sache klar. Es kann aber auch sein, dass nur Verstöße gegen *Moralgesetze* oder Leitlinien der *Sozialethik* (z.B. der Wirtschaftsethik) befürchtet werden. Diese wiegen deutlich geringer als Rechtsverletzungen, jedenfalls ist die Durchsetzung rein ethischer Maßstäbe nicht primär Aufgabe des Staates, sondern Sache der Gesellschaft. Noch geringeres Gewicht hat die Besorgnis, dass nur gegen Regeln des gesellschaftlichen *Anstandes*, des *Takts* und der *Höflichkeit* verstoßen werde (also z. B. jemand taktlos oder ungeschickt angesprochen wird); das ist nicht strafbar und nicht einmal gesetzlich verboten, sondern allenfalls von der Gesellschaft missbilligt und für die Betroffenen lästig. „Missbrauch" von Daten ist also durchaus nicht in jedem Fall ein Skandal.[115]

Prominente Bürgerrechtler verweisen in solchen Diskussionen gern darauf, dass der Datenschutz aus dem obersten Gebot der Verfassung hergeleitet wird, nämlich aus dem Gebot, die Menschenwürde zu achten und zu schützen (Art. 1 Abs. 1 Grundgesetz). Diese Verknüpfung – die, wie gesagt, eine Besonderheit unserer Rechtsordnung darstellt – müsste eigentlich jedem die Augen dafür öffnen, dass gerade nicht jede Verletzung einer Datenschutznorm zugleich eine Missachtung des höchsten Verfassungsgebots darstellen kann; die Datenschutznorm ist möglicherweise ihrerseits überzogen, so dass sie das hohe Gut der Menschenwürde in allzu „kleine Münze" zerteilt und damit letztlich entwertet.

Der recht häufig vorkommende umgekehrte Schluss – weil der Datenschutz in Art. 1 Abs. 1 Grundgesetz verankert sei, sei mit jeder Einbuße an Datenschutz auch das Grundgesetz betroffen – mag zwar logisch erscheinen, ist aber für die rechtliche und politische Gewichtung sozialer Vorgänge geradezu irreführend. Schutz der Menschenwürde bedeutet Verbot der Folter, der Erniedrigung von Menschen, ihrer Bloßstellung und Knebelung. Auf den Schutz personenbezogener Daten wird die Menschenwürde-Formel mit einem sprachlichen Kunstgriff[116] ausgedehnt: Man sagt, der Mensch werde auch durch den Gebrauch seiner Daten „zum Objekt gemacht", und meint damit nicht nur die Unterwerfung unter den Willen eines ande-

115 Der Skandal liegt allerdings häufig darin, dass aus irgendwelchen Informationen falsche, unsichere oder verleumderische Schlüsse gezogen werden, die ihrerseits nicht begründet sind, oder dass Kontrahenten, Konkurrenten und Neider eine Person mit Informationen konfrontieren bzw. öffentlich diskreditieren, die nach Maßstäben des Rechts längst verjährt und in amtlichen Registern getilgt wären. Solche Vorgänge können durch noch so perfekte Vorschriften über den Umgang mit den Daten kaum verhindert werden. Man denke an die üblichen Verdächtigungen gegen mehr oder minder prominente Mitmenschen, die durch Indiskretionen oder Spekulationen befördert werden.

116 Und unter Vernachlässigung des Umstandes, dass der Persönlichkeitsschutz von den Gerichten aus dem allgemeinen Freiheitsrecht (Art. 2 Abs. 1 GG) *in Verbindung mit* Art. 1 Abs. 1 GG hergeleitet worden ist. Es geht also gar nicht um die „reine" Menschenwürde.

ren, sondern auch die unter ein Computerprogramm, mit dessen Hilfe andere den Einzelnen beeinflussen, eben die schon besprochene „Verdatung".

Das hat natürlich eine gewisse Plausibilität für sich, aber überzeugend ist es nur, wenn die Bezugnahme auf das höchste Verfassungsgebot durch Tatsachen gerechtfertigt ist. Die Kritiker blenden die Realität weitgehend aus, wenn sie auf der zweiten Stufe ihrer Argumentation regelmäßig behaupten: „Alles was möglich ist, wird tatsächlich realisiert". Hier kommt nun ein tiefsitzendes Misstrauen zum Ausdruck. Dieses Misstrauen gilt heute als Ausweis wahrer Liberalität; es grassiert nicht nur unter Anhängern der FDP, sondern ist in vielen Parteien präsent und beeinflusst auch die Entscheidungen von Parlamenten, Regierungen und Gerichten. Es geht zwar nicht so weit wie die Grundauffassung vieler US-amerikanischer Republikaner, dass alles schlecht sei, was der Staat anstelle der Einzelnen tut, aber es führt doch dazu, dass den staatlichen Stellen alles Schlechte zugetraut und alles Gute nur von der Gesellschaft, vom Volk erwartet wird. Diese moralische Zweiteilung der Welt ist naiv und behindert den Fortschritt. (Sie wird übrigens in dem Augenblick wieder aufgegeben, in dem auch die Gesellschaft zweigeteilt wird, nämlich in „gute" Individuen und „böse" Großunternehmen, gegen deren Macht wiederum der Staat helfen muss.)

Eine besondere Ironie der Geschichte liegt darin, dass die Bürgerrechtler, die besonders nachdrücklich auf die möglichen Gefährdungen der Individualrechte hinweisen, im Grunde nicht anders argumentieren als jene Vertreter der Sicherheitsbehörden, die ihre Ermittlungskompetenzen möglichst weit ins „Vorfeld" des Verbotenen ausdehnen wollen: Sie wollen ihrerseits rechtliche Schranken schon im „Vorfeld" des verbotenen Umgangs mit Daten errichten, damit potentielle Daten-„Sünder" gar nicht erst in Versuchung geraten können (und nehmen in Kauf, dass die dafür nötigen Schranken für die normale, rechtmäßige Datennutzung zu hoch werden). Die Kriminalisten wollen Informationen über die kriminelle „Szene", aus denen sie auf mögliche künftige Straftaten schließen können, um im konkreten Fall besser gerüstet zu sein; sie misstrauen ihrer eigenen Fähigkeit, geschehene Verbrechen ohne solche Vorfeldinformationen aufzuklären (und übersehen, dass die erforderlichen Informationen aus der Privatsphäre der Betroffenen stammen). Die Bürgerrechtler misstrauen den Behörden – und erst recht den Bürgern; denn sie halten es für ungewiss, ob die eindeutigen Verbote und Gebote (z.B.: bestimmte Informationen nicht an Arbeitgeber oder Vermieter und Polizei oder Verfassungsschutz weiterzugeben) eingehalten werden. „Sicher ist sicher" ist insofern das gemeinsame Motto von Datenschützern und Datenverarbeitern.

Zwei Beispiele für Risiko-Phantasien

An zwei Beispielen soll gezeigt werden, wie professionelle Datenschützer die Risiken beschreiben, die angeblich durch neue Techniken oder neue Methoden der Datenverarbeitung entstehen: das „Selbstmordwarnsystem" von Facebook und das schon einmal erwähnte Smart Metering.

Das Warnsystem, von dem die Rede ist, soll dazu dienen, dass Facebook-Mitgliedern, die in ihren Kontakten mit Freunden eine Suizidabsicht erkennen lassen, auf Hilfsangebote hingewiesen werden. Wer von einem Freund als selbstmordgefährdet gemeldet wird, erhält (nach einer Prüfung durch einen Facebook-Mitarbeiter) eine Nachricht mit der Aufforderung, sich Hilfe zu holen; die Telefonnummern von Hilfsorganisationen wie der Telefonseelsorge sind beigefügt. Eine Datenschutz-Beamtin soll dazu nach einem Zeitungsbericht in kritischer Absicht gesagt haben: Es sei „denkbar, dass Facebook genau für diejenigen, die in einer Lebenskrise stecken, entsprechende Werbung schaltet oder auch entsprechende Werbung nicht schaltet, also etwa keine Lebensversicherungen bewirbt".[117] Dass diese Möglichkeit als ein Risiko für einen Selbstmordgefährdeten angesehen wird, das durch rechtliche Regeln ausgeschlossen werden müsse, ist grotesk.

Durch das genaue Messen des Energieverbrauchs von Haushaltsgeräten soll nach verbreiteter Ansicht das Recht auf informationelle Selbstbestimmung gefährdet sein, außerdem auch die Unverletzlichkeit der Wohnung und das Grundrecht auf Integrität und Vertraulichkeit informationstechnischer Systeme, das „Computer-Grundrecht".[118] Metaphorisch werden die angeblichen Gefahren mit Begriffen aus der Optik beschrieben: Die Informationen bildeten einen „Datenschatten", eine „immer präzisere Abbildung" unserer Aktivitäten vom TV-Konsum über das Babywickeln bis zum nächtlichen Toilettengang; oder: unsere häuslichen Handlungen „spiegeln" sich vermeintlich im Stromverbrauch.[119] Wie das geschehen soll, wird in allgemeinen Wendungen umschrieben: die sensiblen Informationen „lassen sich gewinnen", heißt es, die Daten seien „interpretationsfähig", oder es wird einfach von der „Aussagekraft" der Daten gesprochen. Tatsächlich handelt es sich bei all diesen Interpretationen – die ganze Hefte von Fachzeitschriften füllen – stets um die gleichen Spekulationen: Man unterstellt aufgrund sehr schlichter Alltagserfahrungen, dass der oder die Bewohner sich in dieser oder jener Weise verhalten, wenn sie Haushaltsgeräte, Fernseher, Computer oder andere Stromverbraucher anstellen oder angestellt lassen. Davor, dass diese „Erkenntnisse" zur Überwachung der Bewohner genutzt werden, müssen diese nach der Ansicht der Beobachter geschützt werden. Dass ich aber in Wahrheit vielleicht gar nicht zusehe, wenn der Fernseher

117 Frisse 2012.
118 Hornung/Fuchs 2012, S. 21.
119 BfDI 2011, 57. S. a. Müller 2010; Roßnagel/Jandt 2010.

läuft, dass ich das Licht versehentlich oder absichtlich brennen lasse oder dass ich nachts lese, statt zu schlafen, dass man also etwas ganz anderes tut als die stromverbrauchenden Geräte ihrem Zweck gemäß zu nutzen, kommt nicht in den Blick. Selbst wenn es so ist, wie angenommen, wenn also die Bewohner zu bestimmten Zeiten das TV-Gerät anschalten und zu anderen ausschalten, ist nicht erkennbar, welche Schlüsse daraus die potentiellen Überwacher ziehen mögen. Natürlich möchte ich im Allgemeinen nicht, dass andere erfahren, welche Fernsehprogramme ich bevorzuge oder wann ich nachts aufstehe. Aber wen interessiert das wirklich?

Der einzig „harte Kern" all dieser Spekulationen ist die Sorge, dass Einbrecher meinen können, das Haus sei unbewohnt, wenn längere Zeit kein Strom oder Gas verbraucht wird. Auch dann besteht eine ernst zu nehmende Gefahr nur unter der Bedingung, dass die Verbrauchsdaten zeitnah einer kriminellen Szene zugänglich werden – was durch angemessene Datensicherung weitgehend verhindert werden kann. Ein anderes Schreckgespenst ist „der Versicherungsvertreter an der Haustür", der als belästigend empfunden wird; für ihn seien die Verbrauchsdaten „lukrativ im Beratungsgeschäft rund um Energieeffizienz" – [120] aber wo ist hier die Gefahr, der man mit den Mitteln des Rechts begegnen müsste? Schließlich wird befürchtet, dass Ermittlungsbehörden derartige Daten eines Tages auswerten könnten – aber warum sollte dieses (individuell sehr geringe) Risiko der rechtsstaatlich geordneten Strafverfolgung ausgeschlossen werden? Staatsanwaltschaften, Polizei und Justiz sind an die Strafprozessordnung gebunden; sie sind überdies geschult darin, Verdachtsmomente gezielt zu erarbeiten und nicht etwa pauschalen Spekulationen zu folgen. Die Datenschutzvorschriften im Energiewirtschaftsgesetz[121] reichen jedenfalls aus, die Daten vor der normalen Neugierde Dritter abzuschirmen und die phantasievollen Gefahrenszenarios zu verhindern.

Misstrauen auf allen Ebenen

Erstaunlicherweise hat sich gerade auch das Bundesverfassungsgericht dabei hervorgetan, die Missbrauchsmöglichkeiten aufzuzeigen, die aus mehrdeutigen oder zu weit gefassten Gesetzesbegriffen erwachsen. Ohne empirische Nachweise hat das oberste Gericht mehrfach ausgemalt, was alles mit den gesammelten Daten geschehen könne, wenn Beamte ihre Befugnisse extensiv auslegen.

So hat man sich vorgestellt, dass die Kfz-Kennzeichen, die von automatischen Erfassungsgeräten der Polizei gelesen und für Fahndungszwecke ausgewertet werden dürfen, mit anderen Daten verknüpft und dann dazu benutzt werden könnten, „Informationen über einen ganzen Kriminalitätsbereich, das Umfeld, die ‚Szene'

120 Heckmann 2011 a, S. 3.
121 § 21 g EnWG mit Rechtsverordnungsermächtigung in § 21 i Abs. 1 Nr. 4.

und den gesellschaftlichen Hintergrund zu sammeln" – also auch über „einen Personenkreis, der durch sein Verhalten keinen Anlass für die Aufnahme in den Fahndungsbestand gegeben hat".[122] Weil das im Gesetz angeblich nicht klar genug ausgedrückt war, hat das Gericht die Befugnis annulliert, überhaupt Lesegeräte zu benutzen.

Den Kern der Begründung des Urteils zur Kfz-Kennzeichenerfassung bildet die Sorge, durch die „vielfältigen Nutzungs- und Verknüpfungsmöglichkeiten" könnten „weitere Informationen erzeugt und so Schlüsse gezogen werden, die sowohl die grundrechtlich geschützten Geheimhaltungsinteressen des Betroffenen beeinträchtigen als auch anschließende Eingriffe in seine Verhaltensfreiheit nach sich ziehen können".[123] Die Richter ziehen ihrerseits „Schlüsse", ohne sich und den Lesern klar zu machen, ob denn die „möglichen" Nutzungen und Verknüpfungen zulässig wären und auf welche Weise sich Eingriffe „anschließen" sollten. Ich muss es wiederholen: Das Bundesverfassungsgericht misstraut den handelnden Beamten; es vermutet letztlich, diese würden ihre Amtspflicht verletzen, sich gesetzeskonform zu verhalten und ihre Kompetenzen nicht nur formal einzuhalten, sondern auch den Sinn und Zweck der Befugnisnormen zu beachten. Für ein Gericht ist das eine befremdliche Einstellung. Seine Aufgabe ist nicht, über Möglichkeiten zu spekulieren, sondern das Recht durchzusetzen, und zwar gerade auch gegen sinnwidrige extensive Auslegung, gegen eine Praxis, die den Grundsatz der Verhältnismäßigkeit missachtet. Wie eigenwillig diese Rechtsprechung ist, ergibt sich auch daraus, dass das Gericht die Befugnisnorm gebilligt hätte, wenn sie nur detaillierter formuliert gewesen wäre. Der freiheitsfördernde Effekt dieser Judikatur verpufft also, wenn der Gesetzgeber immer kompliziertere Vorschriften erlässt!

Das Misstrauen mancher Beobachter gegen die Datenverarbeitung der Behörden geht so weit, dass sogar die Stelle des Bundes, die der Sicherheit in der Informationstechnik dienen soll, als potentielle Überwachungsinstanz angesehen wird. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat nach dem Gesetz sorgfältig eingegrenzte Befugnisse. Es darf u.a. die „Protokolldaten, die beim Betrieb von Kommunikationstechnik des Bundes anfallen, erheben und automatisiert auswerten, soweit dies zum Erkennen, Eingrenzen oder Beseitigen von Störungen oder Fehlern bei der Kommunikationstechnik des Bundes oder von Angriffen auf die Informationstechnik des Bundes erforderlich ist".[124] Die automatisierte Auswertung muss „unverzüglich" erfolgen, und die Daten müssen „nach erfolgtem Abgleich sofort und spurenlos gelöscht werden".[125] Seitenlange Detailvorschriften sollen sicherstellen, dass die Daten wirklich nur für den gesetzlichen Zweck ver-

122 BVerfGE 120, 378 (410 f.).
123 BVerfGE 120, 378 (398).
124 § 5 Abs. 1 Satz 1 Nr. 1 des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz) v. 14. 8. 2009 (BGBl. I S. 2821).
125 § 5 Abs. 1 Satz 2 BSI-Gesetz.

wendet werden. Nun aber liest man, dass zwei prominente „Datenschützer“ (ein Bundestagsabgeordneter und ein freiberuflich tätiger Experte) meinen, diese Daten dürften nicht ohne „konkreten Anlass“ aufgezeichnet werden. Denn dabei könne „beispielsweise ermittelt werden, wer sich auf dem Internetportal der Bundeszentrale für gesundheitliche Aufklärung über Impotenz informiert hat“. Was um Himmels willen werden die Datensicherheits-Experten des BSI mit dieser Information anfangen? Stellen sich die Beschwerdeführer wirklich vor, irgendjemand werde die zu Kontrollzwecken gespeicherten Daten aus privater Neugierde durchsehen und etwa damit rechnen, einen Bekannten mit solch einer Information blamieren oder lächerlich machen zu können? Nachdem sie mit dieser Beschwerde beim Bundesverfassungsgericht nicht zum Erfolg gekommen sind, haben sie jetzt den Europäischen Gerichtshof für Menschenrechte angerufen.[126] Man sollte das ohnehin überlastete Straßburger Menschenrechtsgericht nicht mit derart weltfremden Klagen behelligen.

Die Sorge, dass die Beamten ihre Rechte extrem weit interpretieren oder gar überschreiten würden, findet sich freilich auch bei einigen Insidern. Manche trauen ihren Kollegen sehr wohl zu, sich über rechtliche Grenzen hinwegzusetzen, sobald die Gelegenheit günstig ist. „Ich kenne meine Pappenheimer“, sagt einer, der jahrelang als Kriminalbeamter gearbeitet hat und heute einen anderen Beruf ausübt, nachdem er sich bei den Kollegen durch liberale Ansichten unbeliebt gemacht hat. Andere Kenner der Sicherheitsbehörden erblicken dort ebenfalls ein großes Maß an Jagdeifer und manchmal ein zu geringes Maß an rechtlichen Skrupeln.

Gemeinsam ist vielen Zweiflern also, dass sie Rechtsverletzungen von großem Gewicht nicht nur für möglich, sondern sogar für wahrscheinlich halten. Viele übersehen jedoch, dass der tatsächliche Eintritt von Grenzüberschreitungen noch von einer weiteren Bedingung abhängig ist, nämlich von fehlender Abschreckung und erfolgloser *Kontrolle*. Die Akteure der Datenverarbeitung sind in das dichte Netz der Datenschutzbestimmungen eingebunden; sie sind der Aufsicht unabhängiger Datenschutzbeauftragter unterworfen und müssen ihre Handlungen gegenüber Aufsichtsbehörden und Gerichten verantworten – ganz zu schweigen von der Kontrolle durch die Medien, die von vielen mehr gefürchtet werden als die Justiz.

Es ist verzeihlich, wenn jemand, der die Technikentwicklung allein aus der Perspektive des Informatikers oder Elektronikers verfolgt, die technische Machbarkeit mit der Verwirklichung von Rechtsverletzungen gleichsetzt. Einen solchen Kurzschluss sollte sich aber niemand leisten, der regelmäßig soziale, wirtschaftliche und politische Vorgänge beurteilt. Manager und Beamte, Journalisten und Sozialwissenschaftler wissen, dass es viele Faktoren sind, die das Verhalten der Menschen bestimmen. Sie sollten die *Interessenlage* der Akteure realistisch einschätzen und

126 Bericht (dapd) in der Süddeutschen Zeitung vom 25. 1. 2012.

überlegen, wie hoch für diese selbst das Risiko ist, wegen Pflichtwidrigkeiten bestraft, vielleicht sogar aus dem Dienst entfernt zu werden.

Wenn man sich z.B. vorstellt, Polizeibeamte könnten systematisch die Telekommunikations-Verbindungsdaten einzelner Personen „auf eigene Rechnung" zu Lasten der Betroffenen „vermarkten", also etwa „Dossiers" und „Bewegungsprofile" bestimmter Mitmenschen herstellen und an private Interessenten verkaufen, wird man auf den Gedanken kommen, dass es dazu eines Kreises potentieller Käufer bedarf. Schon diese Bedingung dürfte nicht ganz einfach zu erfüllen sein. Ein Interesse Außenstehender ist zwar vorstellbar, und sei es, dass jemand auf diese Weise klären will, ob sein zukünftiger Schwiegersohn eine „weiße Weste" hat. Belastende Informationen können für Konkurrenten und Nebenbuhler wertvoll sein. Aber es dürfte schwierig sein, einen ertragreichen Markt für solche Informationen aufzubauen – schwieriger jedenfalls als etwa illegal mit Waffen zu handeln. Dass der Informationshandel aber über kurz oder lang von den korrekt handelnden Kollegen entdeckt und aufgelöst werden wird, ist schon deshalb ziemlich sicher, weil Abfragen aus dem Polizeicomputer automatisch dokumentiert werden. Die illegalen Datenhändler müssten mit der Entlassung rechnen. Es ist tatsächlich schon vorgekommen, dass pflichtvergessene Beamte persönliche Daten aus polizeilichen Beständen „privat" an Dritte gegeben haben, um ihnen gefällig zu sein oder weil ihnen dafür Geld geboten wurde. Sie wurden bestraft, und niemand behauptet, solche Fälle seien typisch für die ganze Polizei.

Gesetze werden nicht dadurch unbrauchbar, dass viele gegen sie verstoßen – im Gegenteil! Wäre dem so, hätten wir das Strafgesetzbuch und viele andere Normen längst abschaffen (oder durch wesentlich schärfere Gebote ersetzen!) müssen. Gleichwohl ist es ein beliebtes Argumentationsmuster, dass wegen der Möglichkeit von Rechtsverstößen die Nutzbarkeit von Datensammlungen eingeschränkt werden sollte. Aus Angst vor dem Fehlgebrauch wollen viele den normalen Gebrauch von Dateien bis zur Unzumutbarkeit erschweren.

Die Beschwörung des Unrechtsstaates

Die äußerste Form dieser Argumentation besteht in der Beschwörung eines diktatorischen Regimes, das alle bisherigen Sicherungen über den Haufen wirft. Wenn die Diskussion zu der Feststellung gelangt ist, dass die Risiken von Missbrauch und Pflichtverstößen in unserem heutigen Staat begrenzt und beherrschbar sind, erscheint prompt auf dem Podium das Extremargument: Wir dürfen einer künftigen autoritären, rechtsfeindlichen Regierung nicht die Mittel in die Hand geben, uns vollständig zu unterdrücken. Haben nicht die Nazis die Einwohnerkarteien, Personenstandsregister und Kirchenbücher zur Judenverfolgung genutzt? Hat nicht die

DDR ein technikgestütztes Informationssystem über alle aufgebaut, die der kritischen Distanz zur herrschenden Partei verdächtig waren? Nutzen nicht Diktatoren zunehmend das Internet, um geheime Opposition aufzudecken und zu zerschlagen?

Ja, das ist alles richtig – und doch einseitig und unvollständig.[127] Die Nationalsozialisten waren schon im Besitz der Macht, als sie ihre Verfolgungen begannen, und ihre „Machtergreifung" war durch andere Faktoren begünstigt als gerade durch Technik. Die Technik, die von der Stasi benutzt wurde, war nach heutigen Maßstäben unzureichend. Aber das MfS hatte reichlich menschliche Mitarbeiter, die das Volk mit ganz konventionellen Methoden ausspionierten und Dissidenten denunzierten. Geht man in der Geschichte weiter zurück, kommt man zu dem Schluss, dass die Herrscher zwar von der Entwicklung der Waffentechnik profitierten, dass sie aber bei der Unterdrückung ihrer Völker sogar ohne Schreibmaschine und Drucker auskamen. Diktaturen entstehen nicht, weil es perfekte Informationssysteme gibt, sondern weil handgreiflich Gewalt ausgeübt wird, weil die Menschen die Demokratie nicht energisch genug verteidigen oder weil sie von den Machthabern bestochen werden. Man lese die Literatur über das Ende der Weimarer Republik; da finden sich reichlich Belege für diese These.

Selbst wenn man die Bedeutung der Technik stärker gewichtet: Solange wir in rechtsstaatlichen Verhältnissen leben und auf absehbare Zeit keine Revolution zu erwarten ist, wäre ein Verzicht auf die Nutzung von Informationstechnik nicht zu rechtfertigen. Nicht nur Informationstechnik, sondern viele Arten technischer Produkte, angefangen beim Messer, beim Hammer oder beim Motor, können sowohl für gute wie für schlechte Zwecke genutzt werden. Niemand will Messer und Hammer verbieten, obwohl damit Menschen getötet werden können. Weil es diese Ambivalenz gibt, spricht man z.B. bei der Kontrolle des Waffenhandels von „dual use": Viele für militärische Zwecke geeignete Geräte werden in Friedenszeiten für friedliche Verwendungen eingesetzt: Lastwagen können Lebensmittel, aber eben auch Raketen befördern. Niemand denkt daran, Lastwagen zu verbieten oder ihre Nutzung aufs strengste einzuschränken, weil sie unter Umständen auch Kanonen zum Einsatzort bringen.

Was es bedeutet, wenn wir uns „vorauseilend vor Gewalten ducken, die in Zukunft einmal kommen könnten", hat besonders deutlich der Blogger Christian Heller formuliert:

> „Es verschafft vielleicht ein Sicherheitsgefühl. Aber sehr viel tatsächliche Sicherheit steckt hinter diesem Gefühl nicht. Vorauseilendes Ducken führt vor allem zu einem: dass man schon hier und heute so lebt, als wäre die Diktatur längst über uns gekommen.

127 Dazu sehr klarsichtig auch Heller 2011, S. 102 ff., 158 ff.

> Doch mit Duckmäusertum und Flucht ins Verborgene lässt sich keine Freiheit verteidigen. Gibt es eine gesellschaftliche Freiheit, dann muss sie auch laut und stolz in Anspruch genommen, immer wieder neu behauptet und ausgereizt werden. Sich zu verstecken und den Mund zu halten, das kann unter den Bedingungen von Diktatur, Diskriminierung und Intoleranz eine überlebensnotwendige Taktik sein. Aber wer es vorauseilend tut, der wartet diese Umstände nicht nur ab, der arbeitet ihnen durch seine Zurückhaltung vielleicht sogar zu.“[128]

Verdatet und verkauft? Die Standardbeispiele

Als Beispiele für besonders bedenkliche Informationssammlungen werden regelmäßig zwei Fallgruppen diskutiert: die Verwendung von Kundendaten zu Werbezwecken und die polizeiliche oder nachrichtendienstliche Überwachung. Beide Themen sind freilich bei genauer Betrachtung sehr viel differenzierter zu beurteilen.

Persönlichkeitsprofile aus Kundendaten

Dass Unternehmen von ihren Kunden Daten erheben und diese dann zu Werbe- und Marketingzwecken auswerten, gilt vielen – wenn nicht der Mehrheit der Menschen – als anstößig, und zwar schon lange vor der Einführung des Internets. Man empört sich darüber, dass Handelsunternehmen sich Namen, Anschriften und Geburtstage von Kunden geben lassen und diese Daten dazu benutzen, mit individuell adressierten Sendungen für ihre Waren zu werben. Man findet es unangenehm, dass solche Unternehmen zum Zwecke der Kundenbindung Rabatt- oder andere Vergünstigungssysteme einführen und dabei weitere Angaben speichern, z.B. die Art der gekauften Waren.

Was also geschieht, wenn Unternehmen systematisch Informationen über bestimmte Personen sammeln (zum Beispiel Angaben aus Bestellungen, Zahlungsvorgängen oder dem Anklicken bestimmter Internetangebote)?[129] Sie fertigen „Persönlichkeitsprofile“ an. Sie stellen aus den verschiedenen Einzelinformationen eine Art Mosaik zusammen, das die Vorlieben und Abneigungen, typische Verhaltensweisen, häufige Aufenthaltsorte und ähnliche Charakteristika der betreffenden Personen wiedergibt. Für Werbezwecke werden aus diesen „Profilen“ Personen*gruppen* gebildet, die in gleicher Weise angesprochen werden. Man erarbeitet

128 Heller 2011, S. 160.
129 Zu den üblichen Verfahrensweisen s. etwa Pariser 2011 sowie Kurz/Rieger 2011, S. 13 ff..

also eine Sammlung von Namen und Adressen, an die aus bestimmten Anlässen (neue Angebote, Sonderaktionen, Umfragen usw.) mit Hilfe automatischer Drucker zahllose gleiche, aber persönlich adressierte Briefe geschrieben werden.

Sämtliche Methoden der Kundendatenauswertung beruhen auf der Grundüberlegung von Psychologen und Marketingexperten, dass jemand, der einmal oder mehrfach bestimmte Waren bestellt oder Interessen oder Vorlieben gezeigt hat, auch ein zweites oder drittes Mal gleiche oder bestimmte andere Bestellungen aufgeben werde. Diese Grundidee wird x-fach variiert; denn man nimmt an, dass Entscheidungen für die eine Ware oder die eine Dienstleistung Interesse auch für andere – teils verwandte, teils einer anderen Warenart oder Dienstleistungssparte zuzuordnende – Angebote vermuten lässt. Nonkonformistische Auswahlentscheidungen oder vorgetäuschtes Interesse kommen in diesem Kalkül nicht vor. Wenn ich mich einmal über Babywäsche informiert habe, werde ich als jemand angesehen, der sich dauernd für Strampler interessiert. Wenn ich im Internet esoterische Literatur gekauft habe, gelte ich als Liebhaber dieser Gattung. Dass es sich um einmalige Neugierde gehandelt haben kann oder dass ich jemand anders mit dieser Ware beglücken wollte, kann das System nicht erkennen. Dass man manche Druckerzeugnisse gerade deshalb erwirbt, um die Gegenposition zur eigenen Meinung kennenzulernen, ist in der Perspektive der Werbepsychologen nicht vorgesehen. Sie können derartige Abweichungen vom Mainstream nicht berücksichtigen und liegen schon deshalb oft falsch.

Das millionenfach propagierte Bild vom „gläsernen Menschen" führt in die Irre. Die Adressaten sind nur scheinbar transparent. Durch Glas kann man hindurchblicken, die Außenhaut durchdringen, aber was sieht man als Ergebnis der Datensuche und Datenauswertung, sei sie noch so raffiniert angelegt? Jedenfalls nicht die Seele, die geheimen Regungen des Individuums! Der gläserne Mensch ist wie das vom Fleisch befreite Skelett: ein Ausstellungsstück, aber kein Individuum. Die Person, die gemeint ist, lässt sich damit nicht fassen. Die entindividualisierten Abbilder real existierender Menschen sind so wertvoll wie eben eine Adresssammlung potentieller Kunden sein kann.

Warum die Firmen dies praktizieren, ist schon gesagt worden: Sie schließen aus bisherigen Einkäufen auf künftige, hoffen auf die Wiederholung der Routinevorgänge, wollen Kunden an sich binden und neue gewinnen. Das gelingt in vielen Fällen, in anderen misslingt es. Aber in keinem Fall ist der so angesprochene Kunde „verdatet und verkauft". Jeder ist und bleibt frei darin, die Werbesendungen in den Papierkorb zu werfen oder auf dem Computer zu löschen. Insofern besteht kein Unterschied zwischen gezielter und ungezielter Werbung. Dass die Wirtschaftswerbung mit Personendaten hierzulande seit Jahrzehnten Gegenstand einer derart intensiven und teilweise fanatischen Diskussion ist, lässt an unserem Urteilsvermögen zweifeln. In ärmeren Ländern wird man diese Diskussion für die Luxusbe-

tätigung einer Überflussgesellschaft halten und meinen, wir hätten keine anderen Probleme – in Wahrheit haben auch wir wichtigere und sollten unsere Kräfte darauf konzentrieren.

Schutz vor Belästigung – und vor wirklichen Nachteilen

Was der Papierkorb nicht leistet, ist die Abwehr unerwünschter „Anmache". Es ist in erster Linie das Recht des *Verbraucherschutzes*, das die Methoden der Kundenwerbung beschränkt: die unlautere Werbung, die unerbetenen „cold calls", die Überrumpelung der Angesprochenen am Telefon. Diese Rechtsmaterie ist in den letzten Jahren ausgebaut und verfeinert worden und schützt uns jetzt ziemlich umfassend gegen unfaire Methoden. So ist nunmehr die Werbung mit Telefonanrufen, Fax- und E-Mail-Sendungen gegenüber Verbrauchern verboten, wenn keine vorherige ausdrückliche Einwilligung des Angerufenen bzw. Adressaten vorliegt. Auch die Verwendung automatischer Anrufmaschinen gilt als „unzumutbare Belästigung".[130]

In manchen Fällen kommt hinzu, dass die verwendeten Anschriften auf fragwürdige Weise erlangt worden sind, so wenn Kundendaten ohne die erforderliche Einwilligung gespeichert und weitergegeben wurden. Diese Form der Datennutzung ist ebenfalls vor einiger Zeit strenger als zuvor geregelt worden, und das geltende Recht macht es den Adresshändlern ziemlich schwer, ihre Bestände weiter zu verwenden, zu aktualisieren und zu erweitern.[131] Andererseits ist es durchaus möglich, dass die Sammlung der Daten rechtmäßig war und sich Betroffene trotzdem mit Recht über die Art und Weise beschweren, wie ihnen Werbung geschickt wird – zum Beispiel wenn entgegen einem Aufkleber „Keine Werbung" der Briefkasten vollgestopft wird. Der Datenschutz ist also, wenn überhaupt, nur marginal und indirekt einschlägig. Er ist nicht zu dem Zweck eingeführt worden, die Papierproduktion für überflüssige Werbung zu beschränken. Den Zweck, vor Belästigungen zu schützen, erfüllt das Verbraucherschutzrecht, ohne auf die Gefühle der Betroffenen abzustellen und ohne den moralgeladenen Hintergrund des Menschenwürdeschutzes.

Das hat sich aber noch nicht überall herumgesprochen. So hat das Landgericht Lüneburg vor einiger Zeit den Absender einer Werbesendung zur Unterlassung verurteilt und dies nicht nur damit begründet, dass es sich um eine unzumutbare Belästigung handle, sondern auch dass damit in das Recht auf „informationelle

130 § 7 Abs. 2 Nr. 2 und 3 des Gesetzes gegen den unlauteren Wettbewerb (UWG) i.d.F.v. 3.3.2010, BGBl. I S. 254.
131 §§ 28, 29 BDSG i.d.F.v. 14.8.2009, BGBl. I S. 2814.

Selbstbestimmung“ eingegriffen werde.[132] Das ist eine merkwürdige Grundrechtsinterpretation: Mein angebliches Recht, selbst zu bestimmen, welche Daten über mich verwendet werden dürfen, soll als Hebel dienen, um zu verhindern, dass jemand mir unter meiner zutreffenden Anschrift etwas schickt! Nicht die Speicherung oder Weitergabe der Adresse war hier rechtswidrig, sondern (vielleicht) die Zustellung. Übrigens: Wenn der Zeitungsbericht über diese Entscheidung richtig ist, war die Werbung gar nicht adressiert, sondern es handelte sich um ein durch Boten oder durch die Post verbreitetes Anzeigenblatt. Es ging also nicht um informationelle Selbstbestimmung, sondern um den Schutz vor unbefugter Benutzung eines fremden Briefkastens.

Sieht man davon einmal ab und versucht herauszufinden, was den Betroffenen durch eine unerwünschte Benutzung ihrer Namen und Adressen angetan wird, bleibt herzlich wenig übrig. Die Unternehmen spionieren nicht hinter ihren Kunden her – täten sie dies, würden sie die gewünschte Kundenbindung selbst zunichtemachen und wären schnell allgemein in Verruf. Auch die Auswertung von Kaufgewohnheiten und Vorlieben ist keine Bosheit, mag auch mancher es bedauern, dass er immer wieder Gleiches angeboten bekommt und die Unternehmen ihm nicht einmal etwas überraschend Neues vorschlagen.

Dass die aus der allgemeinen Vernetzung entstehenden Unannehmlichkeiten auch ohne Berufung auf den Datenschutz bekämpft werden können, zeigt ein Urteil des Landgerichts Köln, das sich mit der unverlangten Zusendung von E-Mail-Werbung befasst: Zwar wurde der Unterlassungsklage eines Rechtsanwalts gegen den E-Mail-Versender stattgegeben, aber nur mit der Begründung, es handle sich um einen unzulässigen Eingriff in den „eingerichteten und ausgeübten Gewerbebetrieb“ des Anwalts; zum Datenschutz enthält dieses Urteil nichts.[133]

Wer sich schon dadurch beeinträchtigt fühlt, dass er von einer Firma mit seinem korrekten Namen angesprochen und an seine früheren Einkäufe erinnert wird, moniert im Kern, dass in der Verwendung der Daten eine Missachtung der Persönlichkeit liege. Wer nicht will, dass die beteiligten Unternehmen seine Existenz zur Kenntnis nehmen wollen, hält den Gebrauch und erst recht den Verkauf von Daten über ihn oder sie für eine Verletzung des Selbstbestimmungsrechts. Aber die werbenden Unternehmen wollen natürlich keinesfalls ihren möglichen Kunden zu nahe treten; tatsächlich erfahren sie ja gar nicht, welche konkreten Personen in ihren Werbekampagnen angesprochen werden. Die Computer, die derartige Aufträge ausführen, „wissen“ nicht, an wen die Briefe gehen, und „wollen“ gar nichts. Irgendwelche Schäden oder Nachteile materieller Art treten nicht ein, solange die Kundendaten – wie es ganz überwiegend geschieht – nur für Werbung und Marketing verwendet werden.

132 Az. 4 S 44/11, Bericht im Hamburger Abendblatt vom 6.1.2012.
133 Urteil des Landgerichts Köln v. 13.10.1998, abgedruckt bei Kröger/Hanken 2003, S. 523 ff.

Die allenthalben geäußerte Empörung über diese Praxis steht in einem befremdlichen Gegensatz zu der Selbstverständlichkeit, mit der wir von der Wirtschaft Erfolg und immer mehr Expansion erwarten. Existenzgründer sind auf Adressen potentieller Kunden angewiesen, und ein Unternehmen, das neue Kundenkreise sucht, kann nicht erst alle in Betracht kommenden Besteller fragen, ob sie überhaupt (per Post) angesprochen werden möchten (anders, wie gesagt, ist es bei der Telefonwerbung). Ich behaupte, dass die ganz überwiegende Mehrheit derer, die vor die Alternative gestellt würden, Werbung zu akzeptieren oder einen Rückgang des Wirtschaftswachstums hinzunehmen, sich für die erste Alternative entscheiden würde. So sensibel ist wohl kaum jemand, dass er die Datennutzung der werbenden Wirtschaft als schlechthin unerträgliche Kränkung seines informationellen Selbstbestimmungsanspruchs ansähe. Wer in diesem Zusammenhang behauptet, die Menschenwürde selbst sei verletzt, wenn eine Firma Namen und Anschriften regelwidrig verwendet, greift entschieden zu hoch – ich erkenne hier ein gehöriges Maß an Wichtigtuerei.

Wirkliche Nachteile entstehen jedoch aus der Verwendung von Kundendaten, wenn auf dieser Grundlage Entscheidungen zu Lasten der Kunden getroffen werden. So wird die Sammlung und Übermittlung von Daten über Zahlungsvorgänge zum Risiko für die Betroffenen, wenn daraus Aussagen über die Kreditwürdigkeit abgeleitet oder Personalentscheidungen getroffen werden sollen. Die Schufa[134], die Kreditauskunfteien und Detekteien leisten solche Dienste, und man darf vermuten, dass schon vielen Bank- und Sparkassenkunden ein Kredit verweigert worden ist, weil diese Institute negativ bewertete Angaben übermittelt haben. Aber diese Praxis ist schon lange von den Datenschutz-Aufsichtsbehörden kritisch untersucht und in vielerlei Hinsicht kritisiert worden; die Branche selbst und der Gesetzgeber haben reagiert und strengere Regeln eingeführt.[135] Das Verbot der Ableitung nachteiliger Entscheidungen aus automatisierter Datenauswertung (§ 6 a BDSG) wird leider weithin ignoriert.

Wieder anders ist die Lage natürlich, wenn Daten gestohlen und für Betrügereien verwendet werden. Selbstverständlich muss es verhindert werden, dass jemand unter fremdem Namen Bestellungen aufgibt oder kompromittierende Äußerungen versendet oder gar ins Netz stellt. Aber das ist so unbestritten wie die Geltung des Strafgesetzbuches – dass trotz des geltenden Rechts Betrug und Diebstahl vorkommen, deutet nicht auf eine Lücke im Gesetz, sondern Missachtung desselben. Der Vollzug des Datenschutzrechts ist kein politisches Thema, sondern eine Aufgabe der Aufsichtsbehörden und Gerichte – und vor allem der Bürger selbst, die

134 „Schutzvereinigung für allgemeine Kreditsicherung", die Vereinigung der Banken und Sparkassen zum gegenseitigen Informationsaustausch über ihre Kunden.

135 So sind in der Datenschutznovelle 2009 insbesondere die Datenübermittlung an Auskunfteien (§ 28 a BDSG) und das Scoring (Einschätzung der Kreditwürdigkeit aufgrund von Datenanalysen) strenger geregelt worden (§ 28 b BDSG).

sich im täglichen Umgang mit Informationen über Dritte angemessen und fair verhalten sollen. Wenn die Betroffenen von Rechtsverstößen erfahren, können sie sich an staatliche Stellen wenden, die ihnen helfen.

Die beste Vorbeugung gegen Datenmissbrauch besteht übrigens darin, die Regeln der Daten*sicherung* ernst zu nehmen. Hier liegen die Herausforderungen für Informatiker und Techniker. Sie sind es, die ganz praktisch und konkret dafür sorgen müssen, dass die Daten auf den diversen Rechnern und im Netz wirklich sicher sind, dass sie an die richtigen Adressaten geleitet und nicht zwischendurch abgezapft werden. Die gesetzlichen Vorschriften zur Datensicherung sind einigermaßen klar (wenn auch immer noch verbesserungsbedürftig), und die untergesetzlichen Standards und Gebrauchsanleitungen müssen von der Gemeinschaft der Experten erarbeitet und durchgesetzt werden. Die Politiker können die öffentliche Verwaltung dazu nötigen, sich an diese Regeln zu halten; der Ruf nach neuen Gesetzen hilft hier gar nichts.

Das Beispiel Vorratsdatenspeicherung

Kriminalisten gehen anders an die Arbeit. Wenn sie das „Profil" eines gesuchten Straftäters zeichnen wollen, müssen sie gezielter vorgehen als die Marketingleute. Eine Gruppenbildung reicht ihnen nicht aus, sozialpsychologische Gesetzmäßigkeiten mögen ergänzend eine Rolle spielen, aber die Auswertung von Kundendaten dürfte ihnen im Zweifel kaum weiterhelfen. Für manche Straftaten ist es nützlich, Kontobewegungen Verdächtiger zu verfolgen; das ist in gewissem Rahmen zulässig, um die organisierte Kriminalität zu bekämpfen. Bei Rasterfahndungen werden nach recht groben Kriterien Gruppen gebildet, um daraus durch Abgleich mit vorhandenen Daten überhaupt erst einen Kreis von Verdächtigen herauszuarbeiten; erst *nach* diesem Auswahlprozess beginnt die kriminalistische Ermittlungsarbeit an den einzelnen Datensätzen.

Keine Datensammlung hat so viel Empörung ausgelöst wie die „Vorratsdatenspeicherung": die Speicherung der Verkehrs- oder besser Verbindungsdaten aus unseren alltäglichen Telekommunikationsbeziehungen (Telefon, E-Mail, Fax, Internetverbindungen). Wenn diese Angaben ausgewertet werden, lassen sich daraus sämtliche technisch vermittelten Kommunikationen aller Personen zusammenstellen, die sich auf dem Staatsgebiet befinden oder befunden haben. Sicherheitsbehörden können auf diese Weise herausfinden, wer mit wem in Kontakt steht oder gestanden hat, und aufgrund der Besonderheiten solcher Kommunikationsprofile (z.B. der Kommunikationspartner, der Häufigkeit und dem Ort des Gesprächs oder des Internetanschlusses) kann man weiter „kombinieren". Aus auffälligen Verhaltensweisen können kriminalistische Schlüsse gezogen werden, und vielleicht er-

geben sich aus solchen Spekulationen sogar Hinweise auf Eigenschaften einzelner Personen.

Solche Vermutungen und Schlussfolgerungen können entscheidend zur Aufklärung von Straftaten beitragen. So wäre vielleicht auch die Mordserie der Zwickauer Neonazis mit Hilfe von Telefonverbindungsdaten vor Jahren aufklärbar gewesen – wenn man diese Vorratsdaten damals gehabt und ausgewertet hätte, um das Unterstützernetz aufzuspüren und damit an die Täter heranzukommen (das liegt freilich so lange zurück, dass es keine Rolle mehr spielt, ob die Vorratsdatenspeicherung heutzutage zulässig ist oder nicht). Auch zur Abwehr von Angriffen auf Leib und Leben, seien es terroristische Attentate oder „normale" Gewalttaten, kann die Möglichkeit, die Telekommunikations-Kontakte Verdächtiger zu untersuchen oder aus den Daten Dritter auf verdächtige Kontaktpersonen zu schließen, von großem Nutzen sein.

Es liegt auf der Hand, dass eine solche Datensammlung riesige Ausmaße annimmt. Auch wenn die Daten – wie geschehen – „nur" für sechs Monate aufbewahrt werden mussten, waren die erforderlichen Speichervolumina gewaltig – ein Grund für die Telekommunikations-Unternehmen, sich heftig gegen diese Pflicht zu wehren, zumal sie dafür nicht entschädigt werden sollten. Vor allem aber wandten sich viele Bürger gegen die gesetzliche Ermächtigung zu dieser Datensammlung. Einige Prominente, darunter die spätere Bundesministerin der Justiz, Sabine Leutheusser-Schnarrenberger, und ihr Parteifreund Burkhard Hirsch, erhoben in Karlsruhe Verfassungsbeschwerde, und über dreißigtausend andere schlossen sich ihnen an. Die liberalen Medien unterstützten diesen juristischen Kampf gegen eine „Errungenschaft" der Kriminalistik, die ihnen als ein gigantischer Einbruch in die Freiheit des Individuums erschien. Überall las man, die Sammlung dieser Daten ermögliche „besonders intensive Grundrechtseingriffe".

Das hohe Bundesverfassungsgericht hat daraufhin die Vorratsdatenspeicherung zwar als kriminalistisches Instrument gebilligt, aber ihre Regelung im Telekommunikationsgesetz und in der Strafprozessordnung für verfassungswidrig erklärt. Es hat einerseits betont, dass die Verbindungsdaten „für eine effektive Strafverfolgung und Gefahrenabwehr von besonderer Bedeutung" sind. Auch gegen die Dauer der Speicherpflicht – sechs Monate – hatten die Richter keine Bedenken, wohl aber gegen die gesetzliche Ausgestaltung: Es fehle an „hinreichend anspruchsvollen und normenklaren Regelungen hinsichtlich der Datensicherheit, der Datenverwendung, der Transparenz und des Rechtsschutzes".[136] Deshalb verstießen die Vorschriften gegen das Fernmeldegeheimnis (Art. 10 Grundgesetz).

Die Kläger hatten argumentiert: Die Speicherung sei gar nicht geeignet, organisierte Kriminalität zu bekämpfen und terroristische Anschläge zu verhüten. Der

136 Urteil des Bundesverfassungsgerichts v. 2.3.2010, BVerfGE 125, S. 260 ff.

Eingriff in das Fernmeldegeheimnis sei deshalb so schwer, weil „alle Menschen" betroffen seien, „die Telekommunikationsdienste für die Öffentlichkeit in Anspruch nehmen". Andererseits meinten die Beschwerdeführer (mit Recht), „die Wahrscheinlichkeit, dass die gespeicherten Daten später zu Gefahrenabwehr- oder Strafverfolgungszwecken benötigt würden, sei verschwindend gering". Daraus schlossen sie aber nicht, dass die ganze Sammlung harmlos sei, sondern beriefen sich darauf, dass die Speicherung „das Risiko" erhöhe, „zu Unrecht Ermittlungsmaßnahmen ausgesetzt oder unschuldig verurteilt zu werden. Außerdem könnten solche Daten „gezielt gegen missliebige Personen eingesetzt werden". „Nur das Absehen von der Speicherung schütze wirksam vor Missbrauch".[137] – Einen besonderen Teil der Beschwerde bildet die Rüge, dass die Vorratsspeicherung „unverhältnismäßig in die Berufsfreiheit der Angehörigen von Vertrauensberufen" eingreife (und in der Tat kann die Registrierung von Kontakten zu Rechtsanwälten, Steuerberatern, Seelsorgern, sozialen und psychologischen Beratern und Investigativ-Journalisten besonders heikel sein).

Das Gericht hat sich auf die Vermutungen und Befürchtungen der Beschwerdeführer weitgehend eingelassen. Der Kern des Urteils ist eine Aussage, die neue Methode der Datensammlung verursache bei den Bürgern einen Einschüchterungseffekt, ein „diffus bedrohliches Gefühl des Beobachtetseins", also die Angst vor einer unheimlichen, nicht abzuwehrenden Macht, die ihnen etwas Verbotenes oder Unerwünschtes vorhalten und ihnen deswegen ein Übel antun will. Dieses Gefühl könne „eine unbefangene Wahrnehmung der Grundrechte in vielen Bereichen beeinträchtigen".[138] Das ist keine empirisch begründete Feststellung, sondern eine Vermutung der Richter, und sie soll als Begründung dafür dienen, dass die Speicherung nur unter strengen Voraussetzungen erlaubt sein darf. Genau genommen, ist schon dies ein Fehlschluss; denn es ist doch fraglich, ob die diffusen Ängste verschwänden, wenn der Gesetzgeber eine strengere Regelung beschlösse – was er ja nach dem Urteil darf und was überdies von der EU-Kommission angemahnt wird. Mag das künftige Gesetz auch noch so „anspruchsvolle" Voraussetzungen für die Nutzung der gesammelten Daten aufstellen und mag es noch so „normenklar" formuliert sein – der Eindruck, dass das Telekommunikationsverhalten des ganzen Volkes registriert werde, wird bleiben, und demgemäß werden auch die Proteste anhalten. Nicht zufällig fordern die Kritiker die Aufhebung der EU-Richtlinie, auf die sich die Bundesregierung beruft, und weisen darauf hin, dass auch in anderen EU-Mitgliedstaaten verfassungsrechtliche Bedenken gegen die Richtlinie

137 Ebd. S. 282 f.

138 Ebd. S. 320. An anderer Stelle des Urteils (S. 332) wird hervorgehoben, die Befugnisse der geheimen Nachrichtendienste, die TK-Daten zu verwenden, beförderten „das Gefühl des unkontrollierbaren Beobachtetwerdens in besonderer Weise" und entfalteten „nachhaltige Einschüchterungseffekte auf die Freiheitswahrnehmung".

erhoben worden sind (und einige Verfassungsgerichte diesen Bedenken gefolgt sind).

Kritik des Vorratsdaten-Urteils

Das Karlsruher Urteil wird von allen Bürgerrechtlern und ihren Verbündeten aufs höchste gelobt – und ist doch in einem zentralen Punkt höchst anfechtbar.[139] Es erklärt nämlich nicht, die Ängste der Bürger seien unbegründet. Da man somit annehmen muss, dass das Gericht diese Ängste teilt, hätte man Ausführungen darüber erwarten dürfen, wie es denn geschehen könne, dass die Daten missbraucht werden, und dass ein hohes Maß an *Wahrscheinlichkeit* dafür spreche. Mit großer Sorgfalt wird stattdessen ausgemalt, welche „Rückschlüsse" „bis in die Intimsphäre hinein" sich „bei umfassender und automatisierter Auswertung" aus den TK-Verkehrsdaten ziehen lassen. Das Misstrauen wird besonders auf die vielen privaten Anbieter gelenkt, die zur Speicherung der Daten verpflichtet sein sollten.[140] Die „Vorkehrungen", die das Gericht zur Abwehr der Risiken fordert, richten sich aber auch gegen die Behörden, die im Falle des Datenabrufs mit der Auswertung befasst sind. Ihnen wird mehr oder weniger deutlich unterstellt, dass sie regelmäßig ihre Befugnisse extrem weit auslegen, wenn nicht überziehen wollen. Weil der Schutz der Individualinteressen in verschiedenen Aspekten zu schwach ausgestaltet sei, verstoße das Gesetz gegen das Prinzip der *Verhältnismäßigkeit*. Dass dieses Prinzip auch bei der *Anwendung* des Gesetzes zu beachten ist und im Allgemeinen beachtet wird, sagen die Richter nicht. Sie vertrauen auf die Klarstellung durch den Gesetzgeber und misstrauen den Beamten.

Die schärfste Kritik an diesem Urteil ist aus dem entscheidenden Senat selbst gekommen. Die Richter *Wilhelm Schluckebier* und *Michael Eichberger* haben Abweichende Meinungen zu Protokoll gegeben, in denen sie die Vorratsdatenspeicherung für verfassungskonform erklären.[141] Der Richter Schluckebier schreibt, wenn das angemessene Niveau der *Datensicherheit* gewährleistet sei, fehle „jede objektivierbare Grundlage für die Annahme eines eingriffsintensivierenden Einschüchterungseffekts".[142] Die Regelungen seien hinreichend angemessen und zumutbar. „Der Bürger muss sich im Rechtsstaat auf effektiven Schutz *durch* den Staat ebenso verlassen können wie auf den Schutz *gegen* den Staat".[143]

Der Richter Eichberger hat noch einen speziellen Einwand gegen die Mehrheitsentscheidung formuliert, der auch für die öffentliche Diskussion des Themas

139 Nachweise von Zustimmung und Kritik in der Lit. bei Bull 2011 a, S. 96 Fn. 220.
140 Ebd. S. 319 f.
141 Ebd. S. 364 ff. und S. 380 ff.
142 Ebd. S. 366.
143 Ebd. S. 369.

wichtig wäre: Die Senatsmehrheit ist davon ausgegangen, dass die Behörden beim Abruf der Daten stets ein umfassendes Bewegungs- und Persönlichkeitsprofil anstreben; tatsächlich aber untersuchen sie vielfach nur „einzelne Ereignisse, kurze Zeiträume und die Telekommunikationsbeziehungen nur einer oder weniger Personen (etwa die Telekommunikationsverbindungen einer Person an einem Tag oder auch nur in einer bestimmten Stunde)"; diese Abrufe haben „ein nur geringes Eingriffsgewicht" und sind schon gar nicht mit dem Zugriff auf *Inhalte* der Kommunikation vergleichbar.[144]

Je öfter ich mich in dieses Urteil und sein mediales Umfeld vertiefe und die Argumente überdenke, desto klarer wird mir, dass die Opposition gegen die Vorratsdatenspeicherung im Kern keine verfassungsrechtliche, sondern eine sozialpsychologische und politische Aktion ist. Die Bedenken, die aus dem Grundgesetz hergeleitet werden, sind ausräumbar, die in den Köpfen herrschenden Vorstellungen nicht – oder nur unter sehr günstigen Voraussetzungen. Es ist wie seinerzeit bei der Volkszählung, als die Boykottbewegung alle rechtlichen und empirisch-praktischen Argumente vom Tisch fegte: Die Volkszählungsgegner und -verweigerer wollten „der Politik" und „dem Staat" eine Lektion erteilen, und die bevorstehende Volkszählung bildete einen passenden Gegenstand. Dass die Informationen, die bei dem Zensus erhoben werden sollten, und die im Gesetz zugelassene Nutzung nicht den „Überwachungsstaat" herbeiführen würden, war vermutlich vielen Opponenten durchaus klar, aber sie fanden in dem Boykott einen Aufhänger, ihr tiefes Unbehagen über frühere Praktiken der Behörden (wie den – damals längst aufgehobenen – Radikalenerlass) und eine allgemeine Unzufriedenheit mit der Politik auszudrücken.

Die Vorstellung, dass alle unsere TK-Verkehrsdaten für ein halbes Jahr aufbewahrt und ausgewertet werden können, beunruhigt nicht nur die Mitmenschen, die etwas Verbotenes oder gar Strafbares tun wollen, sondern auch viele gesetzestreue Bürger, weil sie glauben, nicht mehr unbefangen telefonieren, faxen und mailen zu können. Dass daraus tatsächlich Ängste entstehen – und zwar gerade auch bei den „braven" Mitbürgern –, ist wahrscheinlich. An die hohen rechtlichen Hürden, die der Verwertung der gespeicherten Daten entgegenstehen, denken viele nicht, und wenn sie daran denken, sind sie sich nicht sicher, ob die Vorschriften wirklich eingehalten werden.

So spitzt sich das Problem auf die *Vertrauensfrage* zu, und es ist offensichtlich, dass Teile des Volkes und speziell große Teile der meinungsbildenden Schicht den Behörden eben nicht vertrauen. Ohne ein Mindestmaß an Vertrauen ist aber kein Staat aufrecht zu erhalten.

144 Ebd. S. 383.

Die Politik kann nicht warten, bis alle Ängste abgebaut sind. Sie muss entscheiden, ob Instrumente wie die Speicherung der TK-Verbindungsdaten wieder zulässig sein sollen oder nicht. Die Innenpolitiker, die überwiegend dazu neigen, die Arbeit der Polizeibehörden (und in engeren Grenzen auch die der Nachrichtendienste) zu erleichtern, liegen darüber im Streit mit Rechtspolitikern (der eigenen oder einer anderen Partei). Die Bundesministerin der Justiz beharrt darauf, dass allenfalls bei konkretem Anlass (wegen eines bestimmten Tatverdachts) ein „Einfrieren" der dann gerade vorhandenen Verbindungsdaten zugelassen sein sollte. Dieses Verfahren des „quick freezing" kann aber die längerfristige Vorratsdatenspeicherung nicht ersetzen; es schafft, wie auch das Bundesverfassungsgericht bestätigt hat, keine „vergleichbar effektive Aufklärungsmöglichkeit".[145] Kompromisse sind bei der Speicherungsdauer und der Eingrenzung der Zugriffsbefugnisse möglich, und hier spielt die EU-Richtlinie eine Rolle, die eine Mindestspeicherung von sechs Monaten vorschreibt.

Ein neues Szenario: Die Überwachungsmaschine

Die Entwicklung geht natürlich weiter, und so berichtet die Presse, dass derzeit – mit Unterstützung der EU – ein umfassendes Kontrollsystem entwickelt werde, dessen Überwachungskapazität alles bisher Dagewesene überschreite: „Die Überwachungsmaschine" schlechthin.[146] Unter dem Titel „Intelligentes Informationssystem zur Überwachung, Suche und Detektion für die Sicherheit der Bürger in urbaner Umgebung" (englische Abkürzung: „Indect") sollten „verschiedene Überwachungsmittel wie Kameras, Drohnen, Gesichtserkennung und Bildanalyse" zusammengeschaltet werden, ebenso wie „Webseiten, Diskussionsforen, Usenet-Gruppen, Dateiserver, Netzwerke und individuelle Computersysteme". Das Ziel sei, auf diese Weise „abnormes Verhalten" frühzeitig zu erkennen.

Ein Mitglied der Piratenpartei nennt Indect nach dem Zeitungsbericht eine „Gedankenpolizei". Über die entsprechend von Orwell erdachte Behörde hinaus brauche diese künftige Gedankenpolizei aber niemanden mehr, der auf den Bildschirm starrt; „die Maschine kann alle Bürger zu jedem Zeitpunkt erfassen". Eine schaurige Vorstellung: Der „allwissende künstliche Polizist" hat technische Augen und Ohren, kann sich Gesichter einprägen und wiedererkennen und aus dem Internet Zusammenhänge und Beziehungen zwischen weit entfernt voneinander existierenden Menschen und Organisationen aufdecken – alles mit der Intention, „abnormales Verhalten" aufzudecken und daraus polizeiliche oder justizielle Maßnahmen abzuleiten.

145 Ebd. S. 318.
146 Behrens 2011.

Diese Geschichte von der Überwachungsmaschine ist ein aktuelles Beispiel einer altbekannten negativen Utopie. Sie ist die Vorstellung einer technischen Erfindung und gleichzeitig ihre publizistische Verwandlung in eine angebliche soziale Möglichkeit, die dann eine Bedrohung für potentiell alle Menschen darstellt, die auf der Welt leben. Keine Frage: Wenn eines Tages Maschinen in Gebrauch kämen, die aus bestimmten Äußerungen, Bewegungen oder Geräuschen auf „abweichendes" Verhalten schließen und damit automatisch die gezielte Überwachung von Personen auslösen oder sogar zu physischen Freiheitsbeschränkungen führen, wäre das nicht hinnehmbar. Es wäre eine verfassungswidrige Einengung des normalen menschlichen Verhaltens, auf diese Weise Verdachtsmomente zu konstruieren, und wenn dies noch mit Hilfe von Gesichtserkennung perfektioniert würde oder zusätzliche Informationen aus dem Netz hinzugefügt würden, wäre das wirklich ein Horrorszenario. Entscheidungen dürfen überhaupt nicht allein aufgrund automatisierter Datenverarbeitung getroffen werden;[147] es muss immer ein menschlicher Entscheidungsakt hinzukommen.

Angenommen, ein derart superperfektes System werde gleichwohl hergestellt – dann hinge es von dem konkreten Zustand des Rechtsstaates, vom Rechtsbewusstsein des Volkes und der Medien und von der Rechtstreue der Regierungen und Verwaltungen ab, ob ein solches System zur Entdeckung und Bekämpfung von Alltagsstraftaten oder gar zur allgemeinen „Gesinnungspolizei" eingeführt würde. Polizei und Nachrichtendienste sind zwar an der Forschung auf diesem Gebiet interessiert, und man kann nicht ausschließen, dass sie zur Bekämpfung schwerer Straftaten und zur Abwehr schwerer Gefahren für die öffentliche Sicherheit auch extreme Mittel anwenden möchten. Aber der Gesetzgeber wird auf die rechtliche Eingrenzung solcher Systeme achten, und die Öffentlichkeit wird ihn daran erinnern. Die hohe Summe staatlicher und privater Mittel, die in die Förderung solcher Projekte fließen, lässt erahnen, dass es auch außerhalb des staatlichen Sicherheitsapparates viele Interessenten geben wird, die sich Vorteile von der technisch intensivierten Überwachung versprechen. Sicherheitstechnik ist ein explodierender Markt, der seinerseits überwacht werden muss.

Der Computer als Privatsphäre

Sehr tief geht der Eingriff der Staatsgewalt auch dann, wenn Polizei oder Verfassungsschutz über das Netz heimlich gezielt in privat genutzte Computer eindringen und Speicherinhalte „absaugen", um Verbrechen aufzuklären oder ihnen vorzubeugen. Eben das ist seit einiger Zeit möglich und unter engen Voraussetzungen

147 Vgl. § 6 a Bundesdatenschutzgesetz, der seine Entsprechung z.B. im französischen Datenschutzgesetz von 1978 hat.

gesetzlich erlaubt. So senden inzwischen die dazu ermächtigten Behörden Viren, Würmer oder „Trojaner" auf die PCs von Verdächtigen und „durchsuchen" sie mittels dieser Eindringlinge. Damit wird die seit längerem praktizierte Telekommunikationsüberwachung (Abhören von Telefonen, Mitlesen von Faxschreiben oder E-Mails) ergänzt; denn die Inhalte können auf diese Weise gelesen werden, bevor sie für den Transport verschlüsselt werden.

Das Bundesverfassungsgericht ist auch zu dieser Frage angerufen worden und hat festgestellt, dass eine solche „heimliche Infiltration eines informationstechnischen Systems" zulässig ist, „wenn tatsächliche Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Rechtsgut bestehen".[148] Das Gericht hat noch eine ganze Reihe von Vorbehalten formuliert, insbesondere dass nur ein Richter die „Online-Durchsuchung" anordnen darf und dass der „Kernbereich privater Lebensgestaltung zu schützen" ist. Es hat das Ganze unter die Überschrift gestellt, dass es ein „Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme" gebe.[149] Die Öffentlichkeit hat mit viel Zustimmung zur Kenntnis genommen, dass hier aus dem allgemeinen Persönlichkeitsrecht ein vermeintlich neues Grundrecht herausgelesen worden ist, und hat es begrüßt, dass die gesetzliche Vorschrift, auf die sich die Praxis gestützt hatte,[150] für verfassungswidrig erklärt wurde. Aber der Streit geht weiter, weil auch andere Rechtsnormen diese Maßnahme erlauben;[151] das Verfassungsgericht wird sich mit dieser Frage noch einmal befassen müssen.

Erstaunlich ist, dass Medien und liberale Öffentlichkeit diese Entscheidung des obersten Gerichts fast kritiklos hingenommen haben. Immerhin wird darin zugelassen, dass ein Computer schon dann heimlich infiltriert wird, „wenn sich noch nicht mit hinreichender Wahrscheinlichkeit feststellen lässt, dass die Gefahr in näherer Zukunft eintritt, sofern bestimmte Tatsachen auf eine im Einzelfall durch bestimmte Personen drohende Gefahr für das überragend wichtige Rechtsgut hinweisen". Auf die Voraussetzung, dass eine „konkrete Gefahr" bestehen muss, wird hier also – aus guten Gründen – verzichtet, sondern es soll die „Gefahrengefahr" genügen. Anders als bei Rasterfahndungen und der umstrittenen Vorratsdatenspeicherung dringt der Staat hier gezielt in einen Bereich ein, den jeder für sich behalten und nicht fremden Blicken öffnen will.

Muss nicht der eigene PC, der alle privaten Notizen und Kommunikationsinhalte enthält, ebenso gegen Durchsuchungen geschützt werden wie der räumliche Rückzugsbereich, die Wohnung? Wenn man dieser Überlegung folgt, ist die Heimlich-

148 BVerfGE 120, 274.
149 Nachweise zu Erläuterungen und Kritik in der Lit.: Bull 2011 a, S. 35 Fn. 86.
150 Es handelte sich um das Verfassungsschutzgesetz Nordrhein-Westfalen (dort § 5 Abs. 2 Nr. 11).
151 So das Gesetz über das Bundeskriminalamt (§ 20 k). Es ist insofern ebenfalls verfassungsrechtlich umstritten.

keit der Durchsuchung nicht hinnehmbar und letztlich in jedem Fall verfassungswidrig. Wir verlangen auch in manchen anderen Konstellationen, dass der Staat auf „an sich" verfügbare Informationen verzichtet, etwa wenn Angehörigen eines Verdächtigen oder bestimmten Berufen ein Zeugnisverweigerungsrecht zugebilligt wird.

Kriminalität und Missbrauch im Internet

Während die Datenschutz-Szene ausgiebig über die Möglichkeiten der Unterdrückung durch den Staat diskutiert, geschehen in der Praxis der Internetnutzung unglaubliche Dinge. Das Netz wird ständig dazu benutzt, anderen Schaden zuzufügen. Es beginnt beim Mobbing und Stalking über E-Mails und soziale Netzwerke, bei Beschimpfungen und Verleumdungen übelster Art und geht bis zu millionenfachem Betrug und zu anonymen Morddrohungen „aus dem Nichts". Täglich können wir Berichte darüber in den Zeitungen lesen; die Polizei veröffentlicht von Zeit zu Zeit zusammenfassende Berichte mit erschreckenden Zahlen. „Cyberbullying" und „Cyberharassment" verursachen Tragödien: Eine ganze Reihe von Schülerinnen und Schülern, die im Netz gemobbt wurden, haben sich das Leben genommen.[152] Offensichtlich äußern manche Menschen unter dem Schutz der Anonymität im Netz Dinge, die sie von Angesicht zu Angesicht nicht sagen würden, und es ist außerordentlich schwer, ihnen das zu verwehren. Manche sind allerdings frech genug, sich für „Hassreden" auf die Meinungsfreiheit zu berufen; „free speech" ist zumindest in der amerikanischen Diskussion über verletzende Äußerungen ein vielbenutzter Rechtfertigungstopos.

Auch der materielle Schaden durch Internetstraftaten ist vermutlich riesig. Es ist vorgekommen, dass prosperierende Unternehmen durch ungetreue Mitarbeiter oder Eindringlinge von außen, die das Computersystem oder den E-Mail-Zugang manipulierten, in den Konkurs getrieben wurden. Einige Hacker halten sich viel darauf zugute, dass sie fremde Systeme stören oder gar zerstören können. Ganze Industriebetriebe wurden durch eingeschleuste Viren, Trojaner oder wie immer die Schadprogramme heißen, lahmgelegt – und vieles mehr.

Dass Computerkriminalität der verschiedenen Arten bekämpft und bestraft werden sollte, ist eigentlich nicht umstritten, aber die Täter profitieren davon, dass Teile der Netzgemeinde jegliche staatliche Kontrolle im Netz ablehnen – sie denken nur an ihre eigene (gesetzeskonforme) Nutzung der Online-Welt und fürchten, die Behörden würden ihre Überwachungsbefugnisse auch gegen die „braven" Netzfreaks richten. In der Tat werden natürlich bei Durchsuchungen immer auch Un-

152 Vgl. etwa Plotkin 2012, S. 2 ff.

schuldige überprüft (da man die Schuldigen noch nicht kennt, ist dies selbstverständlich!) – aber auch dies ist in der realen Welt nicht anders, und wenn gewisse Grenzen eingehalten werden, muss jeder dies ertragen.

Zu diesen Grenzen gehört vor allem die Unschuldsvermutung, und besonders besorgte Netznutzer meinen, wenn die Polizei zu ermitteln anfange, halte sie jeden und jede für verdächtig. Die These von dem „Generalverdacht", der z.B. allen Rasterfahndungen zugrunde liege, ist irgendwann einmal als Argument gegen solche Massenaktionen der Sicherheitsbehörden aufgestellt worden; sie war nie wirklich begründet, aber sie hält sich hartnäckig. Wie aber soll denn eine Behörde auf die Täter kommen, wenn sie nicht stufenweise die möglichen Verdächtigen feststellen und den Kreis der potentiell Verantwortlichen immer weiter einengen darf? Es muss nur sichergestellt sein – und das ist regelmäßig der Fall, jedenfalls in Deutschland –, dass die Daten über die große Zahl der danach nicht Verdächtigen wieder gelöscht werden.