Annex
Datenschutz im 21. Jahrhundert

Die vernetzte Informationsgesellschaft eröffnet **Chancen**, die noch vor zwei Jahrzehnten unvorstellbar waren: Das Internet gibt Menschen in aller Welt die Gelegenheit, sich frei und unzensiert zu informieren. Die Ereignisse im arabischen Raum haben vor einigen Jahren deutlich gemacht, dass es Regierungen nicht mehr möglich ist, ihre Bürger von Informationen abzuschotten. Die Occupy-Bewegung und die Entwicklung der „Piraten“ sind hierzulande Beispiele dafür, dass das Internet die Ausübung von Freiheitsrechten fördern kann und neue Organisationsformen ermöglicht[1]. Auch für die wirtschaftliche Entwicklung bietet das Netz neuen Freiraum: Indem Kunden in aller Welt direkt angesprochen werden, verkürzt sich der Weg neuer Unternehmen zum Markt. Das rasante Wachstum von Unternehmen wie Google, Ebay, Amazon und Facebook liefert hierfür faszinierendes Anschauungsmaterial. 1

1 Vgl. Härting/Schneider, ZRP 2011, 233 ff.; Schneider/Härting, Leitlinien des Datenschutzes, www.schneider-haerting.de/2011/09/leitlinien-des-datenschutzes; Deutscher Anwaltverein, Stellungnahme zu dem Gesamtkonzept des datenschutzes in der Europäischen Union, Stellungnahme 4/2011, www.anwaltverein.de/downloads/Stellungnahmen-11/SN4-2011.pdf; Stellungnahme der DGRI zur DS-GVO vom 21.12.2011, www.dgri.de/index.php/fuseaction/download/lrn_file/stellungnahme-dgri-datenschutzvo.pdf.

2 Der **Schutz der freien Kommunikation** geht sehr weit. Auch dilettantischer Journalismus, selbstdarstellerische Blogs und saftige Klatschgeschichten sind durch Art. 5 GG, Art. 10 EMRK und Art. 11 EU-GRCh geschützt. Der freie Informationsaustausch steht auch dann unter Grundrechtsschutz, wenn er über das Internet erfolgt und wenn dabei Plattformen amerikanischer Anbieters wie Facebook, Google, Twitter oder Apple genutzt werden. Dass diese Plattformen nicht aus idealistischen Gründen, sondern aus **„Gewinnstreben"** betrieben werden, kann man den Betreibern nicht zum Vorwurf machen. Eine Meinungsäußerung ist auch dann durch Art. 5 GG, Art. 10 EMRK und Art. 11 EU-GRCh geschützt, wenn sie über ein kommerzielles Medium erfolgt[1]. Und ein gewisser kommerzieller Erfolg schafft vielfach überhaupt erst die notwendigen Grundlagen für eine freie Kommunikation[2].

3 In der Abwägung zwischen Privatheit und Öffentlichkeit von Informationen gibt es keine „natürliche" Default-Einstellung. Wer Informationen über sich preisgibt, liefert sich damit nicht dunklen Mächten jenseits jeder Kontrolle aus[3]. Die Preisgabe ist ein unverzichtbarer Bestandteil jeder Kommunikation. Und wer mit **Alarmismus** den Informationsaustausch beobachtet, hält Kommunikation für per se gefährlich, ohne dass sich ein rationaler Grund für ein solches Misstrauen nennen ließe.

4 Seltene Krankheiten oder erotische Vorlieben, Probleme mit einem Arbeitgeber oder mit einem Unternehmen, dessen Kunde man ist: Das Netz bietet **unendliche Möglichkeiten** des Austauschs mit Gleichgesinnten. Wer einmal mit einer Selbsthilfegruppe von Kranken gesprochen hat, die sich online gefunden haben, gewinnt eine Ahnung von dem **Solidarisierungspotential**[4], das dem Netz zueigen ist.

5 Tim Berners-Lee, der als Vater des World Wide Web gilt, hat auf die **Chancen** aufmerksam gemacht, die die vernetzte Datenflut eröffnet. Die Datenbestände, die bei Google und Facebook gespeichert sind, eignen sich nicht nur zum sinistren Missbrauch. Sie stellen einen Fundus dar, der eine Auswertung in vielfacher Hinsicht ermöglicht[5]:

> „Mein Computer weiß viel über meine körperliche Fitness, meine Essgewohnheiten und die Orte, an denen ich mich aufhalte. Mein Telefon versteht von allein, wie viel Sport ich getrieben habe, wie viele Treppen ich gelaufen bin und so fort."

---

1 EGMR vom 10.1.2013 – 36769/08, Rz. 34.
2 Vgl. EuGH vom 16.12.2008 – C-524/06, CR 2009, 229.
3 Heller, Post-Privacy, S. 106.
4 Vgl. Heller, Post-Privacy, S. 134 mit überschießendem Pathos: „Um einander zu finden, muss man einander erkennbar werden".
5 Berners-Lee: demand your data from Google and Facebook, The Guardian, 18.4.2012, www.guardian.co.uk/technology/2012/apr/18/tim-berners-lee-google-facebook.

Die Kommunikation vieler mit vielen auf unterschiedlichen Wegen und Kanälen, über alle Grenzen, von stationären und mobilen Endgeräten bildet den Kern und das Herzstück der Funktionen, die das Internet in erfüllt. Dabei darf man nicht übersehen, dass sich die **digitale Informationsgesellschaft** noch am Anfang ihrer Entwicklung befindet. Die Parallele zur Erfindung des Buchdrucks durch Johannes Gutenberg (ca. 1455) ist nicht übertrieben: Im Jahre 2013 befinden wir uns noch nicht einmal im Jahr 20 nach dem Beginn der Massenkommunikation über das Internet. Dies entspricht in Buchdruck-Jahren ungefähr dem Jahr 1475[1]. 6

I. Kein Eigentum an Daten

Häufig kommt es zu Kollisionen zwischen der freien Kommunikation und Persönlichkeitsrechten[2]. Diese Konfliktlagen sind keineswegs neu, werden jedoch verschärft und verzerrt durch eine eindimensionale Wahrnehmung, die viele Diskussionen um den Datenschutz im Netz prägt und die sich in einem weit verbreiteten Satz zuspitzt: „**Meine Daten gehören mir**“[3]. 7

Der Satz ist ebenso populär wie **verkehrt**. Schon in seinem Volkszählungsurteil hat das BVerfG[4] betont, dass es kein absolutes Herrschaftsrecht des Einzelnen über „seine“ Daten gibt. Jegliche Anleihen an eigentumsähnliche Befugnisse (**„meine Daten“**) gehen fehl. Der Einzelne ist eine sich innerhalb der sozialen Gemeinschaft entfaltende, auf Kommunikation angewiesene Persönlichkeit. Informationen, auch soweit sie personenbezogen sind, stellen ein „**Abbild sozialer Realität**“ dar, das nicht ausschließlich dem Betroffenen allein zugeordnet werden kann[5]. 8

Telefonnummern und andere Kontaktdaten sind ein gutes Beispiel für die „soziale Realität“, die das BVerfG meint. **Kontaktdaten** dienen der Kommunikation und werden daher ganz selbstverständlich von jedem gespeichert, der mit der betreffenden Person kommunizieren möchte. Wenn es allein der Entscheidung des „Inhabers“ einer Telefonnummer oder einer Adresse überlassen wäre, wer wann und wie lange die Kontaktdaten speichern darf, würde dies die soziale Interaktion gravierend beeinträchtigen. Kontaktdaten „gehören“ weder dem „Inhaber“ der Daten noch einer Person, die diese Daten auf einem Endgerät gespeichert hat: 9

„Informationen sind das Fluidum unseres Zusammenlebens: Sie sind nicht nur wertvolle Ware in Auskunfteien, nicht nur Gegenstand aller Medien und der Wis-

1 Vgl. Noughton, From Gutenberg to Zuckerberg, London 2012, S. 11.
2 Härting, AnwBl 2011, 246, 248 ff.
3 Künast, ZRP 2008, 201 ff.
4 BVerfG, 15.12.1983 – 1 BvR 209/83 u.a., BVerfGE 65, 1, 41 f. – Volkszählung.
5 BVerfG, 15.12.1983 – 1 BvR 209/83 u.a., BVerfGE 65, 1, 41 f. – Volkszählung.

senschaft. Alle Dienstleistungen werden von den ausgetauschten Informationen meist ganz persönlicher Art geprägt; jeder Vertrag, jeder Güteraustausch wird von Informationen mehr oder weniger bedeutsam begleitet. Alle Informationen über die Ware, ihren Schöpfer und seine Marktstellung, über seine Vertrauenswürdigkeit, seinen Charakter und seine Bonität sind, möglichst detailliert, von Belang."[1]

10 Die Datenbestände, die bei der Auswertung des Verhaltens eines Internetnutzers anfallen, stellen einen erheblichen wirtschaftlichen Wert dar. Sie werden mit einigem Recht als „**digitales Gold**" bezeichnet und sind die Basis der Geschäftsmodelle vieler Internetanbieter. Dennoch ist die (verbreitete) Vorstellung verfehlt, dass „die Daten" den Nutzern gehören und den Online-Anbietern als „Entgelt" für deren Dienstleistungen überlassen werden:

„Personenbezogenen Informationen sollten weder als alleiniges Gut des Nutzers angesehen werden … noch ausschließlich als Eigentum des datenverarbeitenden Unternehmens … Stattdessen sollten personenbezogene Informationen als wertvolle gemeinsame Ressource behandelt werden und als Basis für Wertschöpfung und Innovation."[2]

11 Solange Daten über besuchte Internetseiten nur dem jeweiligen Nutzer zur Verfügung stehen, haben sie keinen messbaren Wert. Zu einem **Wirtschaftsgut** werden die Daten erst durch ihre Anhäufung, Zusammenführung und Auswertung beim Online-Dienst.

12 Ebenso wenig lässt sich von einem **„Kontrollrecht"** des Nutzers ausgehen. Niemand hat ein (quasi-natürliches) Kontrollrecht über Informationen, die die eigene Person betreffen. Würde man dies anders sehen, läge in jedem zwischenmenschlichen Kontakt ein Eingriff in die Privatsphäre. Was andere über mich wahrnehmen, entzieht sich im zwischenmenschlichen Umgang jeder Kontrolle, zumal die Wahrnehmungen Informationen sind, die sich zwar auf meine Person beziehen, deren Entzug jedoch einen Informationsverlust bedeutet, der sich nicht legitimieren lässt. Ebenso wenig wie es Eigentum an Informationen geben kann, lassen sich Kontrollrechte begründen und abgrenzen:

„Anders als körperliche Gegenstände können Informationen gleichzeitig den Köpfen von Millionen Menschen gleichzeitig gehören … Die Komplexität personenbezogener Informationen liegt darin, dass sie sowohl Ausdruck des Individuums sind als auch Tatsachen – die historische Aufzeichnung des individuellen Verhaltens."[3]

---

1 Giesen, Brüssels Griff nach dem Datenschutz ist demokratiewidrig, Süddeutsche Zeitung v. 18.5.2012, http://www.sueddeutsche.de/digital/digitale-buerger rechte-bruessels-griff-nach-dem-datenschutz-ist-demokratiewidrig-1.1360023.

2 Tene/Polonetsky, Big Data for All: Privacy and User Control in the Age of Analytics, 11 Nw. J. Tech. & Intell. Prop. 239 (2013), 269, http://scholarlycommons.law.northwestern.edu/njtip/vol11/iss5/1.

3 Solove, Understanding Privacy, Cambridge/London 2009, S. 27.

II. Kein Schutz von Daten

Daten an sich sind belanglos, langweilig und ignorant. Sie bestehen aus Einsen und Nullen[1] und sind – für sich betrachtet – weder nützlich noch riskant. Daher bedürfen Daten per se weder eines besonderen Schutzes, noch müssen Individuen oder die Gesellschaft gegen Daten geschützt werden. Datenschutz kann daher **nie Selbstzweck** sein. 13

Von einem Datum als solchem geht keine Gefahr aus. Erst wenn die Daten – allein oder i.V.m. anderen Daten bzw. Informationen – Rückschlüsse darauf zulassen, dass ein bestimmter Internetnutzer sich auf Internetseiten mit pikantem Inhalt bewegt hat, ist die Privatsphäre des Nutzers berührt. Die Daten erlangen einen **Informationswert**, der die Persönlichkeitsrechte beeinträchtigen kann[2]. 14

Da es nicht um den Schutz eigentumsähnlicher Rechte geht, geht es auch nicht um den Schutz ***von*** Daten, sondern um den Schutz ***vor*** Daten. Daten sind nicht mehr und nicht weniger als Mittel zum Zweck. Es geht um den Schutz der Bürger- und Persönlichkeitsrechte vor unerwünschten Folgen von Informationen, die Staat und Wirtschaft sammeln. 15

Datenschutz heißt **Schutz gegen Menschen**, nicht jedoch Schutz gegen Rechner. Hierauf hat das BVerfG in seiner Entscheidung zum Abgleich von Kreditkartendaten zu Recht hingewiesen, als es einen Grundrechtseingriff verneinte, solange der (millionenfache) Eingriff computergesteuert und ohne positives Ergebnis verlief. Ein Grundrechtseingriff sei nur in den wenigen „Verdachtsfällen“ zu bejahen, in denen der Abgleich positiv endete mit der Folge, dass die Ermittler Kenntnis von den Daten der einzelnen Kreditkartenabrechnungen erhielten. Die Bedrohung von Grundrechten geht nach der Sichtweise des BVerfG nicht von der Technik aus, sondern von Menschen, die mittels Technik Kenntnis von Daten erhalten können[3]. 16

III. Kein „Recht auf Vergessen(werden)“

Unter den Bedingungen der digitalen Informationsgesellschaft ist jedes Datenschutzrecht zwangsläufig zugleich ein Akt der **Kommunikationsregulierung**. Populäre Forderungen wie das von der EU-Kommission propagierte „Recht auf Vergessenwerden“[4] werfen die Frage auf, inwieweit hierdurch übermäßig in die Kommunikationsfreiheit eingegriffen wird. 17

1 Heller, Post-Privacy, S. 48.
2 Schneider/Härting, ZD 2011, 63, 64; Schneider/Härting, ZRP 2011, 233.
3 Vgl. BVerfG vom 17.2.2009, NJW 2009, 1405, 1407 – Kreditkartendaten.
4 Vgl. Härting, BB 2012, 459, 464.

18 Das „Recht auf Vergessenwerden" steht im Zeichen der **Datensparsamkeit**, schont die Persönlichkeitsrechte der Betroffenen, hat jedoch zugleich ein **doppeltes Gesicht**. In ihrem Jahresbericht 2012 zu den „Feinden des Internet" bezeichnet die Organisation „Reporter ohne Grenzen"[1] das von der EU-Kommission vorgeschlagene „Recht auf Vergessenwerden" als Bedrohung der freien Netzkommunikation („threat … to online free speech").

19 Ein Beitrag aus „The European" zum „Right To Be Forgotten", beginnt lyrisch:

> „Es gab Zeiten, da gab es ein Recht auf Vergessen. Da hat man, als Schluss war, den Packen Liebesbriefe genommen, und dramatisch in Flammen aufgehen lassen – und dann ward nie wieder gelesen, was einst zwei Herzen schrieben."[2]

20 Und Viktor Mayer-Schönberger erinnerte im Jahre 2012 kurz vor Thanksgiving in der „Washington Post" ganz sentimental an gute alte Zeiten:

> „Wenn man sich am Thanksgiving-Tisch gegenübersaß und die Wärme der Familie sowie das Aroma der Kastanienfüllung genoss, hat man sich zumeist nicht an die boshafte Bemerkung erinnert, die Tante Jennifer über Dich vor einigen Jahren fallen ließ. Man hat der unfreundlichen Anspielung nicht nachgehangen, die Onkel Julio letztes Weihnachten über Deine Trinkgewohnheiten zum Besten gab, oder den Sprüchen von Cousin Duwan über Deine Freundin in den schrecklichen Ferien am Strand. Zu Familienfesten umarmen wir für gewöhnlich unsere Verwandten, auch wenn wir sie seit Monaten oder Jahren nicht gesehen haben, trotz aller Auseinandersetzungen, die wir mit ihnen in der Vergangenheit hatten."[3]

21 Das befreiende Gefühl beim Verbrennen alter Briefe, die milde Gnade beim Vergessen familiären Streits: All diese Segnungen der guten **vordigitalen Zeit** sollen in Gefahr sein, wenn über Facebook, Google, Twitter und Co. die Zeugnisse der Vergangenheit auf alle Ewigkeiten abrufbar bleiben. So oder ähnlich klingt die Begleitmusik, mit der die Einführung eines „Rechts auf Vergessen" gefordert wird. Und man ist leicht versucht, in diese Musik einzustimmen, wissen wir doch alle, wie heilsam es ist, wenn das menschliche Gedächtnis selektiert: Mach es wie die Sonnenuhr, zähl die schönen Stunden nur! Gar nicht auszudenken, wenn das „Vergessen" im digitalen Zeitalter in Gefahr wäre.

22 Die EU-Kommission spricht bezeichnenderweise im Passiv: Es geht ihr nicht um ein „Right To Forget", sondern um ein **„Right To Be Forgotten"**. Und dies aus gutem Grund. Ein „Right To Forget" wäre nachgerade unsinnig. In Zeiten, in denen ein Buch mit dem flotten Titel „Digitale

---

1 Reporters Without Border, Internet Enemies Report 2012 vom 12.3.2012, S. 6, http://en.rsf.org/IMG/pdf/rapport-internet2012_ang.pdf.

2 Ulrich, Gelöscht, niemals verloschen, The European v. 31.1.2012, http://www.theeuropean.de/wolf-christian-ulrich/9762-facebooks-umgang-mit-daten.

3 Mayer-Schönberger, Why we need to let our online memories go, Washington Post v. 23. November 2012, http://articles.washingtonpost.com/2012-11-23/opinions/35509224_1_memories-digital-age-human.

Demenz" zum vieldiskutierten Bestseller wird[1], kann man schwerlich, dass das „Vergessen" in Gefahr ist. In Gefahr sind allenfalls die Konversation und die Interaktion:

„Menschliche Beziehungen sind vielfältig; sie sind chaotisch und herausfordernd. Wir haben gelernt, Beziehungen mit Hilfe von Technologie aufzuräumen. Und der Übergang vom Gespräch zur Verbindung gehört dazu. Doch ist dies ein Vorgang, bei dem wir uns selbst betrügen. Schlimmer noch, allem Anschein nach hören wir mit der Zeit auf, uns dafür zu interessieren, wir vergessen den Unterschied."[2]

Bei der täglichen Informationsflut, der wir ausgesetzt sind, ist die Merk- 23
fähigkeit das Problem und nicht die Fähigkeit des Vergessens. Und natürlich können und wollen weder Mark Zuckerberg noch Larry Page Menschen das Verbrennen von Briefen oder das Verdrängen familiärer Konflikte verbieten. Der Facebook-Nutzer des 21. Jahrhunderts vergisst aller Wahrscheinlichkeit nach so viel und so selektiv, wie dies bei den „fernsehsüchtigen" Großstadtkindern der 70er Jahre des letzten Jahrhunderts der Fall war. Für ein gesetzliches **„Recht auf Vergessen"** würde es an jeglichem Sachverhalt fehlen, auf den sich ein solches Recht stützen ließe. Es ist daher konsequent, wenn kein „Recht auf Vergessen", sondern ein „Recht auf Vergessenwerden" gefordert wird.

Allerdings: Liebesbriefe, familiäres Thanksgiving – Die Parallelen zur 24
analogen Vergangenheit werden bei einem „Recht auf Vergessenwerden" mehr als absurd. Wenn mein Ex-Geliebter meine uralten, vor peinlich-ungelenken Liebesbekenntnissen triefenden Briefe in einer Schatztruhe verwahrt, war und ist dies sein gutes Recht. Als Verfasser der Liebesbriefe habe ich kein Recht, die Vernichtung der Briefe zu verlangen. Noch viel weniger habe ich das Recht, von dem Verflossenen „vergessen zu werden".

Und auch das Thanksgiving-Beispiel eignet sich nicht als Beleg für ein 25
natürliches Recht auf „Vergessenwerden". Nicht alle Familientreffen verlaufen so harmonisch, wie dies im Hause Mayer-Schönberger der Fall zu sein scheint. Und so geschieht es, dass der Vater den Sohn oder die Mutter die Tochter zu Weihnachten gerne an picklige Jugendliebschaften oder die Lieblings-Boy-Band der Teenagerzeit und die knallgrün gestrichenen Wände des Kinderzimmers erinnert. Sohn und Tochter fluchen heimlich und wünschen sich, diese alten Geschichten mögen doch endlich „vergessen werden". Die Einführung eines Rechts, von Familie, Nachbarn und Freunden das **„Vergessenwerden"** peinlicher Jugendsünden zu verlangen, hat bis dato noch niemand verlangt.

---

1 Vgl. Kempf, Analoge Ignoranz spielt mit den Ängsten der Menschen, FAZ online v. 3.10.2012, http://www.faz.net/aktuell/wirtschaft/digitale-demenz-analoge-ignoranz-spielt-mit-den-aengsten-der-menschen-11906366.html.

2 Turkle, The Flight From Conversation, New York Times vom 21.4.2012, http://www.nytimes.com/2012/04/22/opinion/sunday/the-flight-from-conversation.html?pagewanted=1&_r=3.

26 Bei einem „Recht auf Vergessenwerden" geht es nicht um Informationen in „meinem Gedächtnis", sondern um Informationen im Gedächtnis der Mitmenschen. Und an diesen Informationen habe ich keine Rechte. Das Selbstbestimmungsrecht des Einzelnen umfasst nicht das Recht, darüber zu bestimmen, wie man selbst **wahrgenommen** wird. Oder mit den Worten des BVerfG:

„Das Persönlichkeitsrecht verleiht seinem Träger keinen Anspruch darauf, nur so in der Öffentlichkeit dargestellt zu werden, wie es ihm genehm ist."[1]

27 Auch in einem Bericht, den die EU-Agentur ENISA im November 2012 veröffentlicht hat, wird ein „Recht auf Vergessenwerden" kritisch gewürdigt[2]. Die für die Netz- und Informationssicherheit zuständige Agentur gibt zu bedenken, dass das „Recht auf Vergessenwerden" bislang nur sehr vage definiert wird. So sei nicht ersichtlich, wer zur Ausübung eines „Rechts auf Vergessenwerden" berechtigt sein soll, wenn sich Informationen auf **mehrere Personen** beziehen (Beispiel: ein Foto mit mehreren Personen). Zudem sei der genaue Inhalt des Anspruchs unklar. Schließlich bleibe offen, ob das „Recht auf Vergessenwerden" ein Recht auf vollständige Beseitigung und Vernichtung von Daten bedeute oder ob es ausreiche, dass die jeweiligen Inhalte über Suchmaschinen oder auf ähnlich Weise nicht mehr auffindbar sind.

28 Wie problematisch ein „Recht auf Vergessenwerden" ist, demonstriert ENISA anhand von zwei Beispielen mit jeweils zwei Personen, deren Informationsinteressen betroffen sind:

„Man stelle sich einmal ein Foto vor, auf dem Alice und Bob zu sehen sind bei einer Aktivität an einem bestimmten Ort zu einer bestimmten Zeit. Wenn man einmal annimmt, Alice wolle das Foto vergessen, während Bob darauf besteht, dass es erhalten bleibt. Wessen Wünsche sollen den Ausschlag geben? Was geschieht, wenn eine Vielzahl von Personen auf einem Gruppenfoto zu sehen ist? Wer soll berechtigt sein zu entscheiden, ob und wann das Foto vergessen werden soll?

Weiteres Beispiel: Bob nimmt einen Tweet teilweise in einen längeren eigenen Blogbeitrag auf. Wenn Alice zu einem späteren Zeitpunkt ihr Recht auf Beseitigung des Tweets ausübt, was bedeutet dies für Bobs Blogbeitrag? Muss Bob den gesamten Beitrag löschen? Muss er den Tweet aus dem Beitrag entfernen und seinen Beitrag umschreiben? Welche Kriterien sollen für die Entscheidung gelten?"[3]

29 Die Beispiele belegen eindrucksvoll, dass sich Informationen nicht ohne Weiteres einer Person zuordnen lassen. Daten und Informationen sind

1 BVerfG, Beschl. v. 8.6.2010 – 1 BvR 1745/06.
2 Druschel/Backes/Tirtea, ENISA Report „The right to be forgotten – between expectations and practice", http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/the-right-to-be-forgotten/at_download/fullReport. Zu technischen Problemen siehe Kalabis/Selzer, DuD 2012, 670 ff.
3 Druschel/Backes/Tirtea, a.a.O., S. 7.

(auch) ein **„Abbild sozialer Realität"**[1]. Und es versteht sich von selbst, dass es keine Individualrechte an dieser „Realität" geben kann.

Zum „Abbild sozialer Realität" gehört auch das **„kollektive Gedächtnis"** – eine zivilisatorische Errungenschaft, der wir Archive, Museen und eine moderne Geschichtsschreibung verdanken. Was soll aus diesem Kulturgut werden, wenn Einzelpersonen darüber entscheiden dürften, welche Information „vergessen werden? 30

IV. „Big Data"

Schon seit langem geht es bei der Verarbeitung von Daten nicht mehr primär um Kausalität, sondern um **Korrelation**[2]. Je umfassender die Datenmenge ist („Big Data"), desto intelligenter wird die Korrelation[3]. Jede Vergrößerung von Datenmengen erhöht die Wahrscheinlichkeit von Erkenntnissen, die aus den Daten gewonnen werden können. Hierin liegt ein grundlegender Unterschied zum menschlichen Denken. Dem Gehirn droht bei großen Mengen an Informationen die Überforderung. Bei der Datenverarbeitung schaffen große Mengen an Informationen dagegen immer wieder **neue Möglichkeiten**, durch Verknüpfungen Erkenntnisse zu gewinnen[4]. Computernetze lassen sich unter den heutigen technischen Gegebenheiten nicht mehr überfordern. 31

Eines der zahlreichen Anwendungsgebiete von Big Data ist die Astronomie, die bereits seit vielen Jahren durch die Innovationskraft von „Big Data" revolutioniert wird. Teleskope werden immer leistungsfähiger und produzieren ein Datenvolumen, das sich jedes Jahr verdoppelt: 32

> „Man stelle sich einmal alle Daten vor, die die Menschen in der langen Geschichte der Astronomie gesammelt haben … Wenn wir diese Daten in Bit ausdrücken würden, der Maßeinheit unserer Tage, wäre die Zahl *astronomisch*. Damit aber nicht genug: Schon nächstes Jahr wird sich die Zahl verdoppelt haben, ein Jahr später wird sie sich erneut verdoppelt haben, und so weiter und so fort."[5]

„Big Data" macht es möglich, die ständig wachsende Menge von „Rohdaten" zu verarbeiten und zu analysieren. Maßgeblich sind dafür vor allem zwei Umstände: 33

– Da Speicherplatz in (nahezu) unbegrenztem Umfang vorhanden ist, setzt eine Datenanalyse nicht mehr eine Vorauswahl „repräsentativer"

1 BVerfG, Urt. 15.12.1983 – 1 BvR 209/83, 1 BvR 269/83, 1 BvR 362/83, 1 BvR 420/83, 1 BvR 440/83, 1 BvR 484/83, BVerfGE 65, 1 ff. zu C.II.1.b), Rz. 150.
2 Vgl. Mayer-Schönberger/Cukier, Big Data, New York 2013, S. 50 ff.
3 Heller, Post-Privacy, S. 64.
4 Vgl. Heller, Post-Privacy, S. 64 f.
5 Andersen, How Big Data is changing Astronomy (Again), The Atlantic v. 19.4.2012, http://www.theatlantic.com/technology/archive/2012/04/how-big-data-is-changing-astronomy-again/255917.

Daten voraus. Es können vielmehr alle Daten in die Analyse einbezogen werden[1].

– Die Analyse der Daten stützt sich auf Algorithmen, das heißt auf Rechenformeln, die ständig verfeinert werden[2].

34 **„The Big Data Explosion"**: Man schätzt, dass sich allein in den Jahren 2011 bis 2016 das Volumen der Internetdaten vervierfachen wird[3]. Wenn Bewegungsdaten zur Verkehrslenkung ausgewertet werden, Stromzählerdaten zwecks Optimierung der Energieversorgung und der Energiekosten analysiert und Gesundheitsdaten zur Verbesserung der Behandlung von Krankheiten und zur Senkung von Gesundheitskosten genutzt werden, dann geht es stets darum, rückwirkend, „in Echtzeit" und prognostisch eine Vielzahl von Informationen über eine Vielzahl von Personen zu analysieren. Big Data-Anwendungen sind in höchst unterschiedlichen Lebensbereichen zu finden: von den Finanzmärkten über Wissenschaft und Medizin bis zum Sport[4].

35 Die Auswertung von Big Data führen keineswegs automatisch und ausnahmslos zu **„richtigen" Ergebnissen**[5]:

– Die Erfassung eines **Sinnzusammenhangs** fällt Algorithmen naturgemäß schwer.

– Algorithmen haben keine **soziale Kompetenz**.

– Algorithmen ziehen im Zweifel dem **Meisterwerk** das durchschnittliche Werk vor.

– Je größer die Datenbestände sind, desto mehr werden auch **unnütze Daten** gesammelt mit „Störgeräuschen" („Noise"), die die Präzision der Auswertung erschweren.

– Je **komplexer** das Problem ist, desto weniger eignen sich Algorithmen für eine Lösung.

– Algorithmen sind stets von Menschen gemacht, deren Bewertungen somit in die Auswertung einfließen. **Komplexe Algorithmen** verschleiern diese Bewertungen und führen zu Ergebnissen, deren Grundannahmen **obskur** bleiben[6].

---

1 Vgl. Mayer-Schönberger/Cukier, Big Data, New York 2013, S. 32 ff.
2 Vgl. Mayer-Schönberger/Cukier, Big Data, New York 2013, S. 35 ff.
3 The Big Data Explosion (Infographic), Whatsthebigdata.com vom 4.2.2013, http://whatsthebigdata.com/2013/02/04/the-big-data-explosion-infographic.
4 Vgl. Naughton, Big data, revolution by numbers, Observer v. 18.11.2012, http://www.guardian.co.uk/technology/2012/nov/18/data-analysis-applied-business-science.
5 Brooks, What Data Can't Do, New York Times v. 18.2.2013, http://www.nytimes.com/2013/02/19/opinion/brooks-what-data-cant-do.html?smid=tw-share&_r=0; vgl. auch Mayer-Schönberger/Cukier, Big Data, New York 2013, S. 163 ff.
6 Vgl. Pariser, The Filter Bubble, London 2011, S. 176 f.

Algorithmen sind keineswegs „vorurteilsfrei". Wenn Nachrichtenportale versuchen, aus dem Verhalten eines Nutzers zu berechnen, welche Nachrichten den Nutzer mit der größten Wahrscheinlichkeit interessieren werden, bedarf es zur Programmierung der Algorithmen gewisser **Grundannahmen**. Diese Grundannahmen können richtig sein oder auch falsch. Der Rückschluss von der Häufigkeit des Anklicken gewisser Nachrichten auf deren Wichtigkeit für den Nutzer ist beispielsweise nicht mehr als eine Annahme, deren Richtigkeit keineswegs sicher ist[1]: 36

„In einer Welt von Big Data geht es vielfach nicht so sehr um die Richtigkeit der ‚Rohdaten', sondern um die Richtigkeit der ‚Rückschlüsse', die aus den Daten gezogen werden. Fehlerhafte, manipulatorische und diskriminierende Schlussfolgerungen können aus vollkommen unverfänglichen, zutreffenden Daten gezogen werden. Der Beobachter einer Big-Data-Analyse kann die Ergebnisse seiner Untersuchung beeinflussen durch die Definition des Datensatzes, die Aufstellung einer Hypothese oder das Schreiben eines Algorithmus. Big Data-Analyse ist letztlich ein Prozess der Interpretation, bei dem die eigene Person und Perspektive die Ergebnisse beeinflusst. Wie bei jedem Interpretationsprozess unterliegt die Analyse den Gefahren des Irrtums, der Inkorrektheit und des Vorurteils[2]."

Was für das gesamte Datenschutzrecht gilt, gilt auch für „Big Data": Es geht keineswegs nur um den Schutz von Persönlichkeitsrechten, sondern auch um den Schutz anderer Freiheiten vor einem **übereifrigen Regulator**: Ob Wissenschaftsfreiheit, Kommunikationsfreiheit oder auch die unternehmerische Betätigungsfreiheit. Neben dem gesellschaftlichen Bedürfnis nach Innovation und wirtschaftlichem Wachstum stehen auch gewichtige Freiheitsrechte auf dem Spiel, wenn im Zeichen des Datenschutzes „Big Data"-Anwendungen regulatorisch beschränkt oder verboten werden. Daher bedarf es nicht nur neuer Schutzinstrumentarien für neue Gefährdungen von Persönlichkeitsrechten. Ebenso wichtig ist es, andere Freiheitsrechte davor zu bewahren, dass sie durch ein starres Festhalten an „bewährten Prinzipien" in Gefahr geraten[3]. 37

V. Profiling

1. Begriff

Amazon, Google und Facebook gehören zu den Vorreitern des Phänomens, das man als „Profiling" bezeichnet. Mit diesem Begriff bezeichnet man die systematische Auswertung des **Nutzerverhaltens**. Es wird erfasst, für welche Seiten, Bücher, Werbebanner und Suchbegriffe ein Besucher der Website sich interessiert hat. Algorithmen errechnen sodann, 38

1 Vgl. Crawford, Thing Again: Big Data, Foreign Policy vom 9.5.2013, www.foreignpolicy.com/articles/2013/05/09/think_again_big_data.

2 Tene/Polonetsky, Big Data for All: Privacy and User Control in the Age of Analytics, 11 Nw. J. Tech. & Intell. Prop. 239 (2013), 270 f., http://scholarlycommons.law.northwestern.edu/njtip/vol11/iss5/1.

3 An den Prinzipien festhalten möchte Weichert, ZD 2013, 251, 255 ff.

welche Suchergebnisse, Waren oder Werbeanzeigen den Besucher voraussichtlich interessieren werden. Der Internetnutzer erhält auf diese Weise „maßgeschneiderte", zielgerechte („**targeted**") Werbung und erfährt (nur noch) das, was ihn mutmaßlich interessiert[1].

39 Die Entwicklung immer intelligenterer Algorithmen steht noch am Anfang. Immer größere Datenmengen („**Big Data**") erfassen das Nutzerverhalten, und die Daten werden immer raffinierter ausgewertet und analysiert. Der Besucher einer Nachrichtenseite erhält dann nur noch Nachrichten, die (voraussichtlich) zu seinem Leseverhalten passen. Der Nutzer einer Musikplattform wird laufend mit Musikvorschlägen konfrontiert, die den individuellen Musikgeschmack treffen sollen. Und der Online-Spieler, der sich „Angry Birds" (des finnischen Spieleanbieters Rovio) als App auf sein Smartphone lädt, muss damit rechnen, dass die App laufend seinen Aufenthaltsort erfasst und auch andere Daten auswertet, die auf dem Mobiltelefon gespeichert sind:

> „Als äußerstes Mittel rät Rovio Nutzern, die die Sammlung von Daten oder Werbeanzeigen vermeiden wollen, auf das Spiel zu verzichten: ‚Wenn Du sicher sein möchtest, dass Du von verhaltensbezogener Werbung verschont bleibst, benutze bitte unsere Dienste nicht und halte Dich von ihnen fern.'"[2]

2. Kritik

40 Das Profiling baut auf der Prämisse auf, dass ein Nutzer Interessen hat, die sich aus seinem Nutzerverhalten mathematisch ableiten lassen – eine Annahme, die nicht unumstritten ist. Eine **„Welt der Vorhersagen"**, die zu einer „Welt der Vorherbestimmung" wird, bei der der freie Wille auf der Strecke bleibt[3], ist gewiss alles andere als wünschenswert. Dies umso weniger, als Kreativität, Flexibiliät und Spontaneität auf der Strecke bleiben könnten[4].

41 Wenn zudem Algorithmen geheim bleiben, ist die Grundlage der Beziehung des Nutzers zu einem Online-Dienst weder Transparenz noch Augenhöhe, sondern (blindes) Vertrauen[5]. Und Vertrauen fällt bei einem Unternehmen wie Google schwer, wenn das Unternehmen sich sogar von einem Bewunderer als „undurchsichtig und geheimniskrämerisch wie (Ex-US-Vizepräsident) Dick Cheney"[6] bezeichnen lassen muss.

---

1 Zu datenschutzrechtlichen Aspekten verhaltensbezogener Onlinewerbung vgl. Rammos, K&R 2011, 692 ff.
2 O'Brien, Data-Gathering via Apps Presents a Gray Legal Area, New York Times v. 28.10.2012, http://www.nytimes.com/2012/10/29/technology/mobile-apps-have-a-ravenous-ability-to-collect-personal-data.html?ref=technology&_r=0.
3 Schirmacher, Payback, München 2009, S. 221.
4 Vgl. Schirrmacher, Payback, München 2009, S. 69 f.
5 Vgl. Levy, In The Plex, New York 2011, S. 56 f.
6 Jarvis, What Would Google Do?, New York 2008, S. 97.

3. „Diffuse Bedrohlichkeit“

Wenn das Verhalten des Internetnutzers systematisch beobachtet, erfasst und analysiert wird, kann dies beim Nutzer ein „diffus bedrohliches Gefühl des Beobachtetseins“[1] hervorrufen. Hierin liegt eine erhebliche Herausforderung für den Schutz von Persönlichkeitsrechten. Die **„diffuse Bedrohlichkeit“** verlangt nach **Transparenz**. Zu Recht hat das BVerfG in seiner Entscheidung zur Vorratsdatenspeicherung daran erinnert, dass Regelungen zur Information der von Datenerhebungen oder -nutzungen Betroffenen zu den elementaren Instrumenten des grundrechtlichen Datenschutzes gehören[2]. 42

Hohe Transparenzstandards können dem Nutzer ein selbstbestimmtes Handeln ermöglichen. Der Nutzer, der in verständlicher und ausführlicher Form Informationen darüber abrufen kann, wie ein Anbieter mit Daten umgeht, kann eine informierte Entscheidung darüber treffen, ob er einen Internetdienst nutzen möchte. Dies wird den Gegebenheiten der Netzwelt wesentlich gerechter als eine starre Fixierung auf Einwilligungserfordernisse[3]. Jedes Postulat, der Nutzer möge selbst über die Preisgabe von Daten bestimmen, wird zu einer Fiktion, wenn Einwilligungserklärungen im Massenverkehr vorformuliert werden. Ohne eine Vorformulierung sind Einwilligungen im Netz indes undenkbar. 43

VI. Das Ende der Datensparsamkeit

Es sei einmal dahingestellt, ob **„Datenminimierung“** überhaupt ein realistisches Ziel moderner Regulierung sein kann. Selbst wenn man noch an die Durchsetzbarkeit von „Datenvermeidung“ glaubt, stellt sich die viel grundlegendere Frage, ob es gesellschaftspolitisch richtig ist, die „Datenflut“ zu bremsen. Und diese Frage muss man entschieden verneinen: 44

- Daten sind der Rohstoff der Kommunikation und Information. „Datenminimierung“ heißt daher zugleich **„Kommunikations- und Informationsminimierung“**. Dies ist sozialschädlich. Eine freie Gesellschaft braucht nicht weniger, sondern mehr Kommunikation.
- Ob Verkehrslenkung (Verkehrstelematik)[4], Gesundheitsvorsorge oder intelligente Stromzähler: Je größer der ausgewertete Datenbestand ist, desto besser werden die Ergebnisse. Ein Stromzähler kann nur entweder „smart“ oder „datensparsam“ sein; nicht jedoch beides zugleich. Wer intelligente technische Lösungen möchte, kann den Anbietern

1 BVerfG vom 2.3.2010 – BvR 256/08, 1 BvR 263/08, 1 BvR 586/08 – Vorratsdatenspeicherung, Rz. 212.
2 BVerfG vom 2.3.2010 – BvR 256/08, 1 BvR 263/08, 1 BvR 586/08 – Vorratsdatenspeicherung, Rz. 242.
3 Härting, AnwBl 2011, 246, 248.
4 Vgl. ‚Every new car‘ connected to web by 2014, BBC News Technology v. 12.2.2013, http://www.bbc.co.uk/news/technology-21411335.

nicht zugleich Datenaskese verordnen. „Datenminimierung" ist **innovationsfeindlich** und rückwärtsgewandt.

45 Wenn immer größere Datenmengen in intelligenten Netzen Wege zu neuen Erkenntnissen, zu Innovation und Fortschritt eröffnen, werden die Prinzipien der **Datensparsamkeit** und Datenvermeidung (§ 3a BDSG) nicht nur wirklichkeitsfern, sondern innovationshemmend und kommunikationsfeindlich[1]. Sie sind realitätsfremd und gehen an den kommunikativen Bedürfnissen der Akteure vorbei.[2] Der vielfältige Austausch von Daten ist kommunikativ gewollt.

46 Man muss froh sein, dass die Entwicklung des Datenschutzes zur **Informationskontrolle** noch nicht allzu weit vorangeschritten war in den Jahren, in denen Wikipedia entstand. Würde Wikipedia heutzutage neu entstehen, wären Diskussionen darüber zu erwarten, wie sich die „Datenflut" mit den Grundsätzen der Datensparsamkeit und Datenvermeidung verträgt und wie man den Bürger dagegen schützen kann, dass über ihn ungewollt – zutreffende oder auch falsche – Informationen bei Wikipedia veröffentlicht werden.

47 Gelegentlich wird behauptet, der **staatliche Zugriff** auf Datenbestände bei Apple, Google & Co. lasse sich nur dann wirksam einschränken, wenn möglichst wenige dieser Daten anfallen. Ein solches Verständnis von „Datensparsamkeit" schießt über das Ziel hinaus, indem es – verfehlt – die Informationen und nicht den informationshungrigen Staat als Gefahr begreift. Die Limitierung staatlicher Eingriffsbefugnisse gehört zu den Kernaufgaben des rechtsstaatlichen Gesetzgebers. Wenn auf eine solche Limitierung verzichtet wird und stattdessen datenverarbeitende Untenehmen zur „Sparsamkeit" verpflichtet werden, kommt dies einem **rechtsstaatlichen Offenbarungseid** gleich.

48 Ebenso wie das Prinzip der Datensparsamkeit gehört auch das Gebot der **Zweckbindung** auf den Prüfstand. So wie sich heute nicht sagen lässt, welche Erkenntnisse spätere Generationen von Astronomen aus den Planck-Daten gewinnen lassen[3], lässt sich beispielsweise auch nicht abschätzen, ob die Tweets von heute schon morgen der Rohstoff von medizinischen Innovationen sein werden, die in der Zukunft Krankheiten besiegen, die heute als unheilbar gelten. Die Analyse von „zufällig" vorhandenen Daten zu neuen Zwecken ist grundlegend für die innovative Kraft, die „Big Data" innewohnt:

---

1 Tene/Polonetsky, Big Data for All: Privacy and User Control in the Age of Analytics, 11 Nw. J. Tech. & Intell. Prop. 239 (2013), 260, http://scholarlycommons.law.northwestern.edu/njtip/vol11/iss5/1.

2 Härting, AnwBl 2012, 718, 720.

3 Vgl. dpa-Meldung vom 21.3.2013, Weltraumteleskop zeigt detailliertes Bild des Universums, http://www.focus.de/wissen/diverses/planck-mission-weltraumteleskop-zeigt-detailliertes-bild-des-universums_aid_945345.html.

„Eine ebenso große Herausforderung liegt im Zeitalter von ‚Big Data' darin, dass zur Zeit der Datenerhebung ein großer Teil des Werts persönlicher Informationen nicht vorhersehbar ist zu dem Zeitpunkt, an dem die Einwilligung normalerweise erteilt wird. Da künftige Nutzungen die Notwendigkeit mit sich bringen würden, die Betroffenen um eine erweiterte Einwilligung zu bitten, werden viele dieser Nutzungen aus Kostengründen schlichtweg unterbleiben trotz ihres erheblichen individuellen und gesellschaftlichen Nutzens."[1]

VII. Schutz vor Missbrauch und Diskriminierung

Statt weiter auf das falsche Pferd der Datensparsamkeit zu setzen, müs- 49
sen persönliche Informationen stärker als bisher gegen **Missbrauch** und **Diskriminierung** geschützt werden:

- **Datensicherheit:** Dienste, die auf „Big Data" setzen, müssen stärker als bisher zur Sicherung der Daten gegen einen missbräuchlichen Zugriff verpflichtet werden.
- **Anonymität und Pseudonymität**: Sie sind eine „Schutzhülle" des Persönlichkeitsrechts, da sie Risiken der Identifizierung mindern. Daher müssen Anreize gesetzt werden für einen Verzicht auf „Klarnamen".
- **Transparenz:** Der Nutzer muss die Möglichkeit haben, sich in den Datenschutzbestimmungen eines Internetanbieters umfassend darüber zu informieren, welche Daten auf welche Weise zu welchen Zwecken gesammelt werden und wie diese Daten durch Maßnahmen des technischen Datenschutzes gegen den missbräuchlichen Zugriff durch Dritte gesichert sind[2].
- **Diskrimierungsschutz**: Je ausgefeilter und undurchschaubarer die Algorithmen werden, mit denen „Big Data" analysiert wird, desto problematischer wird es, wenn Personen- und Verhaltensdaten zur Grundlage von Entscheidungen werden, die sich auf die Lebensumstände einzelner Menschen auswirken[3].

1. Pseudonymität und Anonymität

Eine Förderung der pseudonymen oder anonymen Nutzung von Online- 50
Diensten ist notwendig. Wenn Bürger kommunizieren können, ohne sich identifizieren zu müssen, erleichtert dies die **freie Kommunikation und Information**:

---

1 Cate/Mayer-Schönberger, Notice and consent in a world of Big Data, International Data Privacy Law, 2013, Vol. 3, No. 2, S. 67, 67, http://m.idpl.oxfordjournals.org/content/3/2/67.full.pdf; vgl. auch Solove, Privacy Self-Management and the Consent Dilemma, 126 Harvard Law Review 1880 (2013), 1902, http://www.harvardlawreview.org/media/pdf/vol126_solove.pdf.

2 Härting, AnwBl 2011, 246, 247 f.

3 Vgl. Mayer-Schönberger/Cukier, Big Data, New York 2013, S. 157 ff.

„Anonymität und Pseudonymität schützen Menschen vor Voreingenommenheit gegen die Person und ermöglichen es Menschen, frei zu sprechen, ihr Wahlrecht auszuüben und sich zu versammeln, ohne Sanktionen befürchten zu müssen."[1]

51 Die Nutzung eines Pseudonyms ist eine nach außen gerichtete Selbstdarstellung und daher als Akt der kommunikativen Persönlichkeitsentfaltung durch das allgemeine Persönlichkeitsrecht (Art. 2 Abs. 1 i.V.m Art. 1 Abs. 1 GG) geschützt[2]. Das Recht auf freie Entfaltung der Persönlichkeit umfasst das Verfügungsrecht über die Darstellung der eigenen Person. Dabei ist es Sache des Betroffenen selbst, zu bestimmen, was seinen sozialen Geltungsanspruch ausmachen soll. Der Inhalt des allgemeinen Persönlichkeitsrechts ist wesentlich durch das Selbstverständnis seines Trägers geprägt[3]. Das Pseudonym ist bei der Netzkommunikation ein typisches Instrument der Selbstdarstellung.

52 Die Anonymität zählt zu den Grundbedingungen der freien Rede. Hinter einer anonymen Meinungsäußerung steht oft ein **legitimes Bedürfnis** nach Geheimhaltung. Die Möglichkeit der Anonymität erleichtert die Ausübung der Meinungsfreiheit. Dies schließt es aus, die Meinungsfreiheit bei anonymen Äußerungen stärker einzuschränken, als dies bei Äußerungen unter Namensnennung der Fall ist[4].

53 Eine Beschränkung der Meinungsfreiheit auf Äußerungen, die einem bestimmten Individuum zugerechnet werden können, wäre mit Art. 5 Abs. 1 Satz 1 GG nicht vereinbar. Die Verpflichtung, sich namentlich zu einer bestimmten Meinung zu bekennen, würde die Gefahr begründen, dass der Einzelne aus Furcht vor Repressalien oder sonstigen negativen Auswirkungen sich dahingehend entscheidet, seine Meinung nicht zu äußern. Dieser **Gefahr der Selbstzensur** soll durch das Grundrecht auf freie Meinungsäußerung entgegengewirkt werden[5].

54 Pseudonyme und der Verzicht auf „Klarnamen" haben eine lange Historie als Instrumente des Persönlichkeitsschutzes und des Schutzes vor staatlicher Verfolgung. Sie sind zum Selbstschutz unverzichtbar und haben sich bei der Netzkommunikation fest etabliert.

55 Das Pseudonym ist eine bewährte Methode des Schutzes der Privatsphäre. Dies erfährt der Jurastudent im ersten Semester, wenn er mit dem Fall der Schauspielerin konfrontiert wird, die unter Verwendung eines Phantasienamens ein Hotelzimmer bucht[6]. Der falsche Name bei der Reser-

1 Solove, Understanding Privacy, Cambridge/London 2009, S. 125.
2 Scholz in Simitis, BDSG, § 3 Rz. 213.
3 BVerfG v. 25.10.2005 – 1 BvR 1696/98, Rz. 25; BVerfG v. 23.7.2007 – 1 BvR 150/06, Rz. 19.
4 Vgl. BGH v. 23.6.2009, NJW 2009, 2888 – spickmich.de; OLG Frankfurt v. 8.3.2012 – 16 U 125/11, Rz. 28 ff.
5 OLG Hamm v. 3.8.2011 – I-3 U 196/10, Rz. 4, ITRB 2011, 253 f. (Rössel).
6 Vgl. Medicus, AT, § 56 Rz. 907.

vierung eines Hotelzimmers, die diskreten Initialien am Klingelschild des prominenten Hausbewohners, der Phantasiename beim Besuch einer Rotlichtbar: Der Verzicht auf den „Klarnamen" schützt den Namensträger vor unerwünschten Zudringlichkeiten.

Der Deckname ist auch ein bewährtes Mittel zum Schutz vor staatlicher Verfolgung. Der Auslandsspion tritt nie mit seinem „Klarnamen" in Erscheinung. Und mutige Autoren haben sich in vergangenen Zeiten häufig eines Pseudonyms bedient, um staatlichen Zensoren die Arbeit zu erschweren. Kurt Tucholsky verwendete in seinen Kolumnen neben seinem „Klarnamen" vier verschiedene Fantasienamen[1]. 56

Bei der vordigitalen Kommunikation war der Deckname dennoch die seltene Ausnahme. So wie es den meisten Menschen selbstverständlich war, mit vollem Namen und mit Postanschrift im Telefonbuch verzeichnet zu sein, entsprach es auch sonst den normalen Lebensgewohnheiten, den „**Klarnamen**" zu verwenden. Diese Gewohnheiten haben sich durch die digitale, vernetzte Kommunikation geändert[2]. In weiten Bereichen der Netzkommunikation ist der „Klarname" zur Ausnahme geworden und der Phantasiename zur Regel. Dies fängt bei gängigen E-Mail-Adressen an (mausi94@xxx.de) und setzt sich fort in der Welt der Online-Spiele sowie bei den Datingplattformen. Auch in Blogs und Diskussionsforen sind „Klarnamen" die Ausnahme. 57

2. Diskriminierungsschutz

Wenn anonyme Big Data-Bestände von einer Krankenkasse ausgewertet werden, um Erkenntnisse über die Häufung von Krankheiten in bestimmten Wohngebieten zu gewinnen, stellt sich für den Gesetzgeber die Frage, ob es der Krankenkasse erlaubt sei soll, ihre Tarifstruktur an diesen Erkenntnissen auszurichten. Ein Diskriminierungsschutz, den es im deutschen Datenschutzrecht – jedenfalls ansatzweise – bereits für das **Kreditscoring** gibt (§ 28b BDSG), wird auch in vielen anderen Lebensbereichen notwendig werden. 58

3. Schutz der digitalen Identität

Durch die Auswertung des Verhaltens des Nutzers eines Online-Dienstes entsteht ein Bild, das sich als „digitale Identität" bezeichnen lässt. Wenn der Nutzer weder Kenntnis von dieser „Identität" hat noch Einfluss auf deren Gestaltung, verliert er Einfluss auf das Bild, das sich andere von ihm machen können. Wenn es eine „digitale Identität" gibt, muss es auch ein **Selbstbestimmungsrecht** an dieser Identität geben. Dieses Recht 59

1 Tucholsky schrieb unter den Pseudonymen Kaspar Hauser, Peter Panter, Theobald Tiger und Ignaz Wrobel, vgl. http://www.tucholsky-gesellschaft.de/, zuletzt abgerufen am 9.5.2013.

2 Vgl. Iraschko-Luscher/Kiekenbeck, ZD 2012, 261, 263 f.

kann nicht absolut gelten, die Grenzen bedürfen noch der näheren Untersuchung und Ausgestaltung.

60 Wenn es eine „digitale Identität" gibt, gibt es auch ein Bedürfnis, alle Informationen, aus denen sich diese „Identität" zusammensetzt, gegen den unberechtigten oder missbräuchlichen **Zugriff Dritter** zu schützen. Profiling und Datensicherheit gehören daher zusammen. Dabei wird das Phänomen des **„Identitätsdiebstahls"** mehr und mehr zum Problem. Wenn durch das Abfischen von Zugangsdaten oder auf andere Weise eine „digitale Identität" gekapert wird, können beträchtliche materielle und immaterielle Schäden entstehen[1].

61 In seiner Entscheidung zur Vorratsdatenspeicherung hat das BVerfG die verfassungsrechtliche Dimension technischer Schutzmaßnahmen betont[2]. Je größer die Datenbestände sind, die gesammelt werden, desto größer wird die Bedeutung von technischen Schutzmaßnahmen gegen einen unberechtigten, missbräuchlichen Zugriff. Nur ein hoher Standard an **Datensicherheit** schafft das Vertrauen, das die Netzinfrastruktur benötigt zur Erfüllung ihrer vielfältigen Aufgaben des Informationsflusses und -austauschs[3].

4. Schutz gegen Marktmacht

62 Wenn die durch Profiling entstehenden Datenbestände einen erheblichen wirtschaftlichen Wert darstellen, liegt in jeder Form der Monopolbildung eine natürliche Aufgabe für Kartellbehörden und Kartellrecht. Und innovationsbremsendes **Marktversagen** ist heute schon Realität:

> „Die größte Innovationsbremse ist jedoch womöglich der Umstand, dass die Technologien, die das Sprungbrett sein könnten für Überraschungen der nächsten Generation zunehmend geschlossen und kontrolliert sind. So wurde etwa Facebook auf dem Netz aufgebaut, das eine offene Plattform war. Facebook ist jedoch eifrig bemüht, einen ummauerten Garten zu schaffen, in dem lediglich Innovationen entstehen können, die die Eigentümer erlauben. Dasselbe gilt für die an die Kette gelegten Geräte, die wir Smartphones und Tablets nennen."[4]

63 Monopole sind stets eine Momentaufnahme. Dies gilt in besonderem Maße für die Internetgiganten der heutigen Zeit und sollte stets bedacht werden, bevor voreilig die **Regulierungskeule** geschwungen wird:

> „Im Moment sind Apple, Google, Facebook und Amazon die vier führenden Monster. Vor 18 Jahren war jedoch Apple was kurz vor dem Aussterben, Amazon

1 Vgl. Solove, Understanding Privacy, Cambridge/London 2009, S. 126 ff.
2 BVerfG vom 2.3.2010, NJW 2010, 833, 840 – Vorratsdatenspeicherung.
3 BVerfG vom 2.3.2010, NJW 2010, 833, 840 – Vorratsdatenspeicherung.
4 Naughton, Has the internet run out of ideas already?, Observer v. 29.4.2012, http://www.guardian.co.uk/technology/2012/apr/29/internet-innovation-failure-patent-control.

war gerade neu, bis zur Gründung von Google dauerte es noch drei Jahre und Facebook lag neun Jahre in der Zukunft."[1]

Die Marktmacht einiger weniger Unternehmen stellt dennoch eine ernst zu nehmende **Gefahr** dar: 64

„Wir nutzen die Dienste dieser Unternehmen mit lustvoller Selbstvergessenheit und vergessen, dass sie zugleich eine Menge über uns erfahren. Eines Tages könnte uns die Weisheit des alten Sprichworts bewusst werden: Im Informationszeitalter *ist Wissen Macht*."[2]

„Datenportabilität" kann ein probates Instrument sein, um einem Marktversagen entgegenzuwirken, da die „Portabilität" dem Nutzer – beispielsweise bei einem monopolistischen Cloud-Anbieter – die einfache „Mitnahme" von Daten bei einem Wechsel zum Konkurrenten ermöglicht. Unerwünschte Nebeneffekte inklusive: Wenn die „Mitnahme" von Daten erleichtert wird, bedarf es erhöhter technischer und regulatorischer Anstrengung, um **Missbräuchen** durch den Staat oder durch private Dritte entgegenzuwirken[3]. 65

„Datenportabilität" kann auch ein Steuerungsinstrument sein, um sicherzustellen, dass der Nutzen maximiert wird, der sich aus umfangreichen Datenbeständen ziehen lässt. Warum soll ein Unternehmen, das eine „Fitness-App" anbietet, die jeden einzelnen Laufsport mitprotokolliert, über Daten verfügen, die Rückschlüsse auf die Gesundheit des Nutzers zulässt, ohne verpflichtet zu sein, dem Nutzer diese Daten uneingeschränkt (auf Anforderung) zu überlassen? **Gesellschaftspolitisch** spricht alles dafür, auch unter diesem Gesichtspunkt dem Nutzer ein **Recht auf „Datenportabilität"** einzuräumen: 66

„Als ‚Gegenleistung' für Lockerungen bei Verarbeitungsverboten und der Datensparsamkeit, sollten Organisationen bereit sein, mit den Nutzern das Wirtschaftsgut zu teilen, das durch die Daten der Nutzer entsteht. Dies bedeutet, den Nutzern Zugang zu ihren Daten zu gewähren in einem „nutzbaren" Format und den Nutzern die Möglichkeit zu eröffnen, Anwendungen Dritter fruchtbar zu machen, um ihre eigenen Daten zu analysieren und nützliche Schlüsse daraus zu ziehen (z.B. weniger Eiweiß konsumieren, Ski fahren gehen, in Anleihen investieren)."[4]

Bei der „Portabilität" geht es nicht um den Schutz personenbezogener Daten gemäß Art. 8 EU-GRCharta[5], sondern um **das Wohl der Allge-** 67

1 Naughton, Even Google won't be around for ever, let alone Facebook, Observer v. 3.3.2013, http://www.guardian.co.uk/technology/2013/mar/03/google-facebook-nothing-lasts-for-ever.
2 Naughton, From Gutenberg to Zuckerberg, London 2012, S. 269.
3 Vgl. Goldman, A Dark Side of Data Potability; Litigators Love It, Forbes v. 17.10.2012, http://www.forbes.com/sites/ericgoldman/2012/10/17/a-dark-side-of-data-portability-litigators-love-it.
4 Tene/Polonetsky, Big Data for All: Privacy and User Control in the Age of Analytics, 11 Nw. J. Tech. & Intell. Prop. 239 (2013), 264, http://scholarlycommons.law.northwestern.edu/njtip/vol11/iss5/1.
5 Vgl. Härting, BB 2012, 459, 465.

meinheit, das Beschränkungen der unternehmerischen Freiheit legitimiert (Art. 17 Abs. 1 Satz 3 EU-GRCharta)[1]. Die Legitimation der Beschränkung liegt in der marktmächtigen Stellung von Unternehmen wie Google, Facebook und Apple. Je mehr Facebook, Apple und andere Anbieter „Netze im Netz" bilden und abschotten, desto mehr stellt sich die Frage, wie man die abgeschirmten Datenbestände dagegen sichert, dass **„Informationsinseln"** entstehen, die die offene Netzstruktur, den freien Informationsaustausch und die sich daraus ergebenden Innovationschancen behindern[2].

68 Je marktmächtiger Unternehmen werden, die ihre Algorithmen geheim halten, desto lauter wird der Ruf nach einer (gesetzlichen) Offenlegung der Algorithmen. Wenn ein Monopolist per Algorithmus, aber keineswegs „automatisiert"[3] Informationen filtert, besteht auch unter dem Gesichtspunkt der Informationsfreiheit ein erhebliches **Bedürfnis nach Transparenz**.

5. Schutz gegen staatlichen Zugriff

69 Wenn Datenbestände, die durch Profiling bei Apple, Google & Co. entstehen, gegen den missbräuchlichen Zugriff Dritter geschützt werden müssen, gilt dieses Schutzbedürfnis in besonderem Maße gegenüber dem langen Arm des Staates. Orwells „Big Brother" konnte von der Menge, Dichte und Tiefe an Informationen, die das Profiling ermöglicht, bestenfalls träumen:

> „Für Regierungen aller politischen Richtungen – von autoritären Regimes zu liberalen Demokratien – ist das Internet ein Überwachungswerkzeug, das ihnen der Himmel geschenkt hat, weil die Überwachung größtenteils durch Computer erledigt werden kann statt durch teure und fehlsame Menschen."[4]

70 Der staatliche Zugriff auf diese Daten muss **streng limitiert** werden, um den Bürger nicht gegenüber staatlichen Behörden unfreiwillig „gläsern" werden zu lassen:

> „Die Sicherheitsbehörden schielen neidvoll darauf, und es gibt kaum Möglichkeiten – Gefahr im Verzug vorausgesetzt –, ihnen den Zugang zu verweigern. Den Firmen liefern die Konsumenten ihre Daten freiwillig. Jede Transaktion hinterlässt eine Spur im Netz, die mit der dazugehörigen Person verbunden werden kann.

---

1 Vgl. Tene/Polonetsky, Big Data for All: Privacy and User Control in the Age of Analytics, 11 Nw. J. Tech. & Intell. Prop. 239 (2013), 269, http://scholarlycommons.law.northwestern.edu/njtip/vol11/iss5/1.

2 Vgl. Heller, Post-Privacy, S. 91.

3 Vgl. Lohr, Algorithms Get a Human Hand in Steering Web, New York Times v. 10.3.2013, http://www.nytimes.com/2013/03/11/technology/computer-algorithms-rely-increasingly-on-human-helpers.html?smid=tw-nytimestech&seid=auto&_r=0; Orlowski, Revealed: Google's manual for its unseen humans who rate the web, The Register v. 28.11.2012, http://www.theregister.co.uk/2012/11/27/google_raters_manual.

4 Naughton, From Gutenberg to Zuckerberg, London 2012, S. 261.

Dieser Daten-Striptease ist der Preis für die allumfassende Verfügbarkeit der Angebote aus der bunten Warenwelt. Die Freiheit des Konsumenten erscheint grenzenlos, so er über ein mobiles Kommunikationsgerät und eine Kreditkarte verfügt."[1]

6. Accountability

Accountability" ist ein Konzept, das hilfreich sein könnte, um Gefährdungen von Persönlichkeitsrechten entgegenzuwirken. Die Übersetzung ins Deutsche fällt schwer, da sich nicht klar sagen lässt, ob „Verantwortlichkeit" oder „Verantwortung" den Begriffskern besser trifft. 71

Um „Accountability" ging es 2009 in dem Galway Project, an dem zahlreiche Datenschutzexperten aus Europa und den USA mitwirkten. Zum Abschluss des Projekts veröffentlichten die Experten ein Diskussionspapier, in dem ein neuer, „Accountability-orientierter Ansatz" folgendermaßen definiert wurde[2]: 72

„Eine accountability-orientierte Herangehensweise an Datenverarbeitung zeichnet sich dadurch aus, dass die Definition von Zielen im Mittelpunkt steht, die Organisationen zum Schutz von Persönlichkeitsrechten zu beachten haben. Die Ziele fußen auf gesetzlichen Vorgaben, wobei den Organisationen Spielräume bei der Bestimmung geeigneter Maßnahmen zur Erreichung dieser Ziele gelassen werden. Eine accountability-orientierte Herangehensweise ermöglicht es Organisationen, Methoden und Wege zu entwickeln, um diese Ziele in einer Weise zu erreichen, die am besten zu ihren Geschäftsmodellen, Technologien und zu den Bedürfnissen ihrer Kunden passt."

„Accountability" bedeutet demnach eine Verlagerung der Verantwortung für den Schutz der Privatsphäre auf den Datenverarbeiter. Der Datenverarbeiter erhält vom Gesetzgeber klare Zielvorgaben („goals" und „criteria"). Wie er die vorgegebenen Ziele erreicht, bleibt seinem Ermessen („discretion") überlassen. Hierdurch erhält der Datenverarbeiter den notwendigen Spielraum, um seine Technologie und sein Geschäftsmodell datenschutzfreundlich auszugestalten. 73

VIII. „IT-Grundrecht" – der schlummernde Riese

In dem Urteil zur Online-Durchsuchung hat das BVerfG ein **neues Grundrecht** geschaffen: das „IT-Grundrecht" (Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme)[3]. Dass es eines 74

1 Kreissl, Datenspuren – Komplette Umkehr der Beweislast, New Scientist v. 22.2.2013, http://www.newscientist.de/inhalt/datenserver-umkehr-der-beweislast-a-885489.html.

2 Centre for Information Policy Leadership Data Protection Accountability: The Essential Elements, Oktober 2009, http://www.ftc.gov/os/comments/privacyroundtable/544506-00059.pdf.

3 BVerfG vom 27.2.2008, NJW 2008, 822 ff. – Online-Durchsuchung.

solchen „neuen" Grundrechts bedarf, hat das BVerfG unter anderem damit begründet, dass das Recht auf informationelle Selbstbestimmung **Schutzlücken** aufweist[1]. Das Gefahrenpotential, gegen das das „IT-Grundrecht" schützt, liegt nach dem BVerfG darin, dass ein Dritter sich durch Zugriff auf ein informationstechnisches System einen potentiell äußerst großen und aussagekräftigen Datenbestand verschaffen kann, ohne noch auf weitere Datenerhebungs- und Datenverarbeitungsmaßnahmen angewiesen zu sein[2]. Der heimliche Blick auf die Computerfestplatte lässt sich mit dem althergebrachten Blick durch das **Schlüsselloch** vergleichen. Unbemerkt gelangt ein „Eindringling" in die Privatsphäre.

75 Obwohl Einigkeit darüber besteht, dass das in der Online-Durchsuchung geschaffene „IT-Grundrecht" Drittwirkung hat und den Gesetzgeber zu schützenden Maßnahmen im Bereich der Privatwirtschaft aufruft, ist die Diskussion um **gesetzgeberische Konsequenzen**[3] bislang in ersten Anfängen stecken geblieben. Die Grundrechtsgefahren durch Spuren vernetzter Kommunikation erfordern indes eine umfassende Anpassung des Persönlichkeits- und Datenschutzrechts an die Gegebenheiten der Informationsgesellschaft[4].

76 Im Datenschutzrecht wird man sich daran gewöhnen müssen, zwischen dem Recht auf informationelle Selbstbestimmung und dem „IT-Grundrecht" zu **differenzieren**. Möchte man die Grenzen nicht vollständig verwässern und das Datenschutzrecht nicht in ein allgemeines Verbraucher- und Bürgerschutzrecht umfunktionieren, führt kein Weg daran vorbei, das Erfordernis eines Personenbezuges gemäß § 3 Abs. 1 BDSG ernst zu nehmen und Daten nur dann als personenbezogen zu schützen, wenn ein Bezug zu einer konkret und namentlich bestimmbaren natürlichen Person ohne übermäßigen Aufwand herstellbar ist[5]. Neben den Schutz des Bürgers vor einer unkontrollierbaren Verarbeitung personenbezogener Daten tritt der Schutz vor Eingriffen in die Privatsphäre, die in einem unbemerkten und unkontrollierten „Ausspähen" der Computernutzung liegen[6].

1. Profiling als Anwendungsfall

77 Das unbemerkte Eindringen in die auf der Computerfestplatte gespeicherten Daten unterscheidet sich von der Datenerfassung, -verarbeitung und -nutzung insbesondere dadurch, dass es über den Einblick hinaus keiner weiteren Maßnahmen bedarf, um tief in die Privatsphäre des Bür-

1 BVerfG vom 27.2.2008, NJW 2008, 822, 824 – Online-Durchsuchung.
2 BVerfG vom 27.2.2008, NJW 2008, 822, 826 – Online-Durchsuchung.
3 Vgl. Bartsch, CR 2008, 613 ff.; Kutsche, DuD 2011, 461, 462 f.; Luch, MMR 2011, 75 ff.; Roßnagel/Schnabel, NJW 2008, 3534 ff.
4 Vgl. Hoffmann-Riem, JZ 2008, 1009, 1010.
5 Vgl. Dammann in Simitis, BDSG, § 3 Rz. 22 ff.
6 BVerfG vom 27.2.2008, NJW 2008, 822, 824 – Online-Durchsuchung.

gers zu gelangen[1]. Wer Kenntnis vom Innenleben einer Computerfestplatte oder einer Handy-Speicherkarte erlangt hat, ist damit weit in die **Privatsphäre** vorgedrungen, auch wenn es zu keiner Speicherung, Weitergabe oder Zusammenführung von Daten kommt[2].

Der Blick durch das „informationstechnische Schlüsselloch" unterscheidet sich von den herkömmlichen Gefahrenszenarien des Datenschutzrechts zudem dadurch, dass es für den Betroffenen keinen nennenswerten Unterschied macht, ob der Eindringling Kenntnis von seiner **Identität** hat. Die heimliche Ausspähung wird auch dann als Eingriff in die Privatsphäre empfunden, wenn sie gänzlich anonym erfolgt. Der „Spanner" wird auch dann als Eindringling in den Privatbereich empfunden, wenn er nicht weiß, welche Person er heimlich beobachtet. In einer sehr gelungenen, bildhaften Formulierung des BVerfG heißt es, die auf dem Endgerät gespeicherten Informationen ermöglichten es, „Einblick in wesentliche Teile der Lebensgestaltung einer Person zu gewinnen oder gar ein aussagekräftiges Bild der Persönlichkeit zu erhalten"[3]. 78

In der Heimlichkeit der Beobachtung liegt eine **Parallele** zwischen der Onlinedurchsuchung einerseits und der unbegrenzten und unkontrollierbaren Anlegung von **Nutzungsprofilen** im Internet: Die umfangreiche Speicherung von Daten bei Google stellt nach dem Empfinden vieler Nutzer einen Eingriff in die Privatsphäre dar. Dieser Eingriff wird nicht dadurch nennenswert abgemildert, dass die Betreiber von Google keine Kenntnis von der Identität der Person erlangen können, die hinter dem Nutzungsprofil stehen. Die Vorstellung, dass ein Internetanbieter über eine genaue Protokollierung besuchter Seiten die Möglichkeit hat, Interessen, Eigenheiten und Vorlieben des Nutzers sehr präzise zu analysieren, ist vielen Internetnutzern unangenehm. Die heimliche und unkontrollierte Protokollierung und Auswertung der Nutzergewohnheiten stellt ein „**Ausspähen**" des Bürgers dar, das sich von der gezielten Online-Durchsuchung einer Computerfestplatte allenfalls graduell unterscheidet. 79

Bei der Diskussion um die Personenbezogenheit von Daten beim Profiling[4] geht es im Wesentlichen darum, ob die Gefahr besteht, dass die anfallenden Datenspuren einem Nutzer zugeordnet werden, der Google namentlich bekannt ist. Für Dienste wie Facebook und Google sind Namen jedoch unwichtige Störgeräusche („**Noise**")[5]. Und beim Webtracking oder beim Profiling liegt der Eingriff in die Privatsphäre nicht darin, dass 80

1 Vgl. BVerfG vom 27.2.2008, NJW 2008, 822, 626 – Online-Durchsuchung.
2 Härting, AnwBl 2011, 246 f.
3 BVerfG vom 27.2.2008, NJW 2008, 822, 827 – Online-Durchsuchung.
4 Siehe Rz. 38.
5 Vgl. Hardy, Rethinking Privacy in an Era of Big Data, New York Times v. 4.6.2012, http://bits.blogs.nytimes.com/2012/06/04/rethinking-privacy-in-an-era-of-big-data/?ref=technology.

der Internetnutzer ernsthaft befürchten muss, von einem Google-Mitarbeiter namentlich identifiziert zu werden, wobei unter einer Identifizierung die Verbindung von Informationen zu einem Individuum zu verstehen ist[1].

81 Nicht die Sorge vor der **Deanonymisierung** ist es, die ein ungutes Gefühl bereitet, sondern der heimliche Blick durch das **virtuelle Schlüsselloch**. Wie beim Blick durch das Schlüsselloch liegt das Unbehagen nicht darin, dass der Eindringling weiß, wer ich bin. Der Internetnutzer nimmt es vielmehr als freiheitsbeschränkend wahr, dass er sich – anonym – beobachtet fühlt, ohne genau abschätzen zu können, mit welcher Genauigkeit die Beobachtung erfolgt. Bei der Diskussion um Cookies und IP-Adressen geht es letztlich darum, dass ein „potentiell äußerst großer und aussagekräftiger Datenbestand" entsteht, der den tiefen Einblick in die Persönlichkeit ermöglicht, aus dem das BVerfG das „IT-Grundrecht" abgeleitet hat[2]. Google Analytics ruft das „IT-Grundrecht" auf den Plan und nicht die informationelle Selbstbestimmung.

2. Das Ende der Anonymität

82 Das „IT-Grundrecht" kann der Schlüssel sein zu angemessenen Antworten des Rechts auf das Ende der Anonymität im Netz.

83 Bei der Netzkommunikation ist die „**absolute Anonymität**" schon lange eine Illusion:

> „Die gewaltigen Möglichkeiten der Reidentifizierung … verändern die rechtspolitischen Debatten über den Schutz der Privatsphäre. Diese Debatten kreisen heute fast ausschließlich um magische Formeln wie ‚personenbezogene Informationen' oder ‚persönliche Daten'. Die Fortschritte bei der Reidentifizierung zeigen, dass diese Formeln am eigentlichen Problem vollkommen vorbei gehen. Zwar ist es richtig, dass ein bösartiger Gegner personenbezogene Daten wie den Namen und die Sozialversicherungsnummer mit einer Person in Verbindung bringen kann. Der Gegner kann jedoch genau dasselbe erreichen mit Informationen, die niemand als personenbezogen bezeichnen würde."[3]

84 Der „absolute" Begriff des Personenbezugs[4] ist nicht die richtige Antwort auf die erweiterten Möglichkeiten der Reidentifizierung, da er zu einem Übermaß an Verboten führt:

> „Auf der anderen Seite werden aufgrund der erleichterten Reidentifizierung Gesetze wie die EU-Datenschutzrichtlinie übermäßig – faktisch uferlos. Da die Richtlinie darauf abstellt, ob sich Informationen ‚direkt oder indirekt' auf eine Person beziehen, wird die Richtlinie durch jede erfolgreiche Reidentifizierung einer vermeintlich anonymisierten Datenbank erweitert und findet auf diese Datenbank

1 Vgl. Solove, Understanding Privacy, Cambridge/London 2009, S. 122.
2 BVerfG vom 27.2.2008, NJW 2008, 822 ff. – Online-Durchsuchung.
3 Ohm, Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization, 57 UCLA Law Review 1701 (2010), 1704.
4 Siehe Rz. 76.

Anwendung. Je weiter die Möglichkeiten der Reidentifizierung fortschreiten, desto mehr wird die EU-Richtlinie aufgebläht … Ein Gesetz, das Grenzen haben sollte, wird grenzenlos, und die sorgsame Abwägung des Gesetzgebers zwischen Privatsphäre, Datenschutz und Datenverkehr wird aus den Angeln gehoben"[1].

Das heutige Datenschutzrecht fußt auf einem **„Schwarz-Weiß-Prinzip"**. 85
Wenn Daten Personenbezug haben, ist das kleinteilige Datenschutzrecht uneingeschränkt anwendbar. Fehlt es dagegen an einem Personenbezug, ist die Datenverarbeitung keinerlei Beschränkungen unterworfen. Das **„IT-Grundrecht"** ist ein **Türöffner** zur Durchbrechung des „Schwarz-Weiß-Denkens" und damit eines Regelungskonzepts, das zunehmend als verfehlt angesehen wird:

„Personenbezogene Daten sollten stattdessen anhand einer Risikomatrix definiert warden, ide die Risiken, Absichten und mögliche Konsequenzen einer Reidentifizierung berücksichtigt statt einer Dichotomie zwischen ‚bestimmbaren' und ‚nicht bestimmbaren' Personen. Ein bipolarer Ansatz, der sich darauf stützt, Daten entweder als ‚personenbezogen' anzusehen oder nicht, ist nicht hilfreich und führt zwangsläufig zu einem nutzlosen Wettrüsten zwischen Anonymisierung und Reidentifizierung."[2]

Unabhängig von einer nie ausschließbaren Reidentifizierung anonymer 86
Informationen wird eine Ausspähung auch dann als Eingriff in die Privatsphäre empfunden, wenn sie erfolgt, ohne dass dem Späher die Identität der ausgespähten Person bekannt ist[3]. Die umfangreiche Speicherung von Daten bei Google, Facebook und Apple stellt nach dem Empfinden vieler Nutzer einen Eingriff in die Privatsphäre dar. Die heimliche und unkontrollierte Protokollierung und Auswertung der Nutzergewohnheiten wird als ein „Ausspähen" des Nutzers empfunden, das sich von der gezielten Online-Durchsuchung einer Computerfestplatte allenfalls graduell unterscheidet[4].

3. Die „diffuse Bedrohlichkeit"

Auch bei der **Vorratsdatenspeicherung** geht es um Spuren der Kommuni- 87
kation. Die Nutzung des Internet oder auch des Mobiltelefons hinterlässt zahlreiche Spuren entstehen auf den Rechnern der Telekommunikationsunternehmen. Diese Spuren umfassen Telefonnummern, E-Mail- und IP-Adressen und Funkzellendaten. Sie ermöglichen ein detailliertes Bild über das Kommunikationsverhalten, die Kommunikationspartner und über Aufenthaltsorte[5]. Für diese Spuren gelang es dem BVerfG (in seinem Urteil zur Vorratsdatenspeicherung), die Gefahrenlage prägnant und plas-

1 Ohm, Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization, 57 UCLA Law Review 1701 (2010), 1741.
2 Tene/Polonetsky, Big Data for All: Privacy and User Control in the Age of Analytics, 11 Nw. J. Tech. & Intell. Prop. 239 (2013), 258, http://scholarlycommons.law.northwestern.edu/njtip/vol11/iss5/1.
3 Härting, Internetrecht, 4. Aufl. 2010, Rz. 72.
4 Härting, AnwBl. 2011, 246, 247; Schneider/Härting, ZD 2011, 63, 68.
5 BVerfG vom 2.3.2010, NJW 2010, 833, 838 – Vorratsdatenspeicherung.

tisch zu beschreiben. Das BVerfG erkennt die „**diffuse Bedrohlichkeit**", die durch staatliche Zugriffsrechte entsteht:

„Der Einzelne weiß nicht, was welche staatliche Behörde über ihn weiß, weiß aber, dass die Behörden vieles, auch Höchstpersönliches über ihn wissen können."[1]

88 Ersetzt man „Behörde" durch „Google", „Facebook" oder „Apple", ergibt dies einen Satz, der die vielfach empfundene „diffuse Bedrohlichkeit" der Aktivitäten der Unternehmen im Kern trifft[2].

89 Die „diffuse Bedrohlichkeit" des Profiling schafft ein unbestreitbares Bedürfnis an Transparenz. Das heimliche Profiling greift nachhaltig in das Selbstbestimmungsrecht des Betroffenen ein. Und selbst wenn dem Betroffenen die Auswertungsmaßnahmen grundsätzlich bekannt sind, muss Transparenz oberstes Gebot sein, da durch das Profiling aus zahlreichen Einzelinformationen ein umfassendes **Persönlichkeitsbild** entstehen kann:

„Das Ganze wird größer als die einzelnen Teile."[3]

4. Transparenz statt Einwilligung

90 So sehr das heimliche Profiling in das Selbstbestimmungsrecht eingreift, so wenig lässt sich die Einwilligung als probate Antwort auf das Profiling begreifen. Eine Einwilligung schafft per se keine Transparenz und kann allenfalls ein **Hilfsmittel** sein. Dies gilt umso mehr, als Online-Nutzungen stets Massenvorgänge sind, bei denen sich die Einwilligung notwendig in dem Anklicken einer vorgegebenen Formulierung erschöpft.

91 Wenn Nutzer gefragt werden, ob sie es für wünschenswert erachten, gefragt zu werden, bevor ein Online-Dienst Daten per Profiling erfasst, werden sie dies stets mehrheitlich bejahen[4]. Zugleich werden sie mehrheitlich wünschen, dass Dienste **kostenfrei** bleiben[5]. Einwilligungserfordernisse, die dazu führen, dass Dienste kostenpflichtig werden, kommen daher allenfalls vordergründig den Bedürfnissen der Nutzer entgegen.

92 Das Unbehagen, das die Profilbildung bei Google, Apple und Facebook vielen Nutzern bereitet, ist auch – ähnlich wie früher beim Scoring – auf die **fehlende Durchschaubarkeit** der Methoden zurückzuführen, mit de-

1 BVerfG 2.3.2010, NJW 2010, 833, 843 – Vorratsdatenspeicherung.
2 Härting, BB 2010, 839, 839; vgl. auch Masing, NJW 2012, 2305, 2309.
3 Solove, Understanding Privacy, Cambridge/London 2009, S. 118.
4 Vgl. Faltblatt der EU-Kommission: Wie sollen die vorhandenen Datenschutzvorschriften durch die Datenschutzreform der EU an neue technologische Entwicklungen angepasst werden?, http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/8_de.pdf.
5 Vgl. Sengputa, Web Privacy Becomes a Business Imperative, New York Times v. 3.3.2013, http://www.nytimes.com/2013/03/04/technology/amid-do-not-track-effort-web-companies-race-to-look-privacy-friendly.html?ref=technology&_r=0.

nen die Profilbildung erfolgt. Mittelfristig wird der Druck auf die großen Plattformbetreiber wachsen, die Türen der „Geheimküchen", in denen die Algorithmen nach und nach verfeinert werden, ein Stück weit zu öffnen[1]:

„Die Verpflichtung von Unternehmen, ihre Entscheidungskriterien offenzulegen (nicht notwendig die Algorithmen, aber die Faktoren, die in die Algorithmen einfließen), markiert eine Trennlinie zwischen Recht und Technologie. Fairness und Gerechtigkeit gebieten es, dass der Betroffene informiert wird über die Grundlagen von Entscheidungen, die ihr Leben beeinflussen, dies insbesondere wenn es um Entscheidungen geht, die von Maschinen vorgenommen werden, die mit undurchsichtigen Kriterien arbeiten"[2].

5. Folgerungen aus dem „IT-Grundrecht"

Wenn das „IT-Grundrecht" eines Tages aus dem Dornröschenschlaf erwacht, wird es Grundlage sein für gesetzliche Regelungen, die den Bürger vor einer heimlichen Protokollierung seiner Nutzungsgewohnheiten schützen. 93

Unabhängig von der weiteren Entwicklung der europäischen Reformdebatte lässt sich feststellen, dass drei Grundbedingungen für die „Spuren im Netz" gelten sollten: 94

- Es bedarf einer gezielten Förderung originär anonymer und pseudonymer Datenbestände, bei denen Persönlichkeitsrechte in **stärkerem Maße geschützt** sind als bei einer bloßen Anonymisierung und Pseudonymisierung.
- Es bedarf eines Regelwerks, das die Identifikation pseudonymer und anonymer Nutzer verbietet. Ausnahmetatbestände müssen sorgsam formuliert werden, für Verstöße gegen das Identifikationsverbot müssen **empfindliche Sanktionen** gelten.
- Eine intransparente Sammlung von Informationen über die eigene Person wird mit einem „Gefühl des ständigen Überwachtwerdens" als „diffuse Bedrohlichkeit" wahrgenommen. Um diesem „Gefühl" entgegenzuwirken, bedarf es der **Transparenz** und einer Verpflichtung des Datenverarbeiters, den Nutzer umfassend über Datenverarbeitungsprozesse zu informieren.

a) Originäre Anonymität und Pseudonymität

Die originäre Pseudonymität bzw. Anonymität schützt Persönlichkeitsrechte wesentlich stärker, als dies bei einer Pseudonymisierung bzw. Anonymisierung der Fall ist. Wer den Chatnamen „Sweet 26" nutzt, hat 95

1 Härting/Schneider, ZRP 2011, 233, 235.
2 Tene/Polonetsky, Big Data for All: Privacy and User Control in the Age of Analytics, 11 Nw. J. Tech. & Intell. Prop. 239 (2013), 271, http://scholarlycommons.law.northwestern.edu/njtip/vol11/iss5/1.

es selbst in der Hand, ob und in welchem Umfang er bei der Nutzung des Dienstes Informationen preisgibt, die Rückschlüsse auf die eigene Person zulassen. Werden dagegen bei einem Dienst „Klarnamen" erfasst und die Datenbestände sodann durch einen Vorgang des „Ersetzens" pseudonymisiert, kann der Schleier des Pseudonyms stets gelüftet werden durch einen **inversen Ersetzungsvorgang**. Der Nutzer, der möglichst wenig über sich preisgeben möchte, hat keine Kontrolle über ein inverses „Ersetzen". Er ist darauf angewiesen, darauf zu vertrauen, dass dies nicht geschieht.

b) Verbot der Identifizierung

96 § 15 Abs. 3 Satz 3 TMG ist die einzige Norm des Datenschutzrechts, die es einem Datenverarbeiter ausdrücklich verbietet, die Person zu identifizieren, auf die sich pseudonyme bzw. anonyme Daten beziehen. Dies ist nicht weiter verwunderlich, da sich das Datenschutzrecht auf das **Verbotsprinzip** verlässt (§ 4 BDSG).

97 Verbote der Identifizierung sind notwendig, da der Betroffene bei der Verarbeitung pseudonymer und anonymer Daten typischerweise in erheblichem Maße darauf vertraut, dass er nicht identifiziert wird. Wer würde noch unbefangen Suchbegriffe bei Google eingeben, wenn er wüsste, dass die Begriffe bei Google von einem Mitarbeiter gelesen werden, der den Namen und die Anschrift des Nutzers kennt?

98 **Vertrauen** ist gerade bei der Netzkommunikation ein hohes Gut, so dass es umfassender Verbote der Identifizierung und empfindlicher Sanktionen bedarf, um das Vertrauen der Nutzer angemessen zu schützen.

c) Transparenz

99 In vielen Bereichen des Verbraucherschutzes setzt der Gesetzgeber auf Informationen. Das Datenschutzrecht hinkt dieser Entwicklung hinterher.

100 Transparenz führt zu einer Verstärkung der Selbstbestimmung auf Seiten des Nutzers[1]. Zugleich wird das Vertrauen in Kommunikationsdienste und damit in eine Infrastruktur gestärkt, die für den freien Informationsaustausch und die **freie Entfaltung der Persönlichkeit** in der Informationsgesellschaft einen hohen Stellenwert hat. Es geht nicht nur um die individuelle Grundrechtsausübung, sondern auch um eine **Stärkung der Verlässlichkeit** und Durchschaubarkeit von Kommunikationsinfrastruktur[2].

1 Vgl. Wieczorek, DuD 2011, 476, 480.
2 Vgl. Hoffmann-Riem, AöR 2009, 513, 527.

Anhang
Rechtsprechungsübersicht[1]

A. Persönlichkeitsrechte

EGMR vom 10.1.2013

36769/08

Es gibt eine Wechselwirkung zwischen dem Urheberrecht und der Meinungsfreiheit. Die Ausnahmen, in denen die Meinungsfreiheit eingeschränkt werden darf, sind restriktiv anzuwenden. Das Recht der Meinungsfreiheit ist eine der wesentlichen Grundlagen einer demokratischen Gesellschaft sowie eine der wichtigsten Bedingungen der Entwicklung und Entfaltung des Einzelnen.

(Wechselwirkung; Meinungsfreiheit)

BVerfG vom 17.9.2012

1 BvR 2979/10

Die Bezeichnung Dritter als „rechtsradikal" kann eine zulässige Meinungsäußerung sein. Insbesondere handelt es sich dabei nicht um eine unzulässige Schmähkritik.

(Meinungsäußerung; Schmähkritik)

BVerfG vom 29.2.2012

1 BvR 2883/11

Befindet sich jemand im so genannten „Kampf ums Recht" (hier: Versuch, die Verwaltungsbehörde zur Einstellung eines Bußgeldverfahrens zu bewegen), ist es ihm zur plastischen Darstellung seiner Position grundsätzlich erlaubt, starke und eindringliche Ausdrücke zu benutzen, um seine Rechtsposition zu unterstreichen, ohne jedes Wort auf die Waagschale legen zu müssen.

(Wortwahl beim „Kampf ums Recht")

BVerfG vom 25.1.2012

1 BvR 2499/09, 1 BvR 2503/09

Bei Tatsachenberichten hängt die Abwägung zwischen den widerstreitenden Interessen u.a. vom Wahrheitsgehalt ab, und wahre Aussagen müssen in der Regel hingenommen werden, auch wenn sie nachteilig für den Betroffenen sind. Für die Abwägung ist auch relevant, ob sich die Berichterstattung auf Jugendliche bezieht. Es besteht jedoch keine Regelvermutung dahingehend, dass aufgrund der gesetzgeberischen Wertung im JGG jedes Informationsinteresse hinter dem Anonymitäts-

1 Die Übersicht erstreckt sich auf sämtliche Kapitel des Buchs und enthält die gerichtlichen Entscheidungen, auf die sich die einzelnen Kapitel beziehen. Wegen der Fülle der Entscheidungen beschränkt sich die Übersicht auf die Rechtsprechung des BGH und der Oberlandesgerichte (seit 2008) sowie auf Entscheidungen des BVerfG und des EuGH.