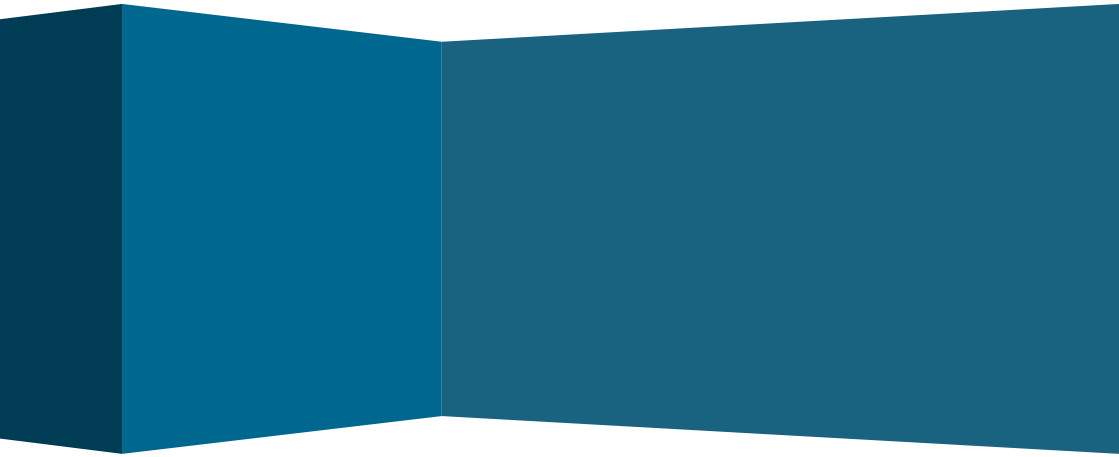
Studie

Johanna Jöns

Daten als Handelsware

DIVSI

www.divsi.de



Johanna Jöns

Daten als Handelsware

DIVSI

Impressum

Deutsches Institut für Vertrauen und Sicherheit im Internet (DIVSI)
Mittelweg 110B, 20149 Hamburg
Matthias Kammer, Direktor
Afia Asafu-Adjei, Projektleitung

Lorenz-von-Stein-Institut für Verwaltungswissenschaften
Olshausenstraße 75, 24118 Kiel
Prof. Dr. Utz Schliesky, geschäftsführender Vorstand
Johanna Jöns, Autorin

© 2016 Deutsches Institut für Vertrauen und Sicherheit im Internet (DIVSI)

Inhalt

Vorwort

© Klaus Knuffmann

Der „Digitale Wandel", der mit vehementer Geschwindigkeit über unsere Gesellschaft gekommen ist, erstreckt sich mittlerweile auf sämtliche Lebensbereiche. Diese Entwicklung bringt zwangsläufig einen massiven Anstieg der Menge an digitalen Daten mit sich, von denen große Teile personenbezogen sind. Nutzer geben ihre Daten hin, um digitale Angebote verwenden zu können. Parallel dazu haben sich prosperierende Märkte entwickelt, bei denen diese Daten der neue Rohstoff sind. Mit den Daten werden gute Geschäfte gemacht.

Es ist ein anerkannter Fakt, dass die aktuelle Datenwirtschaft unser derzeitiges Daten(schutz)recht vor immense Herausforderungen stellt. Fakt ist ebenfalls, dass vor allem ideelle Interessen der einzelnen Nutzer im Fokus der geltenden rechtlichen Regelungen stehen.

Gleichzeitig sind viele Punkte offen. So stellt sich im Zusammenhang mit Big-Data-Analysen immer drängender die Frage, wem Daten „gehören" und wer welche Rechte an Daten geltend machen kann.

Deshalb braucht es zur Förderung der Wirtschaft und zur Fortentwicklung von Nutzerrechten in der digitalen Zeit im Sinne einer erstrebenswerten Rechtsklarheit eindeutige Regelungen über Nutzungs- und Verwertungsrechte an (personenbezogenen) Daten. Derzeit scheint der Datenhandel ein Bereich zu sein, der durch ein erhebliches Machtungleichgewicht zwischen den Beteiligten sowie Intransparenz gekennzeichnet ist.

Die vorliegende Arbeit kommt nach ihrer ebenso sorgfältigen wie umfangreichen wissenschaftlichen Recherche zu dem Schluss, dass das derzeitige Datenschutzrecht den aktuellen Entwicklungen der Datenwirtschaft nicht mehr gerecht werde. Sie hält die datenschutzrechtliche Einwilligung für ein ungeeignetes Instrument zur Realisierung des Datenhandels. Nutzer sollten über eine Kommerzialisierung der auf sie bezogenen Daten entscheiden können. Gleichzeitig sollten sie an der wirtschaftlichen Verwertung „ihrer" Daten partizipieren können.

Die Schrift bietet einen umfassenden Überblick über rechtliche und tatsächliche Konzepte zur Stärkung der Nutzer-Selbstbestimmung im Zusammenhang mit der wirtschaftlichen Verwertung von Daten im Zeitalter der Digitalisierung. Vor- und Nachteile eines Dateneigentums sowie eine mögliche Einordnung von Daten als Immaterialgut werden präzise aufgezeigt.

Damit leistet die Arbeit einen wesentlichen Beitrag, der jeder Untersuchung zu strittigen Themen innewohnen sollte: Sie liefert neue Fakten und Anregungen für einen breiten öffentlichen Disput zum fraglichen Themenkomplex. Sie ergänzt eine mittlerweile lange Reihe von Publikationen des DIVSI, die den gesamten Diskurs unserer Gesellschaft über den stattfindenden digitalen Wandel profund befruchten.

Bundespräsident a.D.
Prof. Dr. Roman Herzog
Schirmherr des DIVSI

A. Zusammenfassung

Mittlerweile haben sich Daten längst zu einem wichtigen Rohstoff und Produktionsfaktor entwickelt – der wirtschaftliche Wert von Daten ist unbestreitbar. Vorrangig bei der Nutzung des Internets fallen enorme Datenmengen an, und es existieren mannigfache Geschäftsmodelle basierend auf Datenerhebung, Datenverarbeitung und dem sich anschließenden Handel mit den Daten selbst oder den Analyseergebnissen. Seit der Schaffung des Rechts auf informationelle Selbstbestimmung hat sich die Art der Daten und der Datenerhebung aufgrund der technischen Neuerungen – insbesondere dem Internet der Dinge – grundlegend verändert. Besonders auffällig ist, dass mit der Zunahme der Datenerhebung aufgrund neuer Methoden und sinkender Speicherkosten auch stetig triviale Daten an Bedeutung gewinnen.

Die Informations- und Kommunikationstechnik ist heute von enormer Bedeutung für die Wettbewerbsfähigkeit jeder Industrienation. Datenschutzbestimmungen sind mittlerweile zu einem Wettbewerbsfaktor geworden, und die Diversität nationaler Regelungen führt zu Standortunterschieden. Viele Unternehmen haben ein Interesse an international vereinheitlichten Datenschutzbestimmungen, die dem Datenverarbeiter Rechtssicherheit bringen und für gleiche ökonomische Bedingungen sorgen. Ein Rechtsrahmen, der einerseits die Privatsphäre des Bürgers schützt und auf der anderen Seite genug Raum für datenbasierte Innovation zulässt, könnte zum europäischen Exportschlager werden.

Dennoch findet der wirtschaftliche Wert von Daten bislang in rechtlicher Hinsicht kaum Berücksichtigung. Im Zusammenhang mit der Datenverarbeitung stehen vorwiegend ideelle Interessen im Vordergrund rechtlicher Regelungen. So dient auch das Bundesdatenschutzgesetz ausweislich dem Schutz der freien Entfaltung der Persönlichkeit, und die datenschutzrechtliche Einwilligung wurde als reines Rechtfertigungsinstrument für eine den Schutzbereich des informationellen Selbstbestimmungsrechts tangierende Datenverarbeitung konzipiert. Jedoch wird von Seiten der Unternehmen zunehmend der wirtschaftliche Wert von personenbezogenen Daten mithilfe des Instruments der Einwilligung ausgeschöpft. Tatsächlich ist die Einwilligung jedoch ungeeignet, ein faktisch bestehendes Austauschverhältnis bei

dem Anbieten eines (vermeintlich kostenlosen) Dienstes im Gegenzug für die Einwilligung in die Datennutzung zu erfassen.

Daher stellt sich mit der zunehmenden Kommerzialisierung die Frage nach dem Reformbedarf des Datenschutzrechts. Sowohl das Rechtsinstitut der datenschutzrechtlichen Einwilligung als auch die Datenschutzprinzipien sind in vielen Bereichen nicht geeignet, den gewandelten Umgang mit personenbezogenen Daten rechtlich zu erfassen. Auch diverse Schutzmechanismen haben sich als wirkungslos herausgestellt – allen voran das Prinzip der Freiwilligkeit und Informiertheit bei Abgabe der datenschutzrechtlichen Einwilligung. Die gesetzlichen Schutzmechanismen des BDSG sind in vielen Fällen ineffektiv, werden umgangen oder lassen sich schlicht nicht kontrollieren.

Dabei muss der Einzelne als selbstbestimmtes Individuum entscheiden können, ab welchem Umfang eine Veröffentlichung und Verbreitung der auf ihn bezogenen Daten das ihm zuträgliche Maß überschreitet. Auch im Zusammenhang mit der Kommerzialisierung von Daten sollte die Herstellung von Nutzer-Selbstbestimmung stets oberstes Ziel sein. Dafür bedarf es Transparenz – allerdings erweist sich die Umsetzung von Informationspflichten in der Realität als unzureichend. Es gibt zu ausführliche und zu knappe, versteckte, unübersichtliche und überflüssige Einwilligungserklärungen. Dies führt dazu, dass überforderte Betroffene ihre Einwilligung erteilen, ohne den angebotenen Text zur Kenntnis zu nehmen. Häufig wird eine Überwindung der Nutzer-Selbstbestimmung angestrebt, und es erfolgt eine (emotionale) Beeinflussung zur Abgabe der Einwilligungserklärung und in der Folge zum Kauf gewisser Produkte oder zur Vornahme anderer von Unternehmen gewünschter Verhaltensweisen. Jedoch kann bei Intransparenz und dem Fehlen einer willentlichen Entscheidung in Kenntnis aller Konsequenzen nicht von einem „Bezahlen" mit den eigenen Daten gesprochen werden. Sind die Daten erst einmal in den Besitz von Unternehmen gelangt, können diese faktisch in zahlreichen Fällen mit ihrem Datenbestand nach Belieben verfahren. Zum einen gibt es zu wenig Kontrolle durch staatliche Aufsichtsbehörden und durch die Betroffenen selbst, zum anderen existieren zu viele rechtliche Grauzonen durch die Konturlosigkeit und Unbestimmtheit des Datenschutzrechts.

Im Zusammenhang mit der wirtschaftlichen Verwertung von Daten ist teilweise unklar, wem in welchem Umfang positive Verwertungsrechte zustehen. Grundsätzlich ist es notwendig, dies im Interesse der Rechtssicherheit und Bestimmtheit eindeutig zu regeln. Da sowohl das Urheberrecht als auch das Datenschutzrecht von ideellen und materiellen Interessen geprägt sind, lassen sich einige grundlegende Wertungen des Urheberrechts auf den Umgang mit personenbezogenen Daten übertragen. Insbesondere das Modell der Einräumung von Nutzungslizenzen mit dinglicher Wirkung wird schon lange auch für den Bereich der Datenwirtschaft befürwortet. Mit der dinglichen Wirkung ergäben sich die Vorteile einer gesicherten Rechtsposition auch gegenüber Dritten, und es entstünde eine Möglichkeit der Weiterübertragung von Rechten an Daten. Ferner bietet eine vertragliche Ausgestaltung die Vorzüge, dass der Umfang des Nutzungsrechts bzw. die erlaubten Nutzungsarten und die Gegenleistung konkret bestimmt werden müssen. Ferner ließe sich eine zeitliche Geltungsdauer vereinbaren, und zur Ausübung der Rechte könnten diese auf einen Datentreuhänder bzw. auf Wahrnehmungsgesellschaften übertragen werden.

In der Tat geht es bei der Zuordnung der Verfügungsbefugnis über personenbezogene Daten zu der betroffenen Person auch darum, die marktmäßige Nutzung effektiv zu steuern. Mit der Analogie zum Urheberrecht könnte der (kontrollierte) Datenhandel leichter realisiert, nach den Interessen aller Beteiligten gestaltet und in beherrschbare Bahnen gelenkt werden. Das Recht des Betroffenen kann freilich nicht uneingeschränkt bestehen. Im BDSG gibt es diverse Erlaubnistatbestände für eine Datenverarbeitung – solche Regelungen müssten bei einer Neugestaltung nach dem Vorbild des Urheberrechts fortbestehen.

Die Vorteile gegenüber einem Dateneigentum liegen darin, dass die Verknüpfung von materiellen und ideellen Interessen besser erfasst wird und keine vollständige Aufgabe der eigenen Rechtsposition durch den Betroffenen möglich ist. Aufgrund der hohen Schutzgüter der uneinschränkbaren Menschenwürde und des allgemeinen Persönlichkeitsrechts dürfen nicht allein die vermögensrechtlichen Interessen im Vordergrund stehen, wie es bei dem Dateneigentum der Fall wäre.

Um die Selbstbestimmung der Nutzer effektiv sicherzustellen, bedarf es praxistauglicher Mechanismen. Hierbei steht insbesondere die Herstellung von Transparenz im Vordergrund, denn diese ist bei stärkerer Selbstbestimmung der betroffenen Parteien hinsichtlich der Ausgestaltung des Datenverarbeitungsverhältnisses essenziell. Es gibt bereits diverse Ansätze wie die Einführung eines Datenschutzbriefs oder eines Bürgerkontos. Hauptproblem ist, dass im Bereich der digitalen Datenwirtschaft die Politik und der Gesetzgeber nicht angemessen auf seit Langem bekannte Entwicklungen reagieren. Es wird Zeit, dass rechtliche und praktische Konzepte zur Entwicklung von Daten zu einer Handelsware mit dem Ziel der rechtlichen Erfassung des Datenhandels sowie der Förderung der Nutzer-Selbstbestimmung umgesetzt werden.

Im Endeffekt benötigen wir einerseits eine Lockerung des Datenschutzrechts dergestalt, dass nicht jede Datenverarbeitung als unerwünscht betrachtet wird und auch ökonomische Interessen Berücksichtigung finden; andererseits eine Verschärfung dahingehend, dass es dem Einzelnen erleichtert wird, seine ideellen Interessen zu schützen.

Zusammenfassend ergeben sich die folgenden Thesen:

- Das Instrument der datenschutzrechtlichen Einwilligung ist in der Praxis gescheitert und weist dogmatische Unzulänglichkeiten auf. Insbesondere ist sie aufgrund ihrer ursprünglichen Konzeption als reines Rechtfertigungselement nicht geeignet, ein Austauschverhältnis rechtlich zu erfassen.
- Auch der wirtschaftliche Wert von Daten sollte in rechtlicher Hinsicht Berücksichtigung finden. Bislang sind im Zusammenhang mit der Datenverarbeitung vorwiegend ideelle Interessen der Betroffenen Anknüpfungspunkt für rechtliche Regelungen.
- Zu begrüßen wäre eine eindeutige rechtliche Zuordnung von Daten bzw. klare Regelungen über Nutzungs- und Verwertungsrechte – dies gilt sowohl für personenbezogene als auch für nicht personenbezogene Daten.
- Zur Stärkung der Selbstbestimmung der Betroffenen bietet sich die Schaffung eines Regelungsregimes in Anlehnung an das Urheberrecht an, da hier ideelle und materielle Aspekte gelungen miteinander verknüpft sind.

- Mittels der Einräumung von Nutzungslizenzen ließe sich der (kontrollierte) Datenhandel leichter realisieren, nach den Interessen aller Beteiligten gestalten und in beherrschbare Bahnen lenken.
- Wenn die Regelung des Datenverarbeitungsverhältnisses stärker den beteiligten Parteien überlassen wird, muss eine hohe Transparenz der Datenverarbeitung gegenüber den Betroffenen bestehen.

B. Einführung

Das wirtschaftliche Potenzial personenbezogener Daten ist enorm. Dies haben auch Unternehmen längst erkannt und lassen sich vielfach für die Nutzung ihrer vermeintlich kostenlosen Webanwendungen weitreichende Einverständniserklärungen zur Datenverwertung einräumen. Man könnte sagen, dass hier ein Dienst gegen Daten anstatt gegen Geld eingetauscht wird. Aus juristischer Sicht wird jedoch dieses tatsächlich bestehende Austauschverhältnis nicht als gegenseitiger Vertrag begriffen, sondern immer noch von zwei getrennten Vorgängen ausgegangen: zum einen dem Anbieten eines (vermeintlich kostenlosen) Dienstes, zum anderen der Einwilligung in die Datennutzung, ohne dass dabei beide Vorgänge in einem Abhängigkeitsverhältnis stehen.

Würde man jedoch das Verständnis von Daten als Gegenleistung für IT-Leistungen stärken, könnte durch individuelle vertragliche Gestaltungen die Partizipation des Einzelnen an der wirtschaftlichen Verwertung seiner Daten zunehmen. Rechtlich wäre die Konzeption eines „Herrschaftsrechts" des Einzelnen an seinen Daten, über das er in gewissem Umfang verfügen kann, zu begrüßen. Personenbezogene Daten stehen mehr denn je im Spannungsverhältnis zwischen Persönlichkeitsrechten und wirtschaftlichen Nutzungs- bzw. Verwertungsrechten. Dieses Spannungsverhältnis gilt es juristisch zu erfassen und geeignete Modelle für die Lebenswirklichkeit zu entwickeln.

Diese Untersuchung soll die aktuellen Problematiken des Datenhandels aufzeigen. Dafür wird zunächst auf die wachsende Bedeutung von (personenbezogenen) Daten eingegangen (C.). Anschließend sollen die rechtlichen Herausforderungen des Datenhandels dargestellt werden (D.), um den Reformbedarf des Datenschutzrechts herauszufiltern (E.). Danach werden einige aktuelle Ansätze zur Stärkung der Nutzer-Selbstbestimmung untersucht (F.). Schließlich werden Gedanken zu einer möglichen Neugestaltung des Datenschutzrechts mit dem Ziel der Stärkung der Selbstbestimmtheit der Betroffenen durch die Schaffung eines wirtschaftlichen Verwertungsrechts an den eigenen personenbezogenen Daten entwickelt (G.).

Im Vordergrund der Betrachtung stehen hierbei die juristischen Aspekte; auf die wirtschaftliche und politische Dimension des Datenhandels soll dagegen nicht umfassend eingegangen werden.

C. Wachsende Bedeutung (personenbezogener) Daten

I. Der Datenhandel

In der heutigen globalisierten Informations- und Wissensgesellschaft haben sich Daten längst zu einem wichtigen Rohstoff und Produktionsfaktor entwickelt – der wirtschaftliche Wert von Daten ist unbestreitbar. Es wird geschätzt, dass der Wert von Daten bis 2020 auf bis zu 8 % des Bruttoinlandsprodukts der 27 EU-Staaten ansteigen wird[1]. Vorrangig bei der Nutzung des Internets fallen enorme Datenmengen an, und es existieren mannigfache Geschäftsmodelle basierend auf Datenerhebung, Datenverarbeitung und dem sich anschließenden Handel mit den Daten selbst oder den Analyseergebnissen. Die vermeintliche Kostenlosigkeit zahlreicher Webdienste und Webanwendungen muss der Nutzer mit der Hingabe seiner personenbezogenen Daten finanzieren. Die wirtschaftlichen Akteure profitieren dabei von einem geänderten Nutzerverhalten im Netz, welches das Hinterlassen einer immer umfassenderen „Datenspur" mit sich bringt. Während ursprünglich im Internet vorwiegend Informationen abgerufen wurden, werden zunehmend selbst Inhalte produziert. Es werden persönliche Bilder, selbst gedrehte Videos online gestellt; Kommentare in diversen Foren und Blogs hinterlassen; oder es wird gemeinschaftlich an Wikis gearbeitet. So verdoppelt sich das Datenvolumen Studien zufolge – auch aufgrund der stetig sinkenden Kosten für Speichermedien – ca. alle zwei Jahre. Im Jahr 2013 gab es weltweit schätzungsweise 4,4 Zettabytes (entspricht 4.400.000.000.000.000.000.000 Bytes) an Daten[2].

Der Modebegriff „Big Data" umschreibt das Analysieren dieser immensen, diversifizierten Datenvolumina mittels Algorithmen, um effizientere unternehmerische Entscheidungen zu ermöglichen. Es bedeutet, die Daten

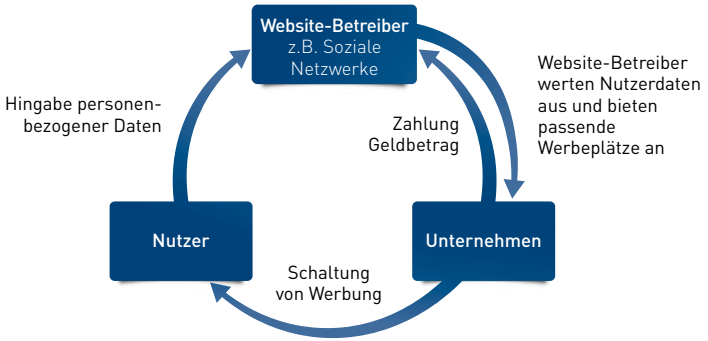
1 The Boston Consulting Group, The Value of Our Digital Identity, 2001, S. 101, abrufbar unter: http://www.libertyglobal.com/PDF/public-policy/The-Value-of-Our-Digital-Identity.pdf.

2 IDC-Studie Data Growth, Business Opportunities, and the IT Imperatives, abrufbar unter: http://germany.emc.com/leadership/digital-universe/2014iview/executive-summary.htm.

nicht nur zu erheben und zu speichern, sondern in eine maschinenlesbare Form zu überführen, Zusammenhänge zu erkennen und richtige Prognosen zu erstellen[3]. Es lassen sich aus einem riesigen Datenpool quasi in Echtzeit nach unterschiedlichen Suchschlüsseln Listen zusammenstellen und somit gezielt Informationen herausfiltern. Gerade die Verknüpfung diverser Daten und Datenbestände miteinander bietet großes Gefährdungspotenzial für die Privatheit des Einzelnen.

Doch auch die Chancen der Datenverarbeitung für gesamtgesellschaftliche Entwicklungen sowie für den ökonomischen Bereich dürfen nicht verkannt werden. Momentan ist der größte Nutzen der Datenverarbeitung aus Sicht von Unternehmen noch in der Schaltung personalisierter Werbung[4] und der Marktforschung zur Entwicklung neuer Produkte und Dienstleistungen[5] zu sehen. Gerade im Bereich der Werbung wird allerdings nicht mit den Daten selbst gehandelt, sondern ein Website-Betreiber wird umso attraktiver für einen Werbekunden, je mehr detaillierte Nutzerprofile er vorweisen kann. Die Daten werden also nur von demjenigen ausgewertet, dem sie auch überlassen werden; der wirtschaftliche Wert der Datenerhebung resultiert jedoch daher, dass die Analyseergebnisse Dritten nutzbar gemacht werden.

Dieses Drei-Personen-Verhältnis veranschaulicht folgende Abbildung:



3 https://www.bitkom.org/Bitkom/Publikationen/Big-Data-und-Geschaeftsmodell-Innovationen-in-der-Praxis-40-Beispiele.html.

4 Facebook hat beispielsweise im Jahr 2014 11,49 Mrd. USD Werbeumsatz erzielt (Quelle: http://www.vzbv.de/pressemitteilung/facebook-fuehrt-nutzer-die-irre).

5 Reiners, ZD 2015, 51 (52).

In vielen Bereichen wird der Nutzer zum Gegenstand der kommerziellen Interessen, ohne sich dessen stets bewusst zu sein und ohne an den Gewinnen beteiligt zu werden. Durch neue Geschäftsmodelle und aufgrund ihres Umfangs wird die Datenerhebung jedoch auch für den Nutzer vermehrt sichtbar, und das Bewusstsein für die zunehmende eigene Transparenz und Manipulierbarkeit und den Verlust der Datenhoheit steigt. Alexander Pentland hält es aufgrund des Sozialbezugs des Menschen für möglich, das Verhalten jedes Individuums durch die neuen technischen Möglichkeiten zu beeinflussen[6]. Diese These untermauert auch eine Studie von Facebook, bei der Nutzern ein vorgefilterter Nachrichtenstrom angezeigt wurde und diese Einflussnahme sich auch auf die selbst produzierten Einträge der Betroffenen auswirkte[7]. Die Ablehnung gegenüber der massenhaften Erhebung von Daten wächst; Nutzer fühlen sich aufgrund ihres mangelnden Einflusses zum Objekt der Datenverarbeitung degradiert[8]. Mit der Produktion von Daten werden wirtschaftliche Werte geschaffen, und die Datenerzeuger werden in Zukunft vermutlich vermehrt an den erzielten Gewinnen partizipieren wollen[9].

II. Aktuelle Entwicklungen im Bereich der modernen Datenverarbeitung

1. Internet der Dinge

Internet der Dinge bezeichnet den Umstand, dass immer mehr Alltagsgegenstände digitalisiert werden, indem kleine, eingebettete Computer unauffällig im Hintergrund arbeiten und sämtliche Lebensbereiche von datenverarbeitenden Prozessen geprägt sind. Bereits 1991 führte Mark Weiser seine Vision, dass die reale Welt von einer allgegenwärtigen Virtualität durchzogen sein wird bzw. dass sich Computer nahtlos in die reale Welt integrieren lassen, in seinem Aufsatz „The Computer for the 21st Century" näher aus.

6 Carr, The Limits of Social Engineering, abrufbar unter: http://www.technologyreview.com/review/526561/the-limits-of-social-engineering/.

7 http://www.zeit.de/digital/internet/2014-06/facebook-nutzer-manipulation-studie.

8 DIVSI-Studie, Daten – Ware und Währung, 2014, S. 13.

9 Reiners, ZD 2015, 51 (55).

Indem unser Körper, unser Verhalten, der Zustand unserer Geräte und unsere Umwelt stets vermessen werden, wird die Informationslücke zwischen der realen und der virtuellen Welt minimiert. Der Personal Computer wird durch diverse „intelligente" Gegenstände ersetzt, welche den Menschen unauffällig und ohne abzulenken in seinem Alltag unterstützen. Moderne Technologien wie die Standortermittlung, Sensorik, biometrische Erkennungsverfahren, neue Telekommunikationsmöglichkeiten, diverse Möglichkeiten zur Analyse des Webnutzungsverhaltens sowie die Verringerung des Energieverbrauchs und sinkende Speicherkosten haben die Art und den Umfang der Datenerhebung nachhaltig verändert.

2. RFID

Als Anfang des Internets der Dinge wird die Entwicklung der RFID-Technologie (Identifikation durch Radiofunktechnik, Radio Frequency Identification) genannt. Durch die Ausstattung mit einem Mikrochip, auch Transponder genannt, werden Gegenstände zu einem Datenträger. Mittels eines Lesegeräts sind die gespeicherten Daten dezentral und berührungslos jederzeit auslesbar. Die Vorteile dieser Technologie liegen in der geringen Größe des Transponders und der unauffälligen Auslesemöglichkeit; die Anwendungsfelder sind vielfältig und reichen von Mautsystemen und Warensicherungssystemen hin zu elektronischen Schlössern und kontaktlosem, bargeldlosem Zahlen. Auch der elektronische Personalausweis enthält einen RFID-Chip, auf dem die Daten digital abgespeichert sind.

Mit dem Schlagwort „Industrie 4.0" wird die Erwartung einer vierten industriellen Revolution durch den Einzug der RFID-Technologie in die Produktion und die damit verbundene Vernetzung von Produktionsprozessen und Entwicklung komplexer Fertigungsmaschinen bezeichnet[10]. Die Ausstattung von Waren mit Smart Tags[11] bietet die Chance, die Produktionsprozesse, die Lagerung, die Wartung und die Reparatur effizienter zu gestalten. Die Vorteile von „intelligenteren" Produkten sind vielfältig: Waren können

10 http://www.bmwi.de/DE/Themen/Industrie/Industriepolitik/moderne-industriepolitik.html; http://www.bmwi.de/DE/Themen/Industrie/industrie-4-0.html.

11 Auf Nahfunk basierende Minichips.

sich jederzeit exakt orten lassen; sie können in der Logistik selbstständig ihre Verteilung organisieren; selbst Informationen über Fertigungsprozesse enthalten; Auskunft darüber geben, wie lange ihre Garantie noch gilt; ihre Kühlung überwachen; den Endverbrauchern mehr Transparenz z. B. über Gütesiegel bieten; den Kundenservice z. B. durch Wartungen aus der Ferne erleichtern. Als entscheidender Vorteil wird auch eine stärker nachfrageorientierte Produktion, insbesondere die Fertigung individueller Waren, gesehen.

Doch nicht nur die Industrie wird digitalisiert, sondern wir stehen am Anfang einer umfassenden digitalen Revolution. Der Einbau von Technologie macht selbst beim menschlichen Körper nicht halt. Aufsehenerregend ist, dass sich Menschen bereits reiskorngroße RFID-Chips transplantieren lassen, um im Alltag und Geschäftsleben zahlreiche Annehmlichkeiten in Anspruch nehmen zu können. In Schweden haben sich schon über 300 Menschen einen Chip unter die Haut setzen lassen, der diverse Funktionen für sie übernimmt. Sobald die Hand in die Nähe eines geeigneten Lesegeräts gelangt, ist die entsprechende Person identifiziert. Es gibt bereits einige Bürogebäude, Fitnessstudios und Cafeterien, die mit der Nahfeldkommunikationstechnik arbeiten. Die Nutzer betonen den Komfort im Alltag dadurch, dass sich mittels des Chips automatisch Türen öffnen, Handys entsperren oder Kopierer nutzen lassen. Zudem kann der Chip Kundenkarten ersetzen, als Zahlungsmethode fungieren und diverse andere Aufgaben übernehmen. Problematisch kann der Verlust der Informationshoheit aufgrund der leichten Zugriffsmöglichkeit auf diese Daten sein – unter Umständen ohne dass der Chipträger Kenntnis davon hat. Beispielsweise könnte eine Datenübertragung in Zukunft unbemerkt beim Händeschütteln erfolgen[12].

Wie anfällig digitale Systeme für Datenklau sind, zeigte auch ein Versuch am Hamburger Flughafen. Hacker waren in der Lage, Sicherheitsausweise des Flughafenpersonals mittels eines nachgebauten Lesegeräts heimlich per Funk zu kopieren und sich damit Zugang zu sicherheitsrelevanten

12 Astheimer/Balzter, Schwedische Arbeitnehmer lassen sich Chip implantieren – freiwillig, abrufbar unter: www.faz.net/aktuell/beruf-chance/arbeitswelt/rfid-chip-bueroangestellte-schweden-13438675.html.

Bereichen zu verschaffen[13]. Mit dem vielfältigen Einsatz von Technologien steigt auch das Missbrauchspotenzial, und es wird vermehrt – auch von Seiten der Nutzer – Wert auf Maßnahmen zur Datensicherheit gelegt. Vermehrte Sicherheitsvorfälle zeigen auf, wie abhängig wir in vielen Bereichen von digitalen Strukturen und Prozessen sind und wie leicht spezialisierte Hacker unsere Systeme angreifen können[14]. Aktuell Schlagzeilen macht der bislang größte Hackerangriff auf den Deutschen Bundestag, bei dem Unbekannte einen Trojaner in Teilstücken an Bundestagsrechner versendeten. Erst nachdem die Angreifer Zugriff auf das Computernetz des Bundestags erlangt hatten, entdeckte das Bundesamt für Verfassungsschutz, dass von Parlamentscomputern aus verdächtige Server angesteuert wurden[15].

Um die Datensicherheit zu erhöhen, hat der Bundestag im Juni 2015 das von der Bundesregierung vorgelegte IT-Sicherheitsgesetz[16] in der durch Anträge von Unions- und SPD-Fraktion geänderten Fassung[17] beschlossen, welches Betreiber von kritischen Infrastrukturen zur Einhaltung eines gewissen Mindestniveaus an IT-Sicherheit verpflichtet sowie eine Meldepflicht bei einem Sicherheitsvorfall an das Bundesamt für Sicherheit in der Informationstechnik (BSI) statuiert. Als Reaktion auf die Datenpanne im Bundestag wurde die Meldepflicht des IT-Sicherheitsgesetzes auf die Bundesverwaltung ausgeweitet. Der BITKOM begrüßt diese Änderung, da auch

13 Deiß, Datenklau per Funk – Sicherheitsrisiko an deutschen Flughäfen, abrufbar unter: www.rbb-online.de/kontraste/ueber_den_tag_hinaus/terrorismus/datenklau_per_funk.html.

14 http://www.welt.de/wirtschaft/webwelt/article126583693/Datenklau-Opfer-muessen-noch-ein-paar-Tage-bangen.html; http://www.welt.de/wirtschaft/webwelt/article134981981/Hacker-erbeuten-unveroeffentlichte-Sony-Filme.html; Pisacane, Firmen unterschätzen Datenklau, abrufbar unter: http://www.handelsblatt.com/unternehmen/management/mittelstaendler-besonders-sorglos-firmen-unterschaetzen-datenklau/2806634.html; http://www.spiegel.de/netzwelt/netzpolitik/us-krankenhaeuser-hacker-stehlen-daten-von-4-5-millionen-patienten-a-986804.html.

15 http://www.tagesschau.de/inland/bundestag-hacker-angriff-101.html.

16 Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme, BT-Drs. 18/4096, abrufbar unter: http://dip21.bundestag.de/dip21/btd/18/040/1804096.pdf.

17 BT-Drs. 18/5121, abrufbar unter: http://dip21.bundestag.de/dip21/btd/18/051/1805121.pdf.

Einrichtungen der Regierung und der Verwaltung per definitionem kritische Infrastrukturen darstellen würden[18].

3. Ubiquitous Computing

Durch Ubiquitous Computing[19], also Rechnerallgegenwart bzw. allgegenwärtig verfügbare Rechenleistung, verändern sich zahlreiche Lebensbereiche. Wurden Gegenstände zunächst zu Datenträgern, sind sie nun selbst Datenquelle. Alltagsgegenstände sollen mittels Sensorik, Standortermittlung und Aufzeichnung von Telekommunikationsprozessen Daten erheben und diese mittels einer Internetverbindung weiterleiten. Während der erste wichtige Schritt der Digitalisierung die Vernetzung von Rechnern war, wird nun in einem zweiten Schritt jeder Einzelne mit einer Vielzahl verschiedener Computer und der Allgegenwart der rechnergestützten Informationsverarbeitung konfrontiert.

Ubiquitous Computing ist technisch nur aufgrund des Verzichts von lokalen Rechnern dank der Verarbeitung in entfernten Rechenzentren sowie der Verfügbarkeit von IT-Infrastrukturen über Netzwerke (Cloud Computing) zu realisieren. Durch die Ausstattung mit Sensoren und einer Netzverbindung lässt sich jeder Gegenstand in eine Datenquelle umfunktionieren. Es werden stetig neue Produkte und Dienstleistungen geschaffen, wobei Daten immer mehr zum Gegenstand der Geschäftskonzepte selbst werden und die aufbereiteten Daten zunehmend auch den Nutzern transparent gemacht werden. Durch die Vorteile für die Nutzer könnte die Datenerhebung mehr Akzeptanz erfahren, andererseits werden sich die Nutzer in zunehmendem Maße darüber bewusst, wie umfänglich die Datenerhebung im Alltag tatsächlich ist. Mittlerweile ist es möglich, detaillierte Profile über einen Menschen anzulegen, welche Angaben über Geschlecht, Alter, Adresse, Familienstand, Beruf, Krankheiten, finanzielle Situation, Interessen und häufige Aufenthaltsorte beinhalten können.

---

18 https://www.bitkom.org/Presse/Presseinformation/Bitkom-sieht-Strafen-im-IT-Sicherheitsgesetz-kritisch.html.

19 Zum Begriff siehe Bundesministerium für Bildung und Forschung, Studie „Technikfolgenabschätzung – Ubiquitäres Computing und Informationelle Selbstbestimmung (TAUCIS), 2006, S. 11ff.

Als Beispiel für allgegenwärtiges Rechnen im Alltag lassen sich Fitness-Armbänder anführen, welche Schrittzähler, Pulsmesser und Routenplaner in sich vereinigen und alle Statistiken auch an das Smartphone oder an den Laptop übertragen können. Prominentes Beispiel ist auch die Apple Watch, mit der Nutzer ihren Puls, Bewegungsdaten, verbrannte Kalorien oder den Cholesterinwert aufzeichnen können. Auch die Firma IBM will nun in den Markt mit elektronischen Gesundheitsinformationen einsteigen und die Daten an einen Online-Speicher übermitteln, Analysesoftware entwickeln und die Informationen Ärzten, Forschern und Versicherungsunternehmen zugänglich machen[20].

Hochaktuell sind auch Smart Cars, die Auskunft über Fahrverhalten, Standort und Zustand des Wagens sowie Pannen und Unfälle geben können. Die EU plant verpflichtend für alle Neufahrzeuge die Einführung eines automatischen Notrufsystems (eCall), das bei Verkehrsunfällen einen Notruf absetzt. In die Kritik geraten sind diese Neuerungen wegen der stets aktiven Internetverbindung, aufgrund derer sich umfassende Bewegungs-, Verhaltens- und Persönlichkeitsprofile erstellen lassen. Auch denkt die Versicherungsbranche bereits über individuelle Verträge je nach durch Datenauswertung ermitteltem Fahrverhalten nach[21].

III. Bedeutsamkeit des Personenbezugs

Will man sich mit den rechtlichen Rahmenbedingungen des Datenhandels auseinandersetzen, ist es essenziell, zunächst den Kernbegriff des personenbezogenen Datums näher in den Blick zu nehmen. Da der Datenschutz der freien Entfaltung der durch die Datenverarbeitung betroffenen Person dienen soll, unterliegen lediglich Daten mit einem Personenbezug dem Schutzregime des Bundesdatenschutzgesetzes (BDSG).

Das deutsche Recht definiert in § 3 Abs. 1 BDSG personenbezogene Daten als „Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person". Das europäische

20 http://www.spiegel.de/wirtschaft/unternehmen/apple-healthkit-ibm-will-gesundheitsdaten-auswerten-a-1028426.html.

21 Zur Problematik individueller Krankenversicherungen siehe G. V. 2.

Sekundärrecht definiert in Art. 2 lit. a) DSRL[22] ebenfalls den Begriff der personenbezogenen Daten als „alle Informationen über eine bestimmte oder bestimmbare Person" und konkretisiert die Bestimmbarkeit dahingehend, dass eine Person bestimmbar ist, „die direkt oder indirekt identifiziert werden kann, insbesondere durch Zuordnung zu einer Kennnummer oder zu einem oder mehreren spezifischen Elementen, die Ausdruck ihrer physischen, physiologischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität sind". Im Zweifel muss die nationale Vorschrift richtlinienkonform ausgelegt werden.

Eine Person ist nach gängiger Definition nicht bestimmbar, wenn das Risiko, einen Personenbezug herzustellen, so gering ist, dass es nach der allgemeinen Lebenserfahrung und dem Stand der Technik als irrelevant angesehen wird. Grundsätzlich sind allein die verhältnismäßigen Möglichkeiten der datenverarbeitenden Stelle zur Ermittlung der betreffenden Person maßgeblich. Inwieweit Zusatzwissen Dritter Berücksichtigung finden muss, ist bislang umstritten. In der Tat besteht ein Risiko für den Einzelnen, wenn dessen Daten aus der Sicht einer datenverarbeitenden Stelle keine personenbezogenen Daten darstellen und diese dann in die Hände eines anderen gelangen, der zur Herstellung des Personenbezugs in der Lage ist. Besonders schwierig ist die Einordnung von Daten, welche mit einer dynamischen IP-Adresse in Verbindung stehen und bei denen der Klarname nicht angegeben wurde. Grundsätzlich kann nur der Internet-Service-Provider den Bezug zwischen der Person und der verwendeten dynamischen IP-Adresse herstellen. Für alle anderen datenverarbeitenden Stellen handelt es sich demnach grundsätzlich nicht um personenbezogene Daten. Aufgrund von diversen Techniken zur Nutzerdatenerfassung (Cookies, Clickstream-Analysen, Web-Bugs, Browser-Fingerabdruck) können jedoch Daten von mehreren Sitzungen eines Computers trotz verschiedener IP-Adressen zu einem Nutzerprofil zusammengeführt werden, und je detaillierter die Informationen sind, desto größer ist die Wahrscheinlichkeit der Zuordnung zu der dahinterstehenden Person. Auch durch die Veröffentlichung bzw. Weitergabe

22 RL 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr.

der Daten erhöht sich das Risiko der Aufklärung der Identität des Betroffenen. Im Vordergrund der Diskussion steht daher die Frage, ob es sich nicht bereits zum Schutz des Nutzers auch dann um personenbezogene Daten handeln muss, wenn lediglich Dritte über das nötige Zusatzwissen zur Herstellung eines Personenbezugs verfügen. Diese Frage wird der EuGH im Rahmen eines Vorabentscheidungsverfahrens gemäß Art. 267 AEUV klären müssen[23]. Für die datenverarbeitenden Stellen ist dringend mehr Rechtssicherheit im Umgang mit Daten notwendig, und es muss zur Kenntnis der Rechtsfolgen eindeutig bestimmbar sein, wann es sich um ein personenbezogenes Datum handelt.

Daten mit einem Bezug zu einer Person, bei denen dieser Bezug jedoch von niemandem hergestellt werden kann (zum Beispiel aufgrund einer Anonymisierung[24]), stellen nach der gesetzlichen Definition keine personenbezogenen Daten dar. Problematisch ist, dass die Möglichkeit der Herstellung eines Personenbezugs aufgrund der technischen Innovationen und der Menge an vorhandenen und verknüpfbaren Daten in der Praxis oft nicht gänzlich und für die Zukunft auszuschließen ist. Dammann nennt diese Daten potenziell personenbezogene Daten, da der Zugang nachträglich erleichtert und damit der datenverarbeitenden Stelle unter verhältnismäßigem Aufwand möglich werden kann[25]. Aufgrund der Relativität der Bestimmbarkeit einer Person würde es sich anbieten, alle potenziell personenbezogenen Daten ebenfalls wie personenbezogene Daten zu behandeln und somit einem stärkeren Schutzniveau zu unterstellen. Aktuell stehen personenbezogene und anonyme Daten noch im Gegensatz zueinander; bei einer Gleichbehandlung aller potenziell personenbezogenen Daten würde diese Unterscheidung aufgegeben werden.

23 BGH, Beschl. v. 28.10.2014, VI ZR 135/13.

24 Anonymisieren ist nach § 3 Abs. 6 BDSG „das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können".

25 Dammann, in: Simitis (Hrsg.), Bundesdatenschutzgesetz, § 3, Rn. 36.

D. Rechtliche Herausforderungen für die wirtschaftliche Verwertung von Daten

I. Internationalität des Datenhandels

Mit der umfassenden Vernetzung durch das Internet hat auch der Datenhandel längst nationale Grenzen überwunden. Es existieren zahlreiche global agierende Unternehmen (oft mit US-amerikanischem Hauptsitz), welche im Bereich der Digitalwirtschaft aufgrund ihrer Datensammlung eine Stellung innehaben, die monopolistische Tendenzen aufweist. In einigen Bereichen wie zum Beispiel bei Suchmaschinen[26] oder Nachrichtendiensten[27] hat der Markt allerdings auf natürliche Weise zu einer Monopolbildung geführt, da einige Dienste überzeugen konnten und sich deren Marktmacht aufgrund von Konzentrationseffekten verfestigt hat – insofern kann hier nicht von einem klassischen Marktversagen gesprochen werden. Dennoch werden global agierende Internetunternehmen aus kartellrechtlicher und wettbewerbsrechtlicher Perspektive schon länger kritisch betrachtet. Bei Vorliegen einer marktbeherrschenden Stellung gilt das kartellrechtliche Verbot, diese Stellung zu missbrauchen. Diverse kartellbehördliche Missbrauchsverfahren wurden in den letzten Jahren gegen Internetdienstleister eingeleitet, und die Frage, ob Internetplattformen bzw. Datenbestände wesentliche Einrichtungen (essential facilities) i.S.d. Kartellrechts darstellen, ist noch ungeklärt[28].

Darüber hinaus wurde die Europäische Kommission durch eine nicht bindende Entschließung der EU-Parlamentarier dazu aufgefordert, eine Entflechtung von Suchmaschinen von anderen „kommerziellen Dienstleistungen" in Erwägung zu ziehen, damit die Internetsuche frei von

26 Google hat einen Marktanteil von 94,84 % (Quelle: http://de.statista.com/statistik/daten/studie/167841/umfrage/marktanteile-ausgewaehlter-suchmaschinen-in-deutschland/).

27 WhatsApp hat einen Marktanteil von ca. 39 %, der Messenger-Dienst von Facebook kommt auf ca. 37 % (Quelle: http://de.slideshare.net/globalwebindex/gwi-trends-mobile-messaging-q3-2014).

28 Hauptgutachten XX der Monopolkommission, Kapitel I – Aktuelle Probleme der Wettbewerbspolitik, abrufbar unter: http://www.monopolkommission.de/images/PDF/HG/HG20/1_Kap_1_A_HG20.pdf.

Diskriminierungen bleibe und der Wettbewerb gefördert werde[29]. Auch in einem Strategiepapier der Europäischen Kommission werden Bedenken hinsichtlich der zunehmenden Marktmacht von Online-Plattformen geltend gemacht, insbesondere im Hinblick darauf, dass einzelne Plattformbetreiber den Zugang zu Online-Märkten kontrollieren könnten und Einfluss auf die Entlohnung verschiedener Marktteilnehmer hätten. Weitere Themen der Strategie für einen digitalen Binnenmarkt für Europa als Antwort auf die Ausbreitung der Informations- und Telekommunikationstechnik sind die Modernisierung und Vereinheitlichung des Urheberrechts in der EU, die Verhinderung von ungerechtfertigtem Geoblocking, Interoperabilität sowie der Aufbau einer Datenwirtschaft[30].

1. Gesetzliche Regelungen

Die digitalen Verarbeitungsprozesse werden von Unternehmen mittlerweile weltweit auf Rechenzentren verteilt. Aufgrund dieser Internationalität der Datenverarbeitung und Datenverwertung greifen nationale Regelungen oftmals ins Leere[31]. Daher gibt es in der Europäischen Union seit Längerem Bestrebungen, ein hohes einheitliches Schutzniveau im Bereich des Datenschutzes zu schaffen. Einen ganz wesentlichen Beitrag dazu hat die europäische Datenschutzrichtlinie (DSRL) geleistet, die nun von der Datenschutzgrundverordnung (DSGVO) abgelöst wird. Anders als eine Richtlinie ist eine Verordnung unmittelbar anwendbares Recht, d. h., bei einer Verordnung bedarf es, anders als bei Richtlinien, keiner Umsetzung in nationales Recht, und somit entfällt der Umsetzungsspielraum der Mitgliedstaaten. Mit der DSGVO wird eine umfassende Harmonisierung angestrebt, sodass weder eine Abweichung vom festgelegten Schutzniveau nach unten noch nach

29 Entschließung des Europäischen Parlaments zur Stärkung der Verbraucherrechte im digitalen Binnenmarkt, abrufbar unter: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+MOTION+B8-2014-0286+0+DOC+XML+V0//DE.

30 Strategie für einen digitalen Binnenmarkt für Europa, abrufbar unter: http://ec.europa.eu/priorities/digital-single-market/docs/dsm-communication_de.pdf.

31 Zum staatlichen Schutz vor Eingriffen von fremden Staaten und Privaten vermittelt durch Grundrechte bei internationalen Internetsachverhalten vgl. Schliesky/Hoffmann/Luch/Schulz/Borchers, Schutzpflichten und Drittwirkung im Internet, Baden-Baden 2014, S. 66 ff.

oben hin möglich ist. Ferner sollen entwicklungsoffene Regelungen auch Datenschutz durch Technik unter Berücksichtigung der jeweils aktuellen technischen Standards ermöglichen.

Ebenfalls sinnvoll wäre, über den europäischen Raum hinaus auf Basis völkerrechtlicher Verträge Regelungen über den Datenschutz zu treffen. Seit 1980 gibt es bereits mit den „OECD Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data" gültige Richtlinien, die eine Harmonisierung der Datenschutzbestimmungen bezwecken. Allerdings sind diese Richtlinien nicht verpflichtend, und die Digitalwirtschaft hat sich seitdem rasant weiterentwickelt. Ein Schritt in diese Richtung war auch die Europäische Datenschutzkonvention, die von den Mitgliedstaaten des Europarats vereinbart wurde und auch der Ratifikation durch Nichtmitgliedstaaten zugänglich ist, wobei dies erst in einem Fall geschehen ist[32].

2. Datenschutz in den USA

Da der Umsatz in den USA im Bereich der Datenverarbeitung nach einer Schätzung für das Jahr 2015 ca. 105 Milliarden US-Dollar betragen wird[33], lohnt ein Blick über den Atlantik. In den USA gibt es kein dezidiertes, konsistentes Datenschutzrecht, das den Umgang privater Akteure mit personenbezogenen Daten regelt. Es gibt kein allgemeines Datenschutzgesetz, sondern lediglich sektorspezifische Vorschriften und unternehmerische Selbstverpflichtungen. Insbesondere kennt das US-amerikanische Recht keine Grundrechtsbindung von Privaten, und grundsätzlich ist jede Datenverarbeitung erlaubt, es sei denn der Kunde hat ihr widersprochen. Lediglich in der kalifornischen Verfassung ist ein unveräußerliches Recht auf Privatsphäre festgeschrieben worden, und durch den „California Online Privacy Protection Act of 2003" werden Website-Betreiber, die Daten über kalifornische Bürger erheben, verpflichtet, einen Hinweis über die Umgangsweise

32 Uruguay ist als erster Nichtmitgliedstaat im August 2013 dem Übereinkommen beigetreten (Quelle: http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=108&CM=2&CL=GER).

33 http://de.statista.com/prognosen/371852/datenverarbeitung-hosting-und-verbundene-taetigkeiten-in-den-usa--umsatzprognose.

mit den personenbezogenen Daten auf der Website zu veröffentlichen und die selbst entwickelten Vorgaben einzuhalten[34].

Um Unternehmen die legale Übermittlung personenbezogener Daten aus Europa in die USA zu ermöglichen, entwickelte das US-Handelsministerium das Safe-Harbor-Verfahren, bei dem US-Unternehmen die Einhaltung der EU-Datenschutzrichtlinie vergleichbarer Standards zertifiziert wird. Die Europäische Kommission hat entschieden, dass durch das Safe-Harbor-Verfahren ein angemessenes Datenschutzniveau im Hinblick auf die Datenübermittlung gewährleistet sei. Angesichts einer Klage des Datenschutzaktivisten Max Schrems geriet in die Kritik, dass die Einhaltung des bescheinigten Datenschutzniveaus von amerikanischer Seite kaum kontrolliert und durchgesetzt wird[35]. Am 6.10.2015 hat der Europäische Gerichtshof die Safe-Harbor-Entscheidung der Europäischen Kommission aus diesen Gründen und wegen unverhältnismäßiger Zugriffe auf die übermittelten Daten durch amerikanische Behörden für ungültig erklärt[36].

Hinsichtlich der staatlichen Datenerhebung und -verarbeitung wurde nach den Anschlägen vom 11. September 2001 der Patriot Act erlassen, der den Geheimdiensten weitreichende Befugnisse, unter anderem die massenhafte Sammlung von Daten zum Kampf gegen den Terrorismus, eingeräumt hatte. Der Patriot Act ist Teil eines umfassenden Anti-Terror-Gesetzespakets, welches nach den Eindrücken der Terroranschläge erlassen und seither immer wieder verlängert wurde. Nach der NSA-Affäre hatte ein Bundesberufungsgericht allerdings entschieden, dass die massenhafte Datensammlung nicht von Section 215 des Patriot Act gedeckt und somit illegal ist. Erstmals konnte nun keine Mehrheit für eine Verlängerung des Patriot Act gefunden werden, und als Folge lief das Überwachungsprogramm der USA am 1. Juni 2015 aus. Wenige Tage später stimmte der Senat jedoch einem Reformgesetz – dem Freedom Act – zu, der die Fortsetzung der Arbeit der Geheimdienste gewährleisten soll. Wesentliche Modifizierung

34 https://oag.ca.gov/privacy/privacy-laws.

35 Meier, Brüssel will Datenübermittlung nach USA neu regeln, abrufbar unter: http://www.tagesspiegel.de/politik/datenschutz-bruessel-will-datenuebermittlung-nach-usa-neu-regeln/11629820.html.

36 EuGH v. 6. Oktober 2015, Rs. C362/14.

ist, dass die NSA nun die Daten nicht mehr selbst speichern, sondern nur noch auf die von den Telefongesellschaften gespeicherten Daten nach einem Beschluss des geheimen Spezialgerichts Foreign Intelligence Surveillance Court (FISC) zugreifen darf. Auch in Bezug auf die Datenverarbeitung der privaten Konzerne werden eine strengere Regulierung und ein stärkerer Schutz der Privatsphäre angestrebt. Eine Regelung mit dem Zweck, den Nutzern mehr Kontrolle darüber zu verschaffen, wer in welchem Umfang die eigenen Netzaktivitäten protokolliert, der sogenannte Do-not-Track Online Act von 2011, wurde dennoch im Kongress abgewiesen.

Ein Teilerfolg konnte mit dem Erlass der Consumer Privacy Bill of Rights erzielt werden, die aber auf eine Selbstverpflichtung der Unternehmen setzt. Vertreter großer Unternehmen sollen mit Politik, Verbraucherschutzbehörden, Datenschützern und anderen Experten ein Regelwerk ausarbeiten, wobei das US-Handelsministerium die Rolle eines Vermittlers einnehmen soll. Die Ergebnisse dieses Prozesses sollen dann in ein verbindliches Gesetz transformiert werden. In den USA existiert keine Datenschutzaufsicht, wie wir sie kennen. Lediglich die FTC (Handelsaufsicht) kontrolliert, ob Unternehmen ihre Selbstverpflichtungen einhalten.

Zu Recht wird festgestellt, dass die USA dringend ein einheitliches, verbindliches Datenschutzrecht benötigen[37]. Die Ausführungen zeigen zwar, dass es in den USA einige Bestrebungen zu einer Verbesserung des Schutzes der Privatsphäre von Nutzern gibt, aus europäischer Sicht sind diese Maßnahmen jedoch nicht weitreichend genug. Vor allem die Consumer Privacy Bill of Rights wird auch in den USA wegen ihrer Unverbindlichkeit scharf kritisiert[38].

3. Wirtschaftliche Konkurrenz

Datenschutzbestimmungen sind mittlerweile zu einem Wettbewerbsfaktor geworden, und die Diversität nationaler Regelungen führt zu

37 Dix, DSB 2015, 62f.

38 Peterson, The White House's draft of a consumer privacy bill is out – and even the FTC is worried, abrufbar unter: https://www.washingtonpost.com/blogs/the-switch/wp/2015/02/27/the-white-houses-draft-of-a-consumer-privacy-bill-is-out-and-even-the-ftc-is-worried/.

Standortunterschieden. Viele Unternehmen haben ein Interesse an international vereinheitlichten Datenschutzbestimmungen, die dem Datenverarbeiter Rechtssicherheit bringen und für gleiche ökonomische Bedingungen sorgen. Im Vergleich zwischen den USA und Europa wird einerseits bemängelt, dass Europa im Wettbewerb zu amerikanischen Konzernen, insbesondere im Bereich der Telekommunikationsindustrie, den Anschluss zu verlieren drohe[39], andererseits wird stets betont, dass das hohe Datenschutzniveau einen Standortvorteil darstellen könne. Insbesondere deutsche Cloud-Services werben mit der Einhaltung hoher Datenschutzstandards, nutzerfreundlichen Voreinstellungen und technischem Schutz von Daten vor Verfälschung, Zerstörung und unzulässiger Weitergabe[40]. Die Europäische Kommission plant zur Begünstigung einer europäischen Cloud-Entwicklung einheitliche Standards zum Datenschutz und zur Datensicherheit. Darüber hinaus soll der Wechsel von Cloud-Anbietern erleichtert werden, um einen freien Datenfluss zu ermöglichen und die Datenwirtschaft voranzutreiben[41]. Ein Rechtsrahmen, der einerseits die Privatsphäre des Bürgers schützt und auf der anderen Seite genug Raum für datenbasierte Innovation zulässt, könnte zum europäischen Exportschlager werden[42].

Mit der Kampagne „E-Mail made in Germany" aus dem Jahr 2013 wurden ebenfalls die deutschen Regelungen zum Datenschutz und zur Datensicherheit genutzt, um das Vertrauen der Kunden zu gewinnen. Erklärtes und mittlerweile erreichtes Ziel diverser Internetprovider war, den E-Mail-Verkehr der Kunden auf dem Transportweg zwischen Mail-Servern und Rechenzentren mit TLS und SSL zu verschlüsseln. Jedoch war diese Verschlüsselungsmethode in den USA zu dem Zeitpunkt längst Standard[43].

39 Berke, Telekom fordert vollständige Deregulierung des Marktes, abrufbar unter: www.wiwo.de/unternehmen/it/positionspapier-telekom-fordert-vollstaendige-deregulierung-des-marktes/8988344.html.

40 http://www.zeit.de/news/2014-03/18/computer-gefeit-vor-der-nsa-deutsche-cloud-anbieter-werben-mit-sicherheit-18143806.

41 Strategie für einen digitalen Binnenmarkt für Europa, abrufbar unter: http://ec.europa.eu/priorities/digital-single-market/docs/dsm-communication_de.pdf.

42 Dehmel, ZD 2015, 197f.

43 http://ccc.de/de/updates/2013/sommermaerchen.

Darüber hinaus sollte die Datenverarbeitung künftig ausschließlich in Rechenzentren in Deutschland erfolgen[44].

Um Daten vor dem Zugriff amerikanischer Geheimdienste zu schützen, entstand die Idee, mit dem „Schengen-Routing" den Datenverkehr und die Datenverarbeitung auf den Schengen-Raum zu begrenzen[45]. Weiterhin gab es jüngst zur Förderung eines sicheren Umgangs mit personenbezogenen Daten einen Vorschlag der Telekom zur Etablierung eines Deutschlandnetzes[46]. Jedoch hat die Telekom stets die Abwicklung des Datentransfers innerhalb Deutschlands behindert, indem sie sich weigerte, mit anderen Providern Peering[47]-Beziehungen aufzubauen, und entgegen der üblichen Praxis ein Entgelt für die Verbindung mit ihrem Backbone-Netz verlangt. Mittlerweile werden diverse Maßnahmen der Abschottung zur Förderung des Datenschutzes, wie etwa die Schaffung eines mit staatlichem Zwangsgeld finanzierten Sozialen Netzwerks in Konkurrenz zu den Angeboten auf dem freien Markt, diskutiert[48]. Allerdings basiert das Internet gerade auf dem globalen, offenen Datenaustausch, und nationalstaatliche Lösungen gefährden das Funktionieren des Netzes und dessen Innovationskraft.

II. Verfassungsrechtliche Vorgaben

1. Recht auf informationelle Selbstbestimmung

Im Grundgesetz existiert kein explizites Grundrecht auf Datenschutz[49], jedoch wird der Schutz der personenbezogenen Daten aus den bestehenden Grundrechten abgeleitet. Aus verfassungsrechtlicher Perspektive sind es

44 Vgl. offizielle Homepage der Kampagne http://www.e-mail-made-in-germany.de/.

45 Clauß, So würde Europas „Schengen-Internet" funktionieren, abrufbar unter: http://www.welt.de/politik/deutschland/article126343060/So-wuerde-Europas-Schengen-Internet-funktionieren.html.

46 http://www.faz.net/aktuell/wirtschaft/netzwirtschaft/plaene-der-telekom-ein-internet-nur-fuer-deutschland-12657090.html.

47 Peering ist der Zusammenschluss von gleichrangigen Computernetzwerken, z. B. Internetprovidern zum Datenaustausch (Quelle: http://www.itwissen.info/definition/lexikon/Peering-peering.html).

48 http://deutsche-wirtschafts-nachrichten.de/2015/06/05/digital-gez-merkel-denkt-ueber-staatliches-internet-nach/.

49 Gegen ein Recht auf Datenschutz mit Verfassungsrang siehe Schulz, ZG 2010, 358ff.

indes nicht die Daten, welche geschützt werden, sondern Datenschutz ist stets Persönlichkeitsschutz.

Besondere Bedeutung kommt hierbei dem vom Bundesverfassungsgericht (BVerfG) in der Volkszählungsentscheidung[50] entwickelten Recht auf informationelle Selbstbestimmung zu, welches eine Ausprägung des Allgemeinen Persönlichkeitsrechts (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) ist. Im Sinne der Selbstbestimmung des Individuums wird die Befugnis des Einzelnen, grundsätzlich selbst zu entscheiden, wann und innerhalb welcher Grenzen persönliche Lebenssachverhalte offenbart werden, gewährleistet. Diese Befugnis wird durch die Möglichkeiten der modernen Datenverarbeitung gefährdet, soweit der Einzelne nicht mehr mit hinreichender Sicherheit überschauen kann, welche ihn betreffenden Informationen seinem sozialen Umfeld bekannt sind, und er dadurch von vornherein in seinem Verhalten dergestalt beeinflusst wird, dass er abweichende Verhaltensweisen vermeidet. In Bezug auf personenbezogene Daten umfasst die informationelle Selbstbestimmung den Schutz vor unbegrenzter Erhebung, Speicherung, Verwendung und Weitergabe persönlicher Daten und schützt die Befugnis, selbst über Preisgabe und Verwendung der personenbezogenen Daten zu bestimmen. Dem informationellen Selbstbestimmungsrecht kommt eine herausragende Bedeutung für den Datenschutz zu, da es zum einen die einfachgesetzlichen Datenschutzgesetze erheblich beeinflusst und zum anderen für mehr Sensibilität im Umgang mit personenbezogenen Daten gesorgt hat[51]. Bis heute ist jedoch der Umfang des Selbstbestimmungsrechts umstritten. Der Begriff der Bestimmungsbefugnis wird in folgender Passage der Volkszählungsentscheidung durch das BVerfG deutlich eingeschränkt:

„Dieses Recht auf informationelle Selbstbestimmung ist nicht schrankenlos gewährleistet. Der Einzelne hat nicht ein Recht im Sinne einer absoluten, unbeschränkten Herrschaft über ‚seine' Daten; er ist vielmehr eine sich innerhalb der sozialen Gemeinschaft entfaltende, auf Kommunikation angewiesene Persönlichkeit. Information, auch soweit sie personenbezogen

50 BVerfGE 65, 1 (41); BVerfG, Urteil v. 15. Dezember 1983, Az. 1 BvR 209, 269, 362, 420, 440, 484/83.

51 Hoffmann, Die Gewährleistung der Vertraulichkeit und Integrität elektronischer Daten- und Dokumentensafes, S. 66.

ist, stellt ein Abbild sozialer Realität dar, das nicht ausschließlich dem Betroffenen allein zugeordnet werden kann."[52]

Das BVerfG hat hier die Gemeinschaftsbezogenheit des Individuums betont und klargestellt, dass der Einzelne Einschränkungen seiner Selbstbestimmtheit im überwiegenden Allgemeininteresse erdulden muss. Die Selbstbestimmung über die eigenen Daten unterliegt daher stets einem Abwägungsprozess[53]. Es liegt nahe, dass es personenbezogene Daten gibt, über die das Individuum kein Bestimmungsrecht haben kann, wie z. B. Daten des Einwohnermeldeamts, des Finanzamts oder Gesundheitsdaten der Krankenkassen.

2. Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme

Aufgrund der technischen Entwicklungen, insbesondere der weitreichenden Verbreitung von informationstechnischen Geräten im alltäglichen Gebrauch, der gestiegenen Nutzung des Internets und neuer Kommunikationsmöglichkeiten steigt die Gefahr einer unerwünschten Ausspähung von Daten durch Dritte. In seiner lückenfüllenden Funktion gewährleistet das allgemeine Persönlichkeitsrecht in seiner Ausprägung als Recht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme Schutz vor Persönlichkeitsgefährdungen, die bei der Nutzung informationstechnischer Systeme zur Persönlichkeitsentfaltung entstehen können. Dieses sogenannte IT-Grundrecht schützt jedoch vor Eingriffen in informationstechnische Systeme nur, soweit der Schutz nicht durch andere Grundrechte, insbesondere Art. 10, 13 GG, sowie das Recht auf informationelle Selbstbestimmung gegeben ist. Die Schaffung dieses „neuen Grundrechts" ist in Abgrenzung zur informationellen Selbstbestimmung notwendig gewesen, da durch eine technische Manipulation von Geräten ein umfassendes Persönlichkeitsprofil eines Nutzers erstellt werden kann, ohne dabei auf Datenerhebungs- und Datenverarbeitungsmaßnahmen angewiesen zu sein

52 BVerfGE 65, 1 (43, 44).

53 Vgl. Leibholz/Rinck, GG Kommentar (Stand: 68. EL, Juli 2015), Art. 2, Rn. 106; Reiners, ZD 2015, 51 (54).

(Infiltration), und das Recht auf informationelle Selbstbestimmung nur vor dem Zugriff auf einzelne Kommunikationsvorgänge bzw. auf einzelne Daten schützt[54].

3. Mittelbare Drittwirkung und staatliche Schutzpflichten

Während das BVerfG bei der Volkszählungsentscheidung noch die Abwehr von staatlicher Datenerhebung vor Augen hatte, steht heute im Fokus des Datenschutzes die umfassende Datenerhebung durch private Akteure. Seit der Schaffung des Rechts auf informationelle Selbstbestimmung hat sich die Art der Daten und der Datenerhebung aufgrund der technischen Neuerungen – insbesondere dem Internet der Dinge – grundlegend verändert. In der digitalen Welt drohen die meisten Verletzungsgefahren von privater Seite, und daher wird die Drittwirkungsproblematik der Grundrechte immer zentraler. In traditioneller Ausrichtung sind Grundrechte Abwehrrechte des Einzelnen gegenüber Eingriffen von staatlicher Seite, doch auch gegenüber Privaten ist die Grundrechtsposition des Einzelnen nicht bedeutungslos. Es ist allgemein anerkannt, dass die verfassungsrechtlichen Grundprinzipien die gesamte Rechtsordnung prägen und das einfache Gesetzesrecht grundrechtskonform auszulegen ist. Daher entfalten die Grundrechte auch in privatrechtlichen Beziehungen eine mittelbare Drittwirkung, indem über die Generalklauseln und sonstige wertungsoffene Zentralbegriffe die grundrechtliche Wertordnung zur Geltung gelangt. Der unmittelbar durch Art. 1 Abs. 3 GG grundrechtsgebundene Richter oder sonstige Gesetzesanwender muss bei der Auslegung und Anwendung des gesamten Rechts den objektiven Gehalt der Grundrechte berücksichtigen und darf nicht Bedeutung und Tragweite einzelner Grundrechte verkennen.

Nicht nur die Judikative und die Exekutive, sondern auch die Legislative ist in gewissem Umfang verpflichtet, den Grundrechten zu voller Geltung zu verhelfen. Nach der Lehre von den grundrechtlichen Schutzpflichten muss der Staat nicht nur eigene Grundrechtsverletzungen unterlassen, sondern auch aktiv tätig werden, um den einzelnen Bürger vor unzulässigen

54 Hoffmann, Die Gewährleistung der Vertraulichkeit und Integrität elektronischer Daten- und Dokumentensafes, S. 69f.; BVerfGE 120, 274 (312f.).

Beeinträchtigungen durch Dritte zu schützen. Nur durch diesen Gehalt der Grundrechte kann die Grundrechtsausübung umfassend sichergestellt werden. Der grundrechtliche Schutz der freien Entfaltung der Persönlichkeit führt dazu, dass der Staat auch vor unrechtmäßiger Datenverarbeitung durch Private schützen und die Informiertheit des Einzelnen über Datenverarbeitungsvorgänge sicherstellen muss.

III. Rechtliche Aspekte des Datenhandels basierend auf der aktuellen einfachgesetzlichen Ausgestaltung des Datenschutzes

1. Datenschutzgesetzgebung

Der Schutzbereich der informationellen Selbstbestimmung bedarf zur Sicherstellung der Selbstbestimmtheit des Einzelnen einer einfachgesetzlichen Konkretisierung. Um seiner Schutzpflicht gerecht zu werden, muss der Gesetzgeber tätig werden und ein gewisses Datenschutzniveau normieren. Bereits 1977 und somit zeitlich vor der „Schaffung" des Rechts auf informationelle Selbstbestimmung durch das BVerfG gab es ein Bundesdatenschutzgesetz als Reaktion auf die zunehmende Automatisierung der Datenverarbeitung. Mit dem Volkszählungsurteil hat das BVerfG betont, dass die Entwicklungen der modernen Informationstechnologie zu einer Notwendigkeit von verfahrensrechtlichen und organisatorischen Schutzmaßnahmen für den Bürger führen. Mit der Neufassung des Bundesdatenschutzgesetzes vom 20.12.1990 entwickelte der Gesetzgeber das Datenschutzrecht in Umsetzung der Volkszählungsentscheidung weiter. Wesentliche Neuerungen waren die Einführung des Zweckbindungsprinzips, der Grundsatz der frühzeitigen Anonymisierung von Daten, umfassende Auskunftsrechte des Betroffenen und die Einrichtung unabhängiger Datenschutzbehörden. Mit der Neufassung des BDSG vom 06.04.2001 wurden die Vorgaben der DSRL in das nationale Datenschutzrecht transformiert.

2. Datenschutzrechtliche Einwilligung

Der Begriff „Datenschutz" ist missverständlich, denn geschützt werden nicht die Daten, sondern die dahinterstehenden Betroffenen und deren Recht auf freie Entfaltung ihrer Persönlichkeit. Datenschutz ist daher auch

kein Selbstzweck, sondern normierte Regelungen sollten sich stets auf die Schutzbedürftigkeit der Betroffenen zurückführen lassen. Dabei muss der Einzelne als selbstbestimmtes Individuum entscheiden können, ab welchem Umfang eine Veröffentlichung und Verbreitung der auf ihn bezogenen Daten das ihm zuträgliche Maß überschreitet. Um gerade diese Selbstbestimmtheit zu gewährleisten, wurden ein grundsätzliches Verbot mit Erlaubnisvorbehalt und das Rechtsinstitut der datenschutzrechtlichen Einwilligung geschaffen. Die Einwilligung erlaubt es dem Betroffenen, selbst über die Rechtfertigung von Eingriffen in sein Recht auf informationelle Selbstbestimmung zu entscheiden. Nach dem BDSG ist eine Verarbeitung personenbezogener Daten grundsätzlich unzulässig, es sei denn, dies ist durch einen gesetzlichen Erlaubnistatbestand oder durch den Betroffenen mittels seiner Einwilligung legitimiert[55]. Eine Einwilligung in die Datenverwendung ist nur wirksam, wenn sie auf der freien Entscheidung des Betroffenen beruht und dieser vorher über den Zweck der Datenverwendung informiert wurde.

Man unterscheidet zwischen der einseitigen und der schuldrechtlichen Einwilligung. Eine einseitige Einwilligung liegt immer dann vor, wenn die Einwilligung in die Datenverarbeitung einen eigenständigen, isolierten Vorgang darstellt. Mit dem Datenhandel kommt der Einwilligung allerdings zunehmend eine neue Funktion als Kommerzialisierungsinstrument zu. Da im Netz eine Gratiskultur herrscht, wird die Nutzung von Diensten unentgeltlich zur Verfügung gestellt, jedoch vielfach von der Abgabe einer datenschutzrechtlichen Einwilligungserklärung abhängig gemacht. So werden „Datenschutzrichtlinien" häufig als Nebenabreden Bestandteil von schuldrechtlichen Verträgen zur kostenfreien Nutzung einer IT-Infrastruktur. Die vertragliche Einordnung von Rechtsverhältnissen, bei denen ein Systembetreiber ein Anwendungsprogramm für wiederkehrende Nutzungen zur Verfügung stellt, ist schwer vorzunehmen. Festhalten lässt sich, dass es sich trotz der Unentgeltlichkeit um ein Rechtsgeschäft handelt. Die Einwilligungserklärung als solche wird oftmals in die Allgemeinen Geschäftsbedingungen (AGB) mit der Folge der AGB-Kontrolle integriert. Daneben gibt es den Fall, dass die Einwilligungserklärung selbst nicht Vertragsbestandteil

55 Vgl. § 4 Abs. 1 BDSG.

ist, sondern dass ihr als Begleiterscheinung einer sonstigen rechtsgeschäftlichen Leistungsbeziehung eine vertragsgestaltende Rolle zukommt[56].

3. Gesetzliche Erlaubnistatbestände

Die Zulässigkeit der Erhebung, Verarbeitung und Nutzung von Daten kann nicht in allen Fällen von der Einwilligung der Betroffenen abhängig sein. Bei öffentlichen Stellen greifen die §§ 13ff. BDSG, wobei die Datenverarbeitung generell zur Erfüllung einer öffentlichen Aufgabe erforderlich sein muss. Im Bereich der Datenverwendung durch Private ist nicht nur das Recht auf informationelle Selbstbestimmung der Betroffenen zu berücksichtigen, sondern die kommerziellen Tätigkeiten privater Akteure sind ebenfalls grundrechtsgeschützt, z. B. durch die Berufs- und Unternehmerfreiheit gemäß Art. 12 Abs. 1 oder die Pressefreiheit gemäß Art. 5 Abs. 1 S. 2 GG, allenfalls durch die allgemeine Handlungsfreiheit gemäß Art. 2 Abs. 1 GG. Um auch diesen Grundrechtsberechtigten gerecht zu werden, gibt es mit den §§ 28ff. BDSG diverse Erlaubnistatbestände für die Datenverwendung. Einer gesetzlichen Legitimation zugänglich sind folgende Arten der Datenverarbeitung: Datenverarbeitung im Rahmen eines Schuldverhältnisses, zur Erfüllung einer rechtlichen Verpflichtung, zur Wahrung lebenswichtiger Interessen des Betroffenen, zur Erfüllung öffentlicher Aufgaben und auf Grundlage einer Interessenabwägung.

4. Datenschutzprinzipien

Das aktuelle Datenschutzrecht beruht auf den nachfolgenden sechs Prinzipien: Grundsatz der Zweckbindung, Erforderlichkeitsgrundsatz, Datenvermeidung und Datensparsamkeit, Transparenzgrundsatz, Rechte der Betroffenen und Kontrolle.

Nach dem Grundsatz der Zweckbindung müssen verantwortliche Stellen[57] bereits vor der Datenerhebung den Zweck der Datenverwendung definieren, und jegliche sich anschließende Datenverarbeitung muss sich im

56 Siehe dazu Rogosch, Die Einwilligung im Datenschutzrecht, S. 41ff.

57 Nach § 3 Abs. 7 BDSG ist verantwortliche Stelle jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt.

festgelegten Rahmen bewegen[58]. Der Erforderlichkeitsgrundsatz sagt aus, dass Daten nur in dem Umfang erhoben, verarbeitet und genutzt werden dürfen, den der festgelegte Zweck erforderlich macht[59].

Nach § 3a S. 1 BDSG wird der verantwortlichen Stelle die Zielvorgabe gemacht, keine (Datenvermeidung) oder möglichst wenig (Datensparsamkeit) personenbezogene Daten zu verwenden. Die Grundsätze der Datenvermeidung und Datensparsamkeit resultieren daher, dass von der grundsätzlichen Unerwünschtheit jeglicher Datenverarbeitung ausgegangen wird. Unter dem Ansatz „Privacy by Design"[60] sollen die Erfordernisse des Datenschutzes bereits bei der Entwicklung neuer Technologien berücksichtigt und der Datenschutz technisch bei dem Design von IT-Systemen umgesetzt werden. Gerade im Zusammenhang mit komplexen IT-Strukturen verfügen viele Nutzer nicht über ausreichend Kenntnisse, um Maßnahmen zum Selbstschutz zu ergreifen. Daher wird unter dem Stichwort „Privacy by default" ein Grundschutz der Nutzer durch datenschutzfreundliche Voreinstellungen diskutiert.

Transparenz bildet die Grundlage dafür, dass der Betroffene sein Selbstbestimmungsrecht wahrnehmen kann. Schon das BVerfG hielt es für unverzichtbar, dass der Bürger auch in der modernen Informationsgesellschaft Kenntnis davon hat, wer was wann und bei welcher Gelegenheit über ihn weiß[61]. Um Mitwirkungs- und sonstige Kontrollrechte wahrnehmen zu können, bedarf es zunächst der Auskunftsrechte gemäß §§ 19, 34 BDSG und der Benachrichtigungsrechte nach §§ 19a, 33 BDSG. Die Auskunftserteilung umfasst Inhalt und Quelle der zu seiner Person gespeicherten Daten, die Identität von Empfängern der Daten und den Zweck der Datenspeicherung. Daneben kann der Betroffene Ansprüche auf Berichtigung, Löschung oder Sperrung nach §§ 20, 35 BDSG geltend machen. Um die Einhaltung des

58 Heckmann, in: Taeger/Gabel (Hrsg.), BDSG, § 13, Rn. 25f.; Taeger, in: Taeger/Gabel (Hrsg.), BDSG, § 28, Rn. 110ff.

59 Scholz, in: Simitis (Hrsg.), BDSG, § 3a, Rn. 33f.

60 Vgl. Beitrag „Privacy by Design" v. Peter Schaar in der Fachzeitschrift „Identity in the Information Society", abrufbar unter: http://www.bfdi.bund.de/SharedDocs/Publikationen/%22PrivacyByDesign%22.pdf?__blob=publicationFile.

61 BVerfGE 65, 1 (43).

Datenschutzrechts zu überwachen, sind staatliche Kontrollinstanzen nötig. Für den Bereich der öffentlichen Stellen des Bundes ist der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit[62] zuständig. Für den öffentlichen Bereich auf Länderebene sind die Landesdatenschutzgesetze maßgeblich. Im nicht öffentlichen Bereich kontrollieren unabhängige Aufsichtsbehörden die Ausführung des Bundesdatenschutzgesetzes[63]. Darüber hinaus gibt es die Datenschutzbeauftragten für öffentliche und nicht öffentliche Stellen nach § 4f BDSG.

62 §§ 22 ff. BDSG.
63 § 38 BDSG.

E. Reformbedarf des Datenschutzrechts

Das derzeitige Datenschutzrecht wird den aktuellen Entwicklungen der Datenwirtschaft nicht mehr gerecht. Sowohl das Rechtsinstitut der datenschutzrechtlichen Einwilligung als auch die Datenschutzprinzipien sind in vielen Bereichen nicht geeignet, den gewandelten Umgang mit personenbezogenen Daten rechtlich zu erfassen. Im Folgenden soll der Reformbedarf des Datenschutzrechts im Hinblick auf das Verhältnis von Betroffenen zu privaten Datenverarbeitern untersucht werden. Auch inwieweit die derzeitigen Regelungen einer Anpassung bedürfen, um Datenschutz im Hinblick auf die rasante Entwicklung neuer Technologien besser umzusetzen, ist nachstehend zu analysieren.

I. Kommerzialisierung von personenbezogenen Daten

Das aktuelle Datenschutzrecht dient dem Schutz der freien Entfaltung der Persönlichkeit. Heute ist aber eine zweite Dimension im Umgang mit personenbezogenen Daten hinzugetreten: ihr wirtschaftlicher Wert. Das Datenschutzrecht beinhaltet keine Regelungen für eine Kommerzialisierung von personenbezogenen Daten, sondern schützt den Betroffenen paternalistisch vor einer Kommerzialisierung und schränkt ihn insoweit in seinen Möglichkeiten ein. Es sollte allerdings dem Einzelnen zumindest bei gewissen Arten von Daten freistehen, diese zu kommerzialisieren. Wichtig dabei ist, dass die Monetarisierung der Daten stets durch den Betroffenen erfolgt und dessen Datenhoheit sichergestellt ist. Man kann rein faktisch die umfassende Datenerhebung nicht aufhalten, und viele Nutzer sind jetzt schon bereit, ihre personenbezogenen Daten für einen kleinen Vorteil preiszugeben. Die gesetzlichen Schutzmechanismen des BDSG sind in vielen Fällen wirkungslos, werden umgangen oder lassen sich schlicht nicht kontrollieren. Auch erscheint es nicht zielführend, auf einem Schutzregime zu beharren, das im Widerspruch zu den tatsächlichen Gegebenheiten und Bedürfnissen steht. Unstreitig ist, dass der Datenhandel bereits Realität geworden ist und dringend ein neuer rechtlicher Rahmen benötigt wird, um den Datenhandel zu kontrollieren und unerwünschte Entwicklungen zu vermeiden.

II. Das personenbezogene Datum

Wie bereits erläutert[64], ist die Unterscheidung zwischen Daten, bei denen sich der Personenbezug herstellen lässt, und solchen, bei denen dies nicht der Fall ist, in der Praxis schwierig vorzunehmen. Darüber hinaus nimmt mit neuen Analysemethoden der Anteil personenbezogener Daten drastisch zu. Besonders auffällig ist, dass mit der Zunahme der Datenerhebung aufgrund neuer Methoden und sinkender Speicherkosten auch stetig triviale Daten an Bedeutung gewinnen. Nicht in jedem Datum spiegelt sich gleichermaßen die Persönlichkeit der betreffenden Person wider. Es stellt sich die Frage, ob alle Daten gleichermaßen dem aktuell hohen Schutzniveau des Datenschutzrechts unterstehen oder ob nicht vielmehr Abstufungen gemacht werden sollten. Zu Zeiten des Volkszählungsurteils und bei Normierung des BDSG schien es noch sinnvoll, alle personenbezogenen Daten dem gleichen umfassenden Schutz zu unterstellen. Seitdem haben sich allerdings der Umgang mit und die Art der Daten tief greifend verändert – Daten sind zu Wirtschaftsgütern geworden, und daher bedarf es anderer gesetzlicher Rahmenbedingungen. Es kann sogar im Interesse des Einzelnen liegen, dass die wirtschaftliche Verwertung bei einigen Arten von Daten erleichtert wird, wenn für ihn damit entscheidende Vorteile einhergehen.

III. Datenschutzprinzipien

1. Datenvermeidung und Datensparsamkeit

Die grundlegendste Zielvorgabe des BDSG ist die der Datenvermeidung und Datensparsamkeit. Es stellt sich jedoch die Frage, ob man heute noch von der Unerwünschtheit jeglicher Datenverarbeitung ausgehen kann. In einem Zeitalter der Informations- und Wissensgesellschaft bietet die Internet- und Kommunikationsindustrie auch große wirtschaftliche Chancen und Möglichkeiten. Es erscheint paradox, dass Daten ein immer größerer Wert aufgrund der damit verbundenen Analysemöglichkeiten und der daraus resultierenden Innovationsfähigkeit und des wirtschaftlichen Wachstums zukommt und dennoch die Datenerhebung und somit die Generierung wirtschaftlicher

64 Vgl. dazu B. III.

Werte restriktiv gehandhabt werden sollen. Die Informations- und Kommunikationstechnik ist von tragender Bedeutung für die Wettbewerbsfähigkeit jeder Industrienation. Deutschland droht im internationalen Vergleich den Anschluss an die amerikanische und asiatische Konkurrenz zu verlieren[65]. Bei geänderten rechtlichen Rahmenbedingungen, beispielsweise in Form einer monetären Beteiligung des Einzelnen an der Verwertung seiner Daten, könnte die Datenverarbeitung auch von Seiten des Betroffenen in vielen Bereichen durchaus erwünscht sein. Gerade die Anonymisierung und Pseudonymisierung lassen sich zunehmend schwieriger verwirklichen und entsprechen auch nicht mehr in allen Fällen den Interessen der Betroffenen.

Datenvermeidung sollte heute nicht mehr das Ziel des Datenschutzes sein. Vielmehr sollte die Selbstbestimmtheit des Betroffenen, die auch die wirtschaftliche Verwertung der Daten und eine Möglichkeit der Beteiligung an von Dritten erzielten Gewinnen einschließt, im Fokus stehen. Sofern der Einzelne eine Kommerzialisierung als erstrebenswert ansieht, sollte es ihm leichter möglich sein, seine personenbezogenen Daten aktiv zu kommerzialisieren.

Die Zielvorgabe der Datensparsamkeit wird ohnehin in weiten Teilen nicht mehr eingehalten, da deren Nichteinhaltung keine Konsequenzen nach sich zieht. Es handelt sich zwar grundsätzlich um eine Rechtspflicht der verantwortlichen Stelle, jedoch führt ein Verstoß weder zur materiellen Rechtswidrigkeit der Datenverarbeitung, noch ist er bußgeld- oder strafbewehrt, und demzufolge kann die Aufsichtsbehörde auch keine Zwangsmaßnahmen ergreifen. Dieser Umstand führt dazu, dass der Datenschutz verstärkt als unzureichend und wirkungslos empfunden wird. Wenn eine Stelle ihre Datenverarbeitung nicht datensparsam und datenvermeidend ausgestaltet, hat dies keine unmittelbaren negativen Auswirkungen. Lediglich wenn zugleich der als Zulässigkeitsvoraussetzung ausgestaltete Erforderlichkeitsgrundsatz verletzt ist, sieht dies anders aus. Jedoch ist auch dann

65 Berke, Telekom fordert vollständige Deregulierung des Marktes, abrufbar unter: http://www.wiwo.de/unternehmen/it/positionspapier-telekom-fordert-vollstaendige-deregulierung-des-marktes/8988344.html.

eine unerwünschte Kommerzialisierung von Daten durch Internetkonzerne faktisch schwer aufzuhalten.

2. Zweckbindungsgrundsatz

Zunehmendes Problem für die Realisierung von Big Data ist der bestehende Widerspruch zum Zweckbindungsgrundsatz. Um Big-Data-Analysen betreiben zu können, bedarf es eines gewissen Datenbestands. Da die konkreten Fragestellungen der diversen Analysen bei der Datenerhebung noch nicht feststehen, kann über die Nutzungen der Daten keine spezifische Aussage getroffen werden. Das Datenschutzrecht verlangt jedoch die Formulierung eines Verwendungszwecks bereits vor der Datenerhebung[66]. In der Praxis wird der Zweck der Datenerhebung daher in vielen Fällen sehr allgemein gehalten, sodass möglichst viele potenzielle Nutzungsarten darunter zu fassen sind. Die datenschutzrechtliche Einwilligung ist aber nur wirksam, wenn sie auf einer freien Entscheidung des Betroffenen beruht, und dies setzt voraus, dass der Betroffene über den Zweck der Erhebung, Verarbeitung und Nutzung in Kenntnis gesetzt wurde. Der Nutzer muss sich ein Bild über die künftige Datenverarbeitung machen können. Unklar ist, ab welcher Unbestimmtheit des Zwecks die datenschutzrechtliche Einwilligung und somit die Datenverwertung unwirksam sind. Hierfür bräuchte es klare Kriterien, beispielsweise durch eine gewachsene Rechtsprechung. Auch die Datenschutzbehörden sind aufgrund ihrer ungenügenden personellen und finanziellen Ausstattung[67] nur bedingt in der Lage, die Ungenauigkeiten bei der Angabe des Zwecks der Datenerhebung und -verwendung hinreichend aufzudecken und zu unterbinden.

3. Transparenz

Transparenz, also eine umfassende und verständliche Aufklärung, ist zur Ausübung des Rechts auf informationelle Selbstbestimmung unerlässlich. Nur wer informiert ist, kann seine Rechte gegenüber der

66 Vgl. § 4 Abs. 3 Nr. 2 BDSG.

67 Xamit Datenschutzbarometer 2013, 2009, abrufbar unter: http://www.xamit-leistungen.de/veroeffentlichungen/studien-und-tests/.

datenverarbeitenden Stelle wahrnehmen und gegebenenfalls auch gerichtlich durchsetzen. Allerdings erweist sich die Umsetzung von Informationspflichten in der Realität als unzureichend. Es gibt zu ausführliche und zu knappe, versteckte, unübersichtliche und überflüssige Einwilligungserklärungen. Oftmals werden die entsprechenden Passagen bewusst allgemein formuliert, sodass der Datenverarbeiter aufgrund der Angabe als „Partnerunternehmen" nicht eindeutig zu bestimmen ist und hinsichtlich des Verarbeitungszwecks ein gewisser Interpretationsspielraum besteht. Ferner müssen die allgemeinen Datenschutzhinweise klarer von der Einwilligungserklärung getrennt werden. Durch seitenlange Ausführungen wird der Nutzer abgeschreckt und ist oftmals nicht in der Lage, wichtige Informationen herauszufiltern. Dies führt dazu, dass überforderte Betroffene ihre Einwilligung erteilen, ohne den angebotenen Text zur Kenntnis zu nehmen. Oftmals wird darauf spekuliert, dass Betroffene einmalig eine Einwilligung vorschnell und ohne Kenntnisnahme der relevanten Informationen erteilen und anschließend mangels spürbarer negativer Konsequenzen auch nicht widerrufen. So verlieren Betroffene zunehmend die Kontrolle über ihre personenbezogenen Daten. In diesem Bereich besteht erheblicher Reformbedarf, um den Nutzern Wissen über die Verwendung ihrer Daten zu verschaffen. Nur Aufklärung kann hier die gewünschte Datenhoheit bringen.

4. Kontrolle

Die staatliche Kontrolltätigkeit im Bereich des Datenschutzes ist unzureichend. Es werden keine flächendeckenden Datenschutzkontrollen vergleichbar den Betriebsprüfungen durch Finanz- oder Gesundheitsämter durchgeführt. Zudem verfügen die deutschen Datenschutzbehörden nur über knappe personelle Ressourcen. Eine Studie von Xamit stellte 88,6 Verstöße oder Gründe zur Beanstandung auf jeweils 100 untersuchten Webpräsenzen fest[68]. Datenschutzverstöße sind alltäglich, da das Risiko der

68 Xamit Datenschutzbarometer 2013, abrufbar unter: http://www.xamit-leistungen.de/veroeffentlichungen/studien-und-tests/.

Entdeckung und der Verhängung eines Bußgelds[69] für Unternehmen sehr gering ist und daher Verstöße bewusst in das unternehmerische Risiko einkalkuliert werden. Es ist gängige Übung von Internetkonzernen, allgemeine und unverständliche bzw. versteckte Einwilligungserklärungen in ihren Allgemeinen Geschäftsbedingungen unterzubringen. Sind die Daten einmal in den Besitz von Unternehmen gelangt, können diese faktisch in zahlreichen Fällen mit ihrem Datenbestand nach Belieben verfahren. Zum einen gibt es zu wenig Kontrolle durch staatliche Aufsichtsbehörden und durch die Betroffenen selbst, zum anderen existieren zu viele rechtliche Grauzonen durch die Konturlosigkeit und Unbestimmtheit des Datenschutzrechts.

Wie bereits erläutert, existieren keine klaren Kriterien dafür, ob eine Datensammlung zulässig oder unzulässig ist – gerade im Bereich der Zweckbindung und der Einwilligungserklärung ist unklar, welche Ausgestaltung zu einer Unzulässigkeit der Datenverarbeitung führt. Es gibt zahlreiche unwirksame Einwilligungserklärungen, die aber allesamt nicht überprüft werden. Ein großes Problem ist, dass zu wenig Betroffene ihre Rechte wahrnehmen und mangels Klagen auch kaum gerichtliche Kontrolle stattfindet[70]. Die geringe Zahl an gerichtlichen Überprüfungen von datenschutzrechtlichen Einwilligungserklärungen wird darauf zurückgeführt, dass die Datenverarbeitung und Datenweitergabe für den Nutzer, abgesehen von der ihn erreichenden personalisierten Werbung, meistens keine spürbaren Auswirkungen hat. Hinzu kommt, dass die Datenverarbeitung oft derart intransparent betrieben wird, dass der Betroffene keine Kenntnis über die Identität des Klagegegners hat und erhebliche Beweisschwierigkeiten bestehen[71].

---

69 Bußgelder werden oft von den Datenschutzbehörden nur als Ultima Ratio verhängt, wenn dem Datenschutzverstoß nicht anderweitig Abhilfe geleistet werden kann.

70 Einige wegweisende Urteile z. B. des OLG Hamburg (AZ 3 U 26/12) oder des OLG Karlsruhe (AZ 6 U 38/11) behandeln den wettbewerbsrechtlichen Aspekt von Datenschutzverstößen; hiernach sind mangelhafte Datenschutzerklärungen wettbewerbswidrig und mit Abmahnungen durch Konkurrenten angreifbar. Als Folge dieser Rechtsprechung wird voraussichtlich mehr unzulässigen Methoden durch Konkurrenzunternehmen Einhalt geboten werden.

71 Weidlich-Flatten, ZRP 2014, 196.

IV. Datenschutzrechtliche Einwilligung

Die datenschutzrechtliche Einwilligung ist zentrales Element des derzeitigen Datenschutzrechts zur Sicherstellung der informationellen Selbstbestimmung und somit des Persönlichkeitsschutzes. Aufkommenden Konzepten der „Datenherrschaft", „Datensouveränität" und „Datenhoheit" ist der Gedanke gemein, dass der Betroffene in seiner Selbstbestimmung gestärkt werden muss und die Privatautonomie Einzug in den Bereich der personenbezogenen Daten erhalten sollte[72]. Die geltende Rechtslage sieht mit § 4a BDSG bereits eine freiwillige Einwilligung in die Datenverarbeitung vor, welche der Sicherstellung der Datensouveränität dienen soll. Die Grundkonzeption, dass der Einzelne aufgrund einer informierten Entscheidung selbst Verantwortung für die Preisgabe seiner Daten trägt, ist zu begrüßen. Leider weist die Einwilligung in ihrer jetzigen Form jedoch einige Schwachpunkte auf.

1. Unzureichende Erfassung eines tatsächlich bestehenden Austauschverhältnisses

In ihrer ursprünglichen Konzeption sollte die Einwilligung als reines Rechtfertigungsinstrument für eine den Schutzbereich des informationellen Selbstbestimmungsrechts tangierende Datenverarbeitung dienen. Es handelt sich grundsätzlich um eine einseitige rechtsgeschäftliche Willenserklärung, die einen isolierten, eigenständigen Vorgang darstellt[73]. Jedoch wird von Seiten der Unternehmen zunehmend der wirtschaftliche Wert von personenbezogenen Daten mithilfe des Instruments der Einwilligung ausgeschöpft. Die Einwilligungserklärung als solche ist dabei häufig in die allgemeinen Geschäftsbedingungen von Konzernen integriert und somit Vertragsbestandteil. Bereits hier zeigt sich, dass nicht mehr von einem eigenständigen, einseitigen Vorgang auszugehen ist, da die Einwilligung vielfach im Zusammenhang mit einem Vertrag steht. Bei den Nutzungsverhältnissen von diversen Online-Diensten wird entgegen der Wirklichkeit aber

72 Vgl. Bosesky/Deussen/Quandt/Schulz/Strick, Datenhoheit in der Cloud, S. 7ff.; Seidel, ZG 2014, 153 (155).

73 Rogosch, Die Einwilligung im Datenschutzrecht, S. 39f.

vielfach immer noch von einer Zweiteilung ausgegangen: Auf der einen Seite steht der Abschluss eines Rechtsgeschäfts zur unentgeltlichen Nutzung der IT-Infrastruktur; auf der anderen Seite wird eine datenschutzrechtliche Einwilligung von Seiten des Nutzers erteilt[74]. Das tatsächlich bestehende Austauschverhältnis sollte sich auch rechtlich in einer Verknüpfung von Leistung und Gegenleistung niederschlagen[75] – die datenschutzrechtliche Einwilligung ist als Instrument für diese Art von Tauschgeschäften jedoch aus mehreren Gründen, die sogleich dargestellt werden, ungeeignet.

2. Ungeeignetheit der Einwilligung als Instrument zur Erfassung eines Austauschverhältnisses

Die datenschutzrechtliche Einwilligung ist grundsätzlich jederzeit frei für die Zukunft widerrufbar. Die Rechtmäßigkeit bereits erfolgter Datenverarbeitungen soll zum Schutz der Interessen der datenverarbeitenden Stelle vom Widerruf unberührt bleiben. Die Widerrufsmöglichkeit folgt aus der informationellen Selbstbestimmung, da es dem Einzelnen jederzeit möglich sein muss, seine Persönlichkeit durch einen veränderten Umgang mit seinen personenbezogenen Daten stärker zu schützen. Oftmals ist sich der Nutzer bei der Erteilung nicht der Tragweite der Einwilligung für seine informationelle Selbstbestimmung und für die Vertraulichkeit seiner Daten bewusst[76]. Im Sinne der Selbstbestimmung muss es eine Möglichkeit für den Einzelnen zu einer Korrektur für die Zukunft geben. Wenn aber nun die datenschutzrechtliche Einwilligung vielfach eine Gegenleistung darstellt, kann der unmittelbar nach Vertragsschluss erfolgende Widerruf zu unbilligen Ergebnissen führen. Der IT-Dienstleister gewährt dem Nutzer einen geldwerten Vorteil in Form der kostenlosen Inanspruchnahme einer IT-Leistung und muss durch die Möglichkeit des jederzeitigen Widerrufs der Datennutzung seinerseits stets mit dem Wegfall des geldwerten Vorteils rechnen. Der

74 Bräutigam, MMR 2012, 635 (636).

75 Ein Gegenseitigkeitsverhältnis und somit die Entgeltlichkeit von IT-Dienstleistungen mit der Konsequenz der Umsatzsteuerpflichtigkeit bei persönlicher Anmeldung des Verbrauchers mittels eines Kontos bejahend LG Berlin, 15 O 402/12, nicht rechtskräftig; siehe dazu Melan/Wecke, DStR 2015, 2267ff.

76 Tinnefeld/Buchner/Petri, Einführung in das Datenschutzrecht, S. 360.

Berechtigte der Datennutzung hat ein Interesse daran, dass ihm die Einwilligung nicht willkürlich nach Belieben wieder entzogen werden kann.

Ferner kann das Kopplungsverbot einer wirksamen Verknüpfung von Leistung und Gegenleistung im Weg stehen. Das Kopplungsverbot nach § 28 Abs. 3b BDSG besagt, dass die verantwortliche Stelle den Abschluss eines Vertrags nicht von einer Einwilligung in eine Datenverarbeitung für Zwecke der Werbung oder des Adresshandels abhängig machen darf, sofern dem Betroffenen ein anderer Zugang zu gleichwertigen vertraglichen Leistungen ohne die Einwilligung nicht oder nicht in zumutbarer Weise möglich ist. Diese Vorschrift soll dem Missbrauch von Marktmacht bzw. einer Monopolstellung entgegenwirken. Es kommt folglich auf die Marktsituation an, sodass eine andere Zugangsmöglichkeit i.S.d. Vorschrift besteht, wenn dem Nutzer ein gleichwertiger Dienst eines anderen Marktteilnehmers zur Verfügung steht. Das OLG Brandenburg hielt in Bezug auf die vergleichbare Vorschrift des § 12 Abs. 3 TMG a.F. einen Marktanteil von ca. 76 % in dem konkret verhandelten Fall für die Annahme einer Monopolstellung nicht für ausreichend[77].

Da die personalisierte Werbung einen Großteil der Verarbeitung von Daten ausmacht, ist diese Vorschrift für die Praxis von besonderer Relevanz. Viele Online-Dienste wollen ihre Leistung dem Nutzer nur zugänglich machen, wenn dieser eine umfassende datenschutzrechtliche Einwilligung abgibt, die auch die Datenverarbeitung zu Werbezwecken umfasst. Facebook beispielsweise gewährt die Nutzung seines Sozialen Netzwerks nur nach vorher erteilter datenschutzrechtlicher Einwilligung und erzielt Milliardengewinne mit dem Anbieten von Werbeplätzen. In dieser Beziehung ist also gerade die Kopplung von der Nutzung des Netzwerks und der Erteilung einer Einwilligung in die Datenverarbeitung zu Werbezwecken das entscheidende Element. Der IT-Dienstleister erbringt die „kostenlosen" Dienste erkennbar in der Erwartung, Nutzerdaten generieren und für Werbezwecke verwerten zu können[78]. Bislang ist diese Verknüpfung noch wirksam möglich, da die Möglichkeit eines anderen Zugangs für den Nutzer zu gleichwertigen

77 OLG Brandenburg, Urt. v. 11.1.2006, CR 2006, 490.
78 Melan/Wecke, DStR 2015, 2267 (2268).

vertraglichen Leistungen i.S.d. § 28 Abs. 3b BDSG für den Bereich der Sozialen Netzwerke noch als gegeben anzusehen ist[79].

Für die Realisierung des Datenhandels ist es außerdem unerlässlich, dass der Betroffene Rechte an seinen personenbezogenen Daten auf den Vertragspartner übertragen kann. Die Parteien haben ein Interesse daran, dass der Persönlichkeitsträger der datenverarbeitenden Stelle eine gesicherte Rechtsposition einräumen kann. Mittels vertraglich erteilter Einwilligung vermittelt der Persönlichkeitsrechtsträger dem Einwilligungsempfänger jedoch nur eine schuldrechtliche Befugnis zur Datenverarbeitung. Schuldrechtliche Ansprüche wirken stets nur zwischen den betreffenden Parteien, sodass der Datenverarbeiter seine Rechte nicht Dritten entgegenhalten kann. Gerade die Exklusivität der Datenverarbeitung lässt sich folglich mithilfe der datenschutzrechtlichen Einwilligung nicht befriedigend herstellen. So trägt die datenverarbeitende Stelle selbst bei der schuldrechtlichen Einräumung einer exklusiven Verwertungsbefugnis stets das Risiko einer konkurrierenden Nutzung. Für den Datenverarbeiter wäre das Recht umso wertvoller, wenn er bei einer unzulässigen Kommerzialisierung durch Dritte gegen diese vorgehen könnte. Die mangelnde rechtliche Verfügungsmöglichkeit über personenbezogene Daten behindert die Wahrnehmung von vermögensrechtlichen Interessen aller Beteiligten, auch denen der Persönlichkeitsträger.

3. Prinzip der undifferenzierten und alternativlosen Einwilligung

Es ist zu kritisieren, dass die datenschutzrechtliche Einwilligung regelmäßig nach dem „Alles oder nichts"-Prinzip erfolgt, das heißt, dass der Nutzer einer vorformulierten, undifferenzierten und alternativlosen Einwilligung zustimmen muss, um die gewünschte Leistung zu erhalten. Die datenschutzrechtliche Einwilligung birgt als „Zahlungsmittel" ein erhebliches Missbrauchspotenzial in sich[80]. Dies liegt insbesondere an der mangelnden Transparenz über das Verhältnis, in dem Leistung und Gegenleistung

79 Facebook hat im Bereich der Social-Media-Portale einen Marktanteil von 76,34 % (Quelle: http://de.statista.com/statistik/daten/studie/241601/umfrage/marktanteile-fuehrender-social-media-seiten-weltweit/).

80 Buchner, DuD 2010, 39 (40).

zueinander stehen. Bei manchen Daten mag der Wert momentan noch als gering einzustufen sein, jedoch können sich in der Zukunft und in Kombination mit anderen Daten weitere Nutzungsmöglichkeiten ergeben. Wie viel genau die eigenen Daten wert sind, kann der Nutzer nicht abschätzen. Dies führt dazu, dass umfassende Einwilligungserklärungen für geringe Prämien oder Werbegeschenke erteilt werden. Dennoch ist hervorzuheben, dass es auch für die datenverarbeitenden Unternehmen keine Alternative zum Erlaubnistatbestand der Einwilligung gibt. Wünschenswert wäre es, ein Konzept zu entwickeln, bei dem individuelle Ausgestaltungen realisierbar sind. Es sollte dem Betroffenen möglich sein, stärker Einfluss zu nehmen und ein eigenes Regelungsregime mit den gewünschten Rechtsfolgen zu entwerfen.

4. Zeitliche Unbegrenztheit der Einwilligung

Ein ganz zentraler Nachteil der datenschutzrechtlichen Einwilligung für die Betroffenen ist ihre zeitliche Unbegrenztheit. Ein gewisser Schutz für den Einzelnen ergibt sich aus dem Anspruch auf Löschung bei Zweckerreichung und aus der grundsätzlichen Widerrufsmöglichkeit. Der Löschungsanspruch ist aber ein stumpfes Schwert, da viele Betroffene weder Kenntnis von der Identität der datenverarbeitenden Stelle haben, noch der Zweck der Datenerhebung klar definiert wurde und der Nutzer daher erst recht den Zeitpunkt der Zweckerreichung nicht bestimmen kann. Zur Wahrnehmung ihrer Widerrufsmöglichkeit müssten die Betroffenen aktiv einen Überblick über alle erteilten datenschutzrechtlichen Einwilligungen erhalten und überprüfen, ob sie mit der Datenverarbeitung (noch) einverstanden sind oder ob sie von ihrem Widerrufsrecht Gebrauch machen möchten. In dieser Hinsicht wird zu viel von den Nutzern verlangt, und die Verantwortung liegt zu wenig auf Seiten der profitierenden Unternehmen.

5. Mangelnde Informiertheit und mangelnde Freiwilligkeit

Nach § 4a Abs. 1 S. 2 BDSG obliegt der verantwortlichen Stelle eine Hinweispflicht gegenüber dem Betroffenen über den vorgesehenen Zweck der Datenerhebung, -verarbeitung und -nutzung sowie – soweit nach den Umständen des Einzelfalls erforderlich oder auf Verlangen – über die Folgen der Verweigerung der Einwilligungserteilung. Nur wenn der Betroffene über Art und

Umfang des Datenumgangs informiert ist, besteht für ihn die Möglichkeit, eine fundierte Entscheidung zu treffen und sein Recht auf informationelle Selbstbestimmung in seinem Sinne auszuüben. Wird der Persönlichkeitsrechtsträger nicht angemessen aufgeklärt, ist eine wirksame Einwilligungserteilung nicht möglich und eine abgegebene Erklärung unwirksam. Die Informiertheit als Grundvoraussetzung für eine wirksame Einwilligung ist in ihrer Umsetzung indes mangelhaft. Viele verantwortliche Stellen wollen eine möglichst unbewusste Handlung der Nutzer erreichen und kommen daher ihrer gesetzlichen Informationspflicht nicht ausreichend nach.

Auch die Freiwilligkeit der Einwilligungserteilung ist in tatsächlicher Hinsicht aufgrund sozialer oder wirtschaftlicher Abhängigkeiten oft nicht gegeben. Die Freiwilligkeit ist vielfach bloße Fiktion, denn um gewünschte Leistungen zu erhalten, besteht häufig keine Alternative zur Erteilung einer datenschutzrechtlichen Einwilligung. Viele Unternehmen machen die Zustimmung der Kunden zur Nutzung ihrer Daten zur Bedingung eines Vertragsschlusses – selbst wenn die Datenverwendung für die Durchführung des Vertrags gar nicht notwendig ist. In Fällen von bestehenden Machtungleichgewichten bedarf es dringend gesetzlicher Regelungen zur Sicherstellung der Datenherrschaft der Betroffenen.

V. Keine rechtliche Zuordnung von Daten im aktuellen Datenschutzrecht

Wie bereits erläutert, gewährt das Recht auf informationelle Selbstbestimmung dem Einzelnen ein Bestimmungsrecht über die auf seine Person bezogenen Daten. Dieses Bestimmungsrecht soll nach dem Bundesverfassungsrecht aber nicht als Recht des Einzelnen „im Sinne einer absoluten, unbeschränkbaren Herrschaft" missverstanden werden. Eine alleinige Zuordnung aller Rechte an einem Datum zum Betroffenen ist wegen entgegenstehender Rechte Dritter und einer Störung des Kommunikationsprozesses nicht möglich – das Recht des Einzelnen ist allgemeinpflichtig ausgestaltet und stets Gegenstand einer Interessenabwägung[81].

81 Siehe bereits unter D.II.1.

Dennoch ist es notwendig, klar zu regeln, wem welche Rechte an personenbezogenen Daten zustehen. Mit dem Aufkommen von Big-Data-Anwendungen stellt sich die Frage, wem Daten „gehören" und in welchem Umfang Nutzungsrechte an Daten bestehen. Da der Gesetzgeber bei der Schaffung des BDSG jedoch primär die ideellen Interessen des Persönlichkeitsträgers im Blick hatte, steht die Abwehr einer unerwünschten und unzulässigen Datenverarbeitung im Vordergrund. Das BDSG sieht daher ein grundsätzliches Verbot der Datenverarbeitung mit einzelnen Ausnahmen vor. Es ist im Zusammenhang mit der wirtschaftlichen Verwertung von Daten teilweise unklar, wem in welchem Umfang positive Verwertungsrechte zustehen.

Exemplarisch kann dies am Beispiel der Entwicklung rund um das Smart Car gezeigt werden. Hier stellt sich die Frage, wer Rechte an den erhobenen Daten geltend machen kann. Zum einen kommt der Fahrzeughersteller in Betracht, der die datenerhebende Technik in das Fahrzeug eingebaut und in der Regel auch den eigenen Zugriff auf die Daten technisch sichergestellt hat. Dann kommt der Eigentümer des Fahrzeugs in Betracht, also derjenige, dessen Sache Objekt der Beobachtung ist. Außerdem kommt der Fahrer des Fahrzeugs in Betracht, da die erhobenen Daten nicht nur Aussagen über das Fahrzeug treffen, sondern auch eine Profilbildung über den Fahrer zulassen und dieser damit ebenfalls Gegenstand der Betrachtung ist. Darüber hinaus können Werkstätten und Zulieferer Interesse an den technischen Daten haben, um die Funktionsfähigkeit einzelner Fahrzeugteile zu überprüfen und gegebenenfalls Fernwartungen durchzuführen. Da es zunehmend Kooperationen mit Konzernen der Unterhaltungsindustrie gibt, werden nicht zuletzt auch Anbieter von Multimedia-Anwendungen Interesse an den personenbezogenen Daten geltend machen.

Da es bislang kein Eigentum an Daten gibt, entscheidet allein das Faktische über die Möglichkeit zur Verwertung. Wer in den Besitz von Daten gelangt ist, kann diese nutzen und anderen vorenthalten – bei personenbezogenen Daten ist allerdings zusätzlich die datenschutzrechtliche Einwilligung des Betroffenen einzuholen. Auch Unternehmen wünschen sich mehr Rechtssicherheit im Umgang mit personenbezogenen Daten und haben ein Interesse an der Normierung verkehrsfähiger Rechte an Daten. Dabei stellt sich die Frage, ob Unternehmen durch Verknüpfung, Verarbeitung

oder Analyse selbst Rechte an den gewonnenen Daten beziehungsweise Analyseergebnissen geltend machen können. Diese Rechte könnten mit den Rechten der Betroffenen an dem Schutz ihrer Privatsphäre kollidieren. Es gibt bereits einen urheberrechtlichen Datenbankschutz, sofern die Auswahl oder Anordnung der enthaltenen Elemente auf einer schöpferischen Leistung beruht[82]. Auch die Algorithmen zur Datenanalyse können geistiges Eigentum und Geschäftsgeheimnisse darstellen[83]. Zunehmend wird allerdings gefordert, dass die aus einer wirtschaftlichen Verwertung resultierenden Gewinne demjenigen gebühren, der als Betroffener im Sinne des BDSG anzusehen ist[84].

VI. Zwischenfazit

Zusammenfassend lässt sich festhalten, dass die momentane Praxis der Einholung einer datenschutzrechtlichen Einwilligung vielfach eher einer Täuschung oder einem Betrug gleichkommt. Häufig wird eine Überwindung der Nutzer-Selbstbestimmung angestrebt, und es erfolgt eine (emotionale) Beeinflussung zur Abgabe der Einwilligungserklärung und in der Folge zum Kauf gewisser Produkte oder zur Vornahme anderer von Unternehmen gewünschter Verhaltensweisen. Häufig wird bemängelt, dass der Nutzer im Netz zu einem Produkt wird und mit seinen personenbezogenen Daten zahlt. Jedoch kann bei Intransparenz und dem Fehlen einer willentlichen Entscheidung in Kenntnis aller Konsequenzen nicht von einem „Bezahlen" gesprochen werden. Bei der Ausübung ihres Grundrechts auf informationelle Selbstbestimmung versagt die breite Masse der Betroffenen. Dies deutet auf strukturelle Probleme hin, die dringend beseitigt werden müssen[85]. Eine Verletzung der Privatsphäre ist bisher nicht klar definiert und bleibt in vielen Fällen sanktionslos. Wir brauchen neue rechtliche Regelungen, die zu einer Ordnung führen, in der die Privatsphäre als hohes Gut geschützt werden kann, dieser Wunsch nach Schutz respektiert wird und

82 Vgl. § 87b UrhG.
83 Dreier, in: Dreier/Schulze (Hrsg.), UrhG, § 69a, Rn. 22; BGH GRUR 1991, 449.
84 Vgl. Zech, CR 2015, 137.
85 Baumann, MERKUR Mai 2015, 86ff.

dennoch der Datenhandel zugelassen sowie in kontrollierte Bahnen gelenkt wird. Wir benötigen einerseits eine Lockerung des Datenschutzrechts dergestalt, dass nicht jede Datenverarbeitung als unerwünscht betrachtet wird und auch ökonomische Interessen Berücksichtigung finden; andererseits eine Verschärfung dahingehend, dass es dem Einzelnen im Gegensatz zur derzeitigen Situation mit der vielfachen Umgehung datenschutzrechtlicher Regelungen leichter und effektiver möglich ist, seine ideellen Interessen zu schützen.

F. Aktuelle Ansätze zur Stärkung der Nutzer-Selbstbestimmung

Die hier beschriebenen Defizite im aktuellen Datenschutzrecht sind zum Teil seit Langem bekannt. Es gibt daher bereits verschiedene Ansätze, um die Rechte des Einzelnen zu stärken. Einige aktuelle Vorschläge sollen im Folgenden dargestellt werden.

I. Stärkung der informationellen Selbstbestimmung durch die Datenschutzgrundverordnung?

Um das Datenschutzrecht auf europäischer Ebene zu vereinheitlichen und grundlegende Minimalstandards für den Schutz personenbezogener Daten festzulegen, wird der Erlass einer europäischen Verordnung anvisiert. Die aktuellen Entwürfe für eine europäische Datenschutzgrundverordnung des Europäischen Parlaments[86] sowie des Rats der Europäischen Union[87] enthalten einige Neuerungen, wovon die wesentlichen nachstehend vorgestellt und hinsichtlich ihres Beitrags zu einer Stärkung der Nutzer-Selbstbestimmung bewertet werden. Alle vorgestellten Neuerungen gelten nach beiden Versionen mit Ausnahme des strengen Kopplungsverbots, das nur durch das Europäische Parlament vorgesehen ist. In einem informellen Trilog wird nun von Vertretern der Kommission, des Rats und des Parlaments angestrebt, sich auf einen gemeinsamen Gesetzestext zu einigen.

Das Instrument der Einwilligung soll gestärkt werden, indem klargestellt wird, dass eine solche ausdrücklich und informiert abgegeben werden muss. Hierfür soll insbesondere die Verständlichkeit von Informationen sichergestellt werden. Zur Gewährleistung eines angemessenen Schutzniveaus sind

86 Legislative Entschließung des Europäischen Parlaments vom 12. März 2014 zu dem Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (allgemeine Datenschutzverordnung) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)), abrufbar unter: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0212+0+DOC+XML+V0//DE.

87 Allgemeine Ausrichtung des EU-Rats zur Datenschutzgrundverordnung v. 15.6.2015, 9565/15, abrufbar unter: http://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/de/pdf.

u. a. technische und organisatorische Maßnahmen vorgesehen. Die Umsetzung des klassischen „Privacy by design"-Ansatzes ist positiv zu verbuchen; die Verwirklichung einer freiwilligen Einwilligung in Kenntnis aller Umstände dürfte ohne konkrete Regelungen und neue Konzepte allerdings ins Leere laufen. Da auch nach geltendem deutschen Recht die Einwilligung bereits freiwillig und informiert erfolgen sollte und in diesem Bereich Anspruch und Wirklichkeit auseinanderfallen, sind hier keine erheblichen Änderungen in der Praxis zu erwarten.

Darüber hinaus soll ein strenges Kopplungsverbot eingeführt werden, sodass die Erfüllung eines Vertrags oder die Erbringung einer Dienstleistung keinesfalls von einer nicht erforderlichen Einwilligung in die Datenverarbeitung abhängig gemacht werden darf. Dadurch wird bezweckt, dass niemand faktisch dazu gezwungen ist, einer Datennutzung zuzustimmen, welche für den Vertragsschluss oder die Vertragsdurchführung gar nicht erforderlich ist[88]. Damit würde jedoch auch der Datenhandel stark eingeschränkt werden, und es wäre stets unmöglich, statt Geld personenbezogene Daten als Gegenleistung anzubieten. Es sollte den Beteiligten aber freistehen, ob sie ihre Daten in kommerzieller Weise nutzen möchten. Weiterer Nachteil wäre, dass immer separate Datenüberlassungsverträge geschlossen werden müssten, die nicht im Zusammenhang mit einer anderen vertraglichen Leistung bzw. einem anderen Vertragsschluss stehen dürften. Gerade das bestehende Austauschverhältnis sollte jedoch auch rechtlich erfasst sein.

Ferner sollen die Rechte auf Auskunft, Korrektur und Löschung gestärkt werden, bspw. indem der Datenverarbeiter ein Verlangen nach Löschung auch an Drittparteien, denen die Daten übermittelt wurden, weiterleiten muss sowie das Verfahren zur Geltendmachung der Betroffenenrechte auch elektronisch durchgeführt werden kann. Darüber hinaus hat die Beantwortung eines Antrags innerhalb einer festgelegten Frist zu erfolgen. Bisher werden die Betroffenenrechte viel zu selten ausgeübt, doch diese Maßnahmen könnten dazu führen, dass in Zukunft mehr Anfragen von Seiten der Nutzer gestellt werden. Nach dem „One-Stop Shop"-Prinzip müssen sich Bürger bei Datenschutzverstößen in der gesamten EU nur noch an die

88 Seidel, ZG 2014, 153 (156).

Datenschutzbehörde in ihrem Mitgliedstaat wenden. Auch dies erleichtert die Wahrnehmung der Betroffenenrechte.

Verantwortliche Stellen und Auftragsdatenverarbeiter[89] werden verpflichtet, im Vorfeld der Datenverarbeitung eine Risikoanalyse und eine datenschutzrechtliche Folgenabwägung vorzunehmen und bei besonderen Risiken die Datenschutzaufsichtsbehörde zu unterrichten, die eine Untersagung aussprechen kann. Es ist jedoch zu befürchten, dass Unternehmen kaum freiwillig Risiken eingestehen und sich eine Untersagung einhandeln werden. Diese Maßnahme wird folglich nur Erfolg haben, wenn eine hinreichende Kontrolle der datenschutzrechtlichen Maßnahmen von verantwortlichen Unternehmen gewährleistet ist. Problematisch ist, dass hier wiederum die Aufsichtsbehörden in der Verantwortung sind und diese nicht über ausreichend Sach- und Finanzmittel verfügen.

Die unzureichenden Kontrollen und die schwachen Sanktionen wurden bereits bemängelt. Zu einer Verbesserung der Kontrolltätigkeit[90] soll ein europäischer Datenschutzausschuss eingerichtet und die Sanktionen sollen deutlich verschärft werden[91]. Positiv ist, dass diese Sanktionen so schmerzlich sein dürften, dass Unternehmen Datenschutzverstöße nicht mehr so einfach einkalkulieren werden. Weitere Vorteile sind, dass nach dem Entwurf auch die Auftragsdatenverarbeiter gegenüber den Betroffenen haften, ein Schadensersatz für immaterielle Schäden normiert und ein Verbandsklagerecht eingeführt wird.

Einer der bedeutendsten Fortschritte ist die Einführung des Marktortprinzips, d. h., die Vorschriften der DSGVO gelten für alle, die ihre Dienste innerhalb der EU anbieten, unabhängig davon, ob die Datenverarbeitung

89 Eine Auftragsdatenverarbeitung liegt nach § 11 Abs. 1 BDSG vor, wenn personenbezogene Daten im Auftrag durch andere Stellen erhoben, verarbeitet oder genutzt werden. Im Rahmen der Auftragsdatenverarbeitung ist der Auftraggeber für die Einhaltung der Vorschriften des Bundesdatenschutzgesetzes und anderer Vorschriften über den Datenschutz verantwortlich.

90 Nach dem Ratsentwurf ist die Benennung eines unabhängigen Datenschutzbeauftragten jedoch im Gegensatz zum Entwurf des Europäischen Parlaments nicht obligatorisch; eine Pflicht zu dessen Bestellung kann allerdings durch nationales Recht angeordnet werden.

91 Das Europäische Parlament sieht gegenüber dem Europäischen Rat deutlich höhere Bußgelder vor.

außerhalb der EU stattfindet. Dies ist ganz wesentlich, da sich dann auch amerikanische Konzerne dem europäischen Datenschutzniveau anpassen müssen.

Vorgesehen ist ferner eine freiwillige Datenschutzzertifizierung, mit der Auftragsdatenverarbeiter nachweisen können, dass die Datenverarbeitung im Einklang mit den Vorgaben der Verordnung erfolgt. Es bleibt aber die Problematik, welche Stelle nach erfolgter Zertifizierung weiterhin effektiv die Einhaltung des Datenschutzniveaus kontrolliert.

Besonders erfreulich zur Förderung des Wettbewerbs unter Diensteanbietern ist die Einführung des Rechts auf Datenportabilität. Dieses ermöglicht es dem Nutzer, eine elektronische Kopie seiner Daten zu erhalten und bei einem Wechsel des Anbieters auf einfache Art und Weise diese Daten „mitzunehmen"[92].

Für eine Datenübermittlung in Drittländer hat die Artikel-29-Datenschutzgruppe Binding Corporate Rules eingeführt. Dies sind (unternehmens)interne Richtlinien zum Umgang mit personenbezogenen Daten, die internationalen Organisationen und Konzernen bei einem dadurch herbeigeführten angemessenen Datenschutzniveau eine legale Datenübermittlung in Drittstaaten ermöglichen[93]. Das Instrument der Binding Corporate Rules soll nun auch in der Datenschutzgrundverordnung verankert und dadurch insgesamt gestärkt werden. Auch bei diesem Verfahren ist ausschlaggebend, dass die Umsetzung der Richtlinien und das konstante Vorliegen eines hohen Datenschutzniveaus hinreichend kontrolliert werden.

Abschließend lässt sich sagen, dass die geplante DSGVO einige Verbesserungen mit sich bringt, insgesamt jedoch nicht bahnbrechend und fortschrittlich genug ist. Daten werden noch nicht als Wirtschaftsgüter begriffen, und es stehen weiterhin die ideellen Interessen der Betroffenen im Fokus der Regelungen. Ferner wird an dem Instrument der Einwilligung zur Realisierung der Nutzer-Selbstbestimmung festgehalten.

92 Giurgiu, CCZ 2012, 226 (228); nach Art. 15 Abs. 1b des Ratsentwurfs der DSGVO kann allerdings für das Zurverfügungstellen eine nicht überhöhte Gebühr verlangt werden.

93 Grapentin, CR 2009, 693f.

II. Konzepte zur Sicherstellung der Datenhoheit in der Praxis

Um die informationelle Selbstbestimmung des Einzelnen in der Praxis sicherzustellen, sind verschiedene organisatorische Maßnahmen denkbar.

1. Bürgerkonto

Das persönliche Bürgerkonto ist ein Angebot diverser Verwaltungseinheiten, Online-Services unkompliziert zu nutzen. Vielen Bürgern ist es schwer zu vermitteln, warum sie sich für unterschiedliche Verwaltungsvorgänge stets erneut identifizieren und erneut Angaben tätigen müssen. Nur in 48 % der Fälle nutzen öffentliche Verwaltungen in Europa Angaben, die sich ohnehin in ihrem Besitz befinden, ohne erneute Abfrage[94]. Auch die Strategie für einen digitalen Binnenmarkt für Europa sieht die Einführung des Prinzips „Once only" vor, sodass Bürger künftig nur noch einmalig ihre Daten der Verwaltung zur Verfügung stellen müssen[95].

Mittels eines Bürgerkontos lässt sich ein über Benutzername und Kennwort geschützter Bereich einrichten. Die dort hinterlegten Daten können für verschiedene Verwaltungsdienstleistungen genutzt und Formulare können automatisch mit bereits bekannten Informationen befüllt werden. Besonders einfach lässt sich ein Bürgerkonto mit der eID-Funktion des neuen Personalausweises anlegen – zumal der Nutzer dann auch seine Identifikation verifizieren kann –, jedoch kann das Konto auch klassisch mittels Eingabe der Daten erstellt werden.

Diese Idee eines Datenpools über Basisdaten lässt sich ebenfalls auf die freie Wirtschaft übertragen. Der Betroffene kann auf dem Server bzw. bei dem App-Anbieter seines Vertrauens ein Profil anlegen, bei dem alle relevanten, sich auf ihn beziehenden Daten gespeichert werden. Wollen Unternehmen nun Zugriff auf gewisse Daten haben, müssen sie die Freigabe des Zugangs zu gewissen Bereichen des Profils erbitten. In einem solchen Profil könnte man auch protokollarisch speichern, welche Datenverarbeiter zu welchem Zweck Daten erhalten haben.

---

94 Strategie für einen digitalen Binnenmarkt für Europa, abrufbar unter: http://ec.europa.eu/priorities/digital-single-market/docs/dsm-communication_de.pdf.

95 Strategie für einen digitalen Binnenmarkt für Europa, abrufbar unter: http://ec.europa.eu/priorities/digital-single-market/docs/dsm-communication_de.pdf.

2. Algorithmen-Kontrolle

Die immensen Datenbestände werden vielfach automatisch mittels Algorithmen analysiert. Ein Algorithmus ist ein Rechenvorgang nach einem bestimmten, sich wiederholenden Schema[96] bzw. eine Verfahrensanweisung, die in einer wohldefinierten Abfolge von Schritten zur Problemlösung führt[97]. Bei der Entwicklung von Algorithmen werden diverse Kriterien mit unterschiedlicher Gewichtung berücksichtigt, und es besteht stets die besondere Gefahr einer Diskriminierung und eines wettbewerbsverzerrenden Verhaltens. Auch in diesem Bereich muss ein schonender Ausgleich zwischen den möglichen Beeinträchtigungen der Entfaltungschancen des Einzelnen aufgrund einer algorithmenbasierten Auswertung von Daten und gleichzeitig den Interessen der Unternehmen an der Datenverarbeitung und der Geheimhaltung ihrer Algorithmen gefunden werden.

Aufgrund des hohen Gefährdungspotenzials algorithmenbasierter Analysen für die informationelle Selbstbestimmung ist es nach § 6a BDSG verboten, belastende Entscheidungen allein auf eine automatisierte Verarbeitung personenbezogener Daten zur Bewertung von Persönlichkeitsmerkmalen zu stützen. Ferner steht dem Einzelnen ein Auskunftsanspruch über zugrunde liegende Angaben und Bewertungsmaßstäbe zu. Mit Rücksicht auf etwaige Geschäfts- und Betriebsgeheimnisse sind technische Einzelheiten, die konkreten Analysemethoden und der Quellcode hingegen nicht von dem Auskunftsrecht erfasst. Um umfassende Transparenz herzustellen, werden zunehmend eine Verschärfung der Offenlegungspflichten und konkret die Preisgabe von Algorithmen bspw. von Google verlangt[98]. Zur Gewährleistung informationeller Selbstbestimmung sollten Betroffene Kenntnis über die konkrete Weiterverwendung der gespeicherten personenbezogenen Daten erlangen.

Google stand bereits im Verdacht, seine marktbeherrschende Stellung auszunutzen; zur Abwendung einer Geldbuße hat sich das Unternehmen

96 http://www.duden.de/rechtschreibung/Algorithmus.

97 http://wirtschaftslexikon.gabler.de/Definition/algorithmus.html.

98 Schultz, Sorge vor Kartell: Maas hätte gerne, dass Google geheime Suchformel offenlegt, abrufbar unter: http://www.spiegel.de/wirtschaft/unternehmen/google-heiko-maas-fordert-offenlegung-von-algorithmus-a-991799.html.

verpflichtet, seinen Algorithmus so zu ändern, dass Konkurrenzdienste deutlich sichtbarer angezeigt werden[99]. Für eine grundlegende Kontrolle von Algorithmen würde sich eine entsprechende Einführung des „In-camera"-Verfahrens nach § 99 Abs. 2 VwGO anbieten, bei dem geheimhaltungsbedürftige Informationen nur dem Gericht offengelegt werden und deren Geheimhaltungsbedürftigkeit überprüft wird. Jedoch wird es in tatsächlicher Hinsicht für die Gerichte immer anspruchsvoller – trotz der Zuhilfenahme von Sachverständigen –, komplexe Technologien zu überprüfen. Auch wenn man an der datenschutzrechtlichen Einwilligung festhält, sollte sich diese explizit auf das Zusammenführen von Daten und deren Auswertung mithilfe von Algorithmen beziehen.

3. Aktive Informationspflicht datenverarbeitender Stellen

Bereits vor einigen Jahren forderte der Chaos Computer Club (CCC) die Einführung eines Datenbriefs zur Stärkung der informationellen Selbstbestimmung von Nutzern und zur Eindämmung der massenhaften Speicherung personenbezogener Daten[100]. In regelmäßigen Abständen sollen datenverarbeitende Stellen aktiv den Betroffenen kostenlos per Brief über die Erhebung, Speicherung, Verarbeitung oder Übermittlung personenbezogener Daten informieren. Durch dieses Instrument wird Transparenz hergestellt, die zu einem bewussteren Umgang der Betroffenen mit personenbezogenen Daten führen könnte. Gegebenenfalls werden Nutzer in der Folge öfter einen Widerspruch oder eine Korrektur veranlassen. Durch aktive Information könnte die Angst der Nutzer vor Datensammlungen gelindert und die Mündigkeit der Betroffenen gefördert werden. Der Mehraufwand soll dazu führen, dass Unternehmen die langfristige Datenspeicherung kritisch überprüfen. Der damalige Bundesbeauftragte für den Datenschutz Peter Schaar hielt einen jährlichen gedruckten Datenauszug für sinnvoll, forderte jedoch darüber hinaus in Weiterentwicklung des Datenbriefs eine Datenschutz-App,

99 http://www.wiwo.de/technologie/digitale-welt/milliardenstrafe-abgewendet-google-und-die-eu-sind-sich-einig/9436322.html.

100 http://www.ccc.de/datenbrief.

mittels derer sich die gespeicherten Daten in kürzeren Abständen vom Smartphone aus einsehen lassen[101].

Mittlerweile würde sich in der Tat eher eine Auskunft auf elektronischem Weg anbieten, jedoch ist die Kernaussage der Notwendigkeit einer proaktiven Informationstätigkeit nach wie vor hochaktuell. Im Bereich der Verarbeitung personenbezogener Daten bedarf es dringend Regelungen zur Beseitigung der herrschenden Intransparenz. Nach dem geltenden Recht müssen die Betroffenen gezielt datenverarbeitende Stellen um Auskunft bitten und ihre eigene Identität nachweisen. Ein Umdenken dergestalt, dass die Nutznießer der Datenverarbeitung stärker in die Pflicht genommen werden, indem ihnen eine Mitteilungspflicht auferlegt wird, ist erforderlich.

Auch nach dem Entwurf der Datenschutzgrundverordnung ist jede verantwortliche Stelle verpflichtet, unaufgefordert die festgeschriebenen Informationen mitzuteilen. Darüber hinaus sind die Informationspflichten der verantwortlichen Stellen inhaltlich ausgeweitet worden. Bedauerlicherweise ist jedoch keine wiederkehrende Wiederholung der proaktiven Mitteilung vorgesehen.

4. Mikrobezahlsystem

Lanier sieht es sehr kritisch, dass die Nutzer im Netz ihre Informationshoheit zunehmend verlieren bzw. abgeben. Besonders die Arbeitsplatzvernichtung durch den Strukturwandel sieht er als großes Problem an. Er meint, das Internet werde zum Herrschaftsinstrument, welches einigen wenigen die Macht gebe, alle anderen auszubeuten.

Er plädiert für eine humanistische Informationsökonomie, bei der die Datenwertschöpfung allen zugutekommt. Es solle keine Gratiskultur im Netz mehr geben, sondern ein Mikrobezahlsystem für alle Informationen. Dies stärke die Wahrnehmung von Daten und Informationen als wirtschaftliche Werte. Dann müssten zwar Nutzer für Daten und Informationen zahlen, jedoch umgekehrt auch die großen Konzerne für die Daten des Einzelnen. Dies führe auch zu einem umsichtigeren Umgang mit personenbezogenen Daten, da Unternehmen sich diese nur noch einholen werden, wenn sich

101 Schmidt, Ein Datenbrief fürs Handy, abrufbar unter: http://www.taz.de/!5139557/.

dies auch wirklich rentiert[102]. Dieses Modell ist zum einen aber technisch schwer umsetzbar, und zum anderen werden die Internetkonzerne kaum freiwillig ihren Wettbewerbsvorteil, den sie durch den alleinigen Besitz immenser Datenmengen haben, aufgeben.

5. Selbstdatenschutz

Grundsätzlich wäre es zu begrüßen, wenn der Staat Nutzer in die Lage versetzt, sich eigenverantwortlich selbst zu schützen. Im Sinne der informationellen Selbstbestimmung bedarf es Instrumenten zur Realisierung einer Datenverarbeitung in dem persönlich favorisierten Maße. Von allen etablierten politischen Parteien wird das Konzept „Datenschutz durch Medienkompetenz" als tragendes Konzept ihrer Datenschutzpolitik befürwortet[103]. Bürger sollen einen bewussten Umgang mit personenbezogenen Daten erlernen und in der Lage sein, in Eigenverantwortung ihre Privatsphäre zu schützen. Medienkompetente Nutzer können durch bestimmte Nutzereinstellungen und Verschlüsselungstechniken sowie Anonymisierung einen gewissen Schutz erreichen. Jedoch braucht es enormes technisches Wissen und technische Fähigkeiten, über die der Durchschnittsnutzer nicht verfügt und welche er nur mit erheblichem Aufwand erlernen kann. Auch aufgeklärte Betroffene werden sich nicht umfassend, beispielsweise im Hinblick auf den Zeitaufwand bezüglich der Kenntnisnahme diverser allgemeiner Geschäftsbedingungen, schützen können. Eine gewisse Eigenverantwortung muss und kann auch im Bereich des Datenschutzes existieren, aber sofern nicht ein gewisser Datenschutz normiert und von Seiten des Staates hergestellt wird, stoßen auch aufgeklärte und umsichtige Nutzer an ihre Grenzen.

---

102 Bartels, Jaron Lanier und die Gratiskultur im Internet – Nichts darf umsonst sein, abrufbar unter: http://www.tagesspiegel.de/kultur/jaron-lanier-und-die-gratiskultur-im-internet-nichts-darf-umsonst-sein/9873822.html.

103 Baumann, MERKUR Mai 2015, 86 ff; https://www.spd.de/linkableblob/96686/data/20130415_regierungsprogramm_2013_2017.pdf, S. 64 f.; https://www.cdu.de/system/tdf/media/dokumente/071203-beschluss-grundsatzprogramm-6-navigierbar.pdf?file=1, S. 45; http://www.gruene-bundestag.de/fileadmin/media/gruenebundestag_de/fraktion/beschluesse/medienkompetenz.pdf; http://www.linksfraktion.de/themen/medienkompetenz/; http://www.fdp.de/files/408/B_rgerprogramm_A5_Online_2013-07-23.pdf, S. 49f.

6. Nutzerunterstützung durch automatisierte Analyse der Vertrauenswürdigkeit

Zur Unterstützung des Nutzers beim Surfen im Web könnte ein Browser-Add-on durch das Internet begleiten und automatisiert besuchte Websites auswerten. Als Maßstab für die Vertrauenswürdigkeit eines Anbieters soll die Einhaltung von Regelungen zum Schutz des Nutzers und eine mangelnde Berücksichtigung allein der Anbieterinteressen zu Lasten der Nutzerinteressen dienen. Mithilfe einer automatisierten Einschätzung könnten Hinweise auf einzelne Risiken gegeben werden. Dabei ist klarzustellen, dass eine derartige Analyse lediglich der Unterstützung einer eigenen Einschätzung dienen kann und nicht fehlerfrei ist. Bei der Analyse werden formale, inhaltliche und technische Anforderungen gestellt. Neben dem Datenschutz sollte auch die IT-Sicherheit Berücksichtigung finden. Die einzelnen Anforderungen sind dann nach ihrem Risiko (ggf. nach individualisierten Gewichtungen) in ein Verhältnis zueinander zu setzen. Wichtig ist, dem Nutzer die Warnhinweise in einer Art und Weise aufzubereiten, dass dieser sie auch versteht und eine konkrete Handlungsempfehlung daraus ableiten kann[104]. Man könnte ähnlich einem Ampelsystem zunächst eine grobe Einschätzung abgeben und nur bei Interesse des Nutzers vertiefende Hinweise und Erläuterungen zur Verfügung stellen. Bei einem sensibleren Umgang der Nutzer mit ihren Daten könnte von einem derartigen System eine erhebliche Prangerwirkung ausgehen, sodass Betreiber von als mangelhaft eingestuften Websites zu einer Überarbeitung gezwungen wären.

104 Boos/Roßnagel, MMR 2015, 215ff.

G. Mögliche Neugestaltung des Datenrechts

Nachstehend werden Konzepte vorgestellt und untersucht, die den aufgezeigten Schwächen des aktuellen Datenschutzrechts Abhilfe leisten könnten. Jedoch ist voranzustellen, dass lediglich Denkanstöße gegeben werden können und eine Patentlösung für den Umgang mit Daten in wirtschaftlicher Hinsicht nicht existiert.

I. Dateneigentum

Aufgrund der enormen wirtschaftlichen Bedeutung von Daten ist die Frage nach dem Eigentum bzw. sonstigen Rechten an Daten wesentlich, da nur der Berechtigte den wirtschaftlichen Wert für sich fruchtbar machen kann. Bisher gibt es keine Rechtspositionen mit dinglicher Wirkung im deutschen Datenschutzrecht; Rechte zur Nutzung werden durch schuldrechtliche Vereinbarungen eingeräumt. Das BDSG gibt keinen Anlass dazu anzunehmen, dass Daten über die bestehenden Schutzmechanismen hinaus in ihrer vermögenswerten Komponente von Ausschließlichkeitsrechten erfasst sein sollen. Jedoch besteht mit dem Datenhandel ein gewisses Bedürfnis danach, dass die Daten den betroffenen Personen auch als Vermögensrecht durch das Gesetz zugewiesen werden. Da Daten wirtschaftliche Werte darstellen können, muss auch das Zivilrecht einen angemessenen Schutz für den Einzelnen bereitstellen. Um bestehende Schutzlücken im Datenschutzrecht zu schließen, wird eine Analogie zu dem zivilrechtlichen Sacheigentum im Sinne des § 903 BGB in Erwägung gezogen.

Zunächst soll ein Überblick über die Rechtsprechung im Hinblick auf die Anerkennung des Schutzes kommerzieller Interessen im Zusammenhang mit Datenverarbeitung gegeben werden.

Der Bundesgerichtshof (BGH) beschäftigte sich bislang vorwiegend mit der Kommerzialisierung von Eigenbild und Namen, die ebenfalls Teilbereiche des allgemeinen Persönlichkeitsrechts darstellen; die entwickelten Grundsätze lassen sich in ihrer Grundwertung aber auch auf personenbezogene Daten übertragen. Schon früh erkannte der BGH, dass das grundrechtliche allgemeine Persönlichkeitsrecht eines zivilrechtlichen Schutzes bedarf, und sprach dem Kläger in der sogenannten

Leserbriefe-Entscheidung[105] einen deliktischen Anspruch gerichtet auf Widerruf zu. Mit der Dahlke-Entscheidung[106] wurde das Recht am eigenen Bild, welches einen Teilbereich des allgemeinen Persönlichkeitsrechts darstellt, vom BGH als vermögenswertes Ausschließlichkeitsrecht bezeichnet. Bei einem unzulässigen Eingriff in dieses Recht kann der Betroffene je nach Einzelfall einen Vermögensschaden erleiden, der auf Grundlage der üblichen Lizenzgebühr berechnet werden kann. Bei der Schadensberechnung legte der BGH die gleichen Erwägungen zugrunde wie bei der Verletzung von Urheber- und Patentrechten.

In der Nena-Entscheidung[107] war zentrales Kernelement die Übertragbarkeit der vermögenswerten Bestandteile des allgemeinen Persönlichkeitsrechts – der BGH hat jedoch die Frage der Übertragbarkeit offen gelassen, indem er eine Verletzung des übertragbaren exklusiven Nutzungsrechts angenommen hat. Im Marlene-Dietrich-Urteil[108] wurde die bisherige Rechtsprechung zur Selbstbestimmung über die wirtschaftliche Verwertung noch einmal bestätigt und bestärkt; der BGH betonte erneut, dass das allgemeine Persönlichkeitsrecht vermögenswerte Bestandteile aufweist. Die kommerzielle Verwertung sei ein Reflex der Rechtsordnung, der sich aus bestehenden datenschutzrechtlichen Vorschriften ergebe. Ferner wurde die Vererbbarkeit vermögenswerter Bestandteile des Rechts am eigenen Bild und Namen bejaht, während die Frage nach einer Übertragung unter Lebenden erneut ausdrücklich offen gelassen wurde. Die Anerkennung der Vererblichkeit sei notwendig gewesen, um hinreichenden Schutz vor einer kommerziellen Verwertung durch Nichtberechtigte zu gewährleisten.

Während zunächst der Vermögensschaden des Betroffenen im Vordergrund stand, wurde schließlich auch der Ersatz immaterieller Schäden Gegenstand der BGH-Rechtsprechung. Im Herrenreiter-Fall[109] sah der BGH einen Nichtvermögensschaden als gegeben an und führte aus, dass die Berechnung des Schadens auf dem Wege der Fiktion eines abgeschlossenen

105 BGH, Urteil v. 25.5.1954, NJW 1954, 1404ff.
106 BGH, Urteil v. 8.5.1956, NJW 1956, 1554ff.
107 BGH, Urteil v. 14.10.1986, NJW-RR 1987, 231ff.
108 BGH, Urteil v. 1.12.1999, NJW 2000, 2195ff.
109 BGH, Urteil v. 14.2.1958, NJW 1958, 827ff.

Lizenzvertrags in diesem Fall zu einer weiteren Persönlichkeitsverletzung führe, da man unterstelle, der Betroffene hätte sich für einen bestimmten Betrag auch freiwillig in diese Lage gebracht. Im Mephisto-Urteil[110] wurde klargestellt, dass auch immaterielle Güter den Tod überdauern können. In der Konsequenz bestehe ein persönlichkeitsrechtlicher Unterlassungsanspruch Verstorbener gegen grobe Entstellungen des Lebensbildes. Problematisch war, dass auch die ideellen Komponenten des allgemeinen Persönlichkeitsrechts ursprünglich nicht durch das BGB geschützt wurden und dieser Schutz erst durch eine Analogie zu § 847 BGB a. F. beziehungsweise anschließend direkt durch das Grundgesetz im Wege richterlicher Rechtsfortbildung[111] hergeleitet wurde.

Das Bundesverfassungsgericht verneint den grundrechtlichen Schutz der materiellen Bestandteile des allgemeinen Persönlichkeitsrechts. Mit der Entscheidung Caroline von Monaco[112] betonte das BVerfG den Umstand, dass keine grundrechtliche Verbürgung der materiellen Interessen an der Persönlichkeit bestehe. In der Entscheidung Marlene Dietrich[113] erläuterte das BVerfG, dass es unschädlich sei, wenn das zivilrechtliche allgemeine Persönlichkeitsrecht anders ausgestaltet sei als das verfassungsrechtliche allgemeine Persönlichkeitsrecht.

Es ist allgemein anerkannt, dass auch die vermögenswerten Bestandteile des Persönlichkeitsrechts, wozu auch personenbezogene Daten zählen, generell dem Betroffenen zuzuordnen sind und eines gewissen Schutzes bedürfen. Grundsätzlich ist es nach der Rechtsprechung möglich, auch an persönlichkeitsbezogenen Rechten ein vermögenswertes Ausschließlichkeitsrecht anzuerkennen. Fraglich ist, um was für ein Ausschließlichkeitsrecht es sich bei personenbezogenen Daten handeln könnte und wie dieses im Einzelnen ausgestaltet sein sollte. Das deutsche Recht kennt im Wesentlichen zwei Arten von Ausschließlichkeitsrechten: das Sacheigentum im Sinne des § 903 BGB und das Immaterialgüterrecht.

---

110 BGH, Urteil v. 20.3.1968, NJW 1968, 1773ff.
111 BGH, Urteil v. 19.9.1961, NJW 1962, 736ff.
112 BVerfG, Urteil v. 15.12.1999, NJW 2000, 1021ff.
113 BVerfG, Beschluss v. 22.8.2006, NJW 2006, 3409ff.

Zivilrechtliches Eigentum ist die rechtliche Zuordnung eines körperlichen Gegenstands zu einer natürlichen oder juristischen Person und das umfassendste Herrschaftsrecht, das unsere Rechtsordnung kennt. Ob es ein Dateneigentum in Analogie zum zivilrechtlichen Eigentum geben kann, ist sehr umstritten. Während das tatsächliche Bedürfnis nach einer Regelung des Datenhandels und einer damit notwendigen Zuordnung von Daten, sowie das Schließen bestehender Schutzlücken dafürsprechen[114], wird von Gegnern des Dateneigentums angeführt, dass sich dieses Rechtsinstitut wegen mangelnder Sacheigenschaft von Daten und mangels einer planwidrigen Regelungslücke nicht auf Daten übertragen lässt[115].

Das Eigentum zeichnet sich dadurch aus, dass nur der Eigentümer nach seinem Belieben mit dem Rechtsgut verfahren darf, andere von der Benutzung ausgeschlossen werden können und sich dieses Recht auch mit dinglicher Wirkung übertragen lässt. Gerade die Übertragbarkeit bzw. die vollständige Veräußerung des potenziellen Dateneigentums ist kritisch zu sehen. Während bisher in der Praxis schon das Prinzip der informierten und freiwilligen Einwilligung in seiner Umsetzung erhebliche Mängel aufweist, steht zu befürchten, dass bei einem Dateneigentum etliche Betroffene dieses ebenfalls unüberlegt übertragen werden. Dann hätte der Betroffene das Eigentum an seinen personenbezogenen Daten jedoch endgültig verloren und für alle Zukunft keinen Einfluss mehr auf den Umgang mit seinen Daten. Dies steht der gewünschten Stärkung der Selbstbestimmung der Betroffenen eindeutig entgegen. Ein Dateneigentum kann es folglich nicht vollumfänglich – in der Gestalt, wie es das Zivilrecht versteht –, also mitsamt vollständiger Übertragbarkeit in Analogie zu § 903 BGB, geben, da sich dies nicht mit dem allgemeinen Persönlichkeitsrecht und der daraus fließenden informationellen Selbstbestimmung vereinbaren ließe.

Das Problem ist in der Tat mehr ein tatsächliches, da in der Realität keine Mechanismen existieren, dem gängigen „Take it or leave it"-Prinzip entgegenzusteuern und den unterlegenen Nutzer zu schützen, der nicht auf Augenhöhe mit weltweit operierenden Konzernen verhandeln kann. Der

114 Hoeren, MMR 2013, 486ff.
115 Dorner, CR 2014, 617 (621ff.).

faktische Zwang des Nutzers, eine datenschutzrechtliche Einwilligungserklärung abzugeben, um gängige Dienste zu nutzen, wird zum zunehmenden Problem. Es muss sichergestellt werden, dass der Betroffene ausreichend Kenntnis sowie Möglichkeiten der Einflussnahme und der finanziellen Beteiligung hinsichtlich der Datenverwertung hat – dazu bedarf es aber anderer oder weiterer Mechanismen, als ein Dateneigentum zu statuieren. Auch wenn es kein vollumfängliches Dateneigentum geben kann, sollten im Datenschutzrecht dennoch klare Regelungen über die Datennutzung und -verwertung getroffen werden.

II. Privacy by Contract

Reiners[116] ist der Ansicht, dass bei der momentanen unsicheren Rechtslage hinsichtlich der Verwertung von Daten Einigkeit darüber herrschen müsse, dass die beteiligten Parteien zumindest auf vertraglicher Grundlage die Verwertung der Daten vereinbaren könnten. Er sieht in dem Abschluss von Verträgen eine Möglichkeit, Einfluss auf den Schutz der eigenen Privatsphäre zu nehmen, und nennt dieses Modell „Privacy by Contract", das dem Einzelnen ermöglichen soll, den Umfang seines Datenschutzes und die konkrete Verwendung der auf ihn bezogenen Daten selbst zu bestimmen[117]. Die Vorteile einer vertraglichen Konzeption liegen darin, dass der Zweck der Datenverarbeitung eindeutig bestimmt und die zu erbringende Gegenleistung explizit geregelt wird. Ferner steigt bei den Betroffenen das Bewusstsein dafür, dass die Preisgabe ihrer Daten eine geldwerte Leistung darstellt und die Daten für Unternehmen einen Produktionsfaktor darstellen. Bislang werden vereinzelt im Bereich der Datenwirtschaft schon Verträge abgeschlossen, die sich jedoch vorwiegend nicht auf das Verhältnis zwischen Nutzer und Datenerheber, sondern auf eine sich anschließende Datenübermittlung beziehen. Den Ansatz, mehr Selbstbestimmung durch individuelle vertragliche Konzeptionen zu erzielen, verfolgt auch der Vorschlag, Regelungen parallel zum Urheberrecht zu schaffen, worauf sogleich noch näher einzugehen ist.

116 Reiners, ZD 2015, 51.
117 Reiners, ZD 2015, 51 (55).

III. Das Datum als Immaterialgut

Immaterialgüter sind unkörperliche Gegenstände von wirtschaftlichem oder ideellem Wert, an denen typischerweise Immaterialgüterrechte bestehen. Immaterialgüterrechte weisen einer Person ein Immaterialgut zur alleinigen wirtschaftlichen Verwertung zu und stellen daher ein Ausschließlichkeitsrecht dar. Das Urheberrecht stellt ein Mischrecht mit vermögens- und persönlichkeitsrechtlichen Elementen dar und ist als solches nicht übertragbar. Man kann das Urheberrecht mangels einer schöpferischen Leistung nicht direkt auf personenbezogene Daten anwenden; da aber beide Bereiche von ideellen und materiellen Interessen geprägt sind, lassen sich einige grundlegende Wertungen des Urheberrechts übertragen. Die Nichtübertragbarkeit einerseits und die Möglichkeit, verkehrsfähige Rechtspositionen einzuräumen, andererseits fehlen dem Datenschutzrecht – daher wird schon länger die Schaffung entsprechender Regelungen in Anlehnung an das Urheberrecht gefordert[118]. Im Gegensatz zu einem Dateneigentum würde bei einer derartigen Neugestaltung das Spannungsverhältnis zwischen Vermögens- und Persönlichkeitsrecht besser erfasst werden. Aufgrund der hohen Schutzgüter der uneinschränkbaren Menschenwürde und des allgemeinen Persönlichkeitsrechts dürfen nicht allein die vermögensrechtlichen Interessen im Vordergrund stehen.

Im Urheberrecht kann der Urheber Dritten einfache und ausschließliche Nutzungsrechte an seinem Werk einräumen. Nach § 31 UrhG ist ein Nutzungsrecht das vom Urheber eingeräumte Recht, das Werk auf einzelne oder alle Nutzungsarten zu nutzen. Während das einfache Nutzungsrecht es dem Rechtsinhaber erlaubt, das Werk auf die festgelegte Art zu nutzen, ohne eine Nutzung durch andere auszuschließen, berechtigt das ausschließliche Nutzungsrecht den Rechtsinhaber, das Werk auf die festgelegte Art unter Ausschluss anderer zu nutzen und wiederum einfache Nutzungsrechte (sog. Unterlizenzen) einzuräumen. Mittlerweile ist anerkannt, dass urheberrechtliche Nutzungsrechte dinglichen Charakter haben[119].

118 Forkel, GRUR 1988, 491.
119 BGH I ZR 153/06.

In Bezug auf personenbezogene Daten könnte man in den Bereichen, in denen eine Datenverarbeitung Dritter nicht durch das Gesetz legitimiert ist, dem Betroffenen das Recht zur wirtschaftlichen Verwertung der Daten zuweisen und das Recht zur Einräumung von Nutzungslizenzen gewähren. Hierbei vorteilhaft für die Betroffenen wäre, dass die Lizenzverträge sehr konkret ausgestaltet werden müssten. Im Urheberrecht gibt es die Besonderheit, dass das Recht nur in dem Umfang entsteht, in dem es vertraglich eingeräumt wurde[120]. Daher besteht bei der Einräumung von Nutzungslizenzen auch in der Praxis die Notwendigkeit, den Umfang und die Art der Datenverarbeitung im Vorfeld genau zu bezeichnen. Dadurch steigen die Möglichkeiten der Einflussnahme des Betroffenen dergestalt, dass er den Zweck der Datenverarbeitung selbst mitbestimmen und einzelne Fälle kategorisch ausschließen kann. Gibt es keine Spezifizierung des Umfangs des Nutzungsrechts bzw. keine Bezeichnung einzelner Nutzungsarten, gilt der Zweckübertragungsgrundsatz zum Schutz des Urhebers. Das heißt, dass sich die erlaubten Nutzungsarten nur auf das zur Erreichung des von beiden Parteien zugrunde gelegten Vertragszwecks Notwendige beschränken sollen. Selbst wenn Verträge über Nutzungslizenzen in Bezug auf personenbezogene Daten im Massenverfahren abgeschlossen würden, bestünden die Vorteile, dass die Zwecke der Datenverarbeitung exakt und explizit geregelt würden und die Betroffenen sich eine konkrete Gegenleistung einräumen lassen könnten.

Die Übertragung von Nutzungsrechten ist mit der Zustimmung des Urhebers möglich. Dabei darf der Urheber seine Zustimmung nicht wider Treu und Glauben verweigern. Unter bestimmten Voraussetzungen ist seine Zustimmung entbehrlich. Um der persönlichkeitsrechtlichen Komponente gerecht zu werden, kann der Urheber bei einer Ausübung des Nutzungsrechts, die ihm nach Treu und Glauben nicht zugemutet werden kann, das Nutzungsrecht zurückrufen. Auf dieses Recht zum Rückruf kann zudem nicht im Voraus verzichtet werden. Insoweit gäbe es bei einer Übertragung dieses Rechtsgedankens auf Daten einen schonenden Ausgleich zwischen

120 Soppe, in: Ahlberg/Götting (Hrsg.), BeckOK UrhG, § 31, Rn. 78.

dem Interesse an einem sensiblen Umgang mit den personenbezogenen Daten und dem Interesse an einer verkehrsfähigen, stabilen Rechtsposition.

Wie bereits dargelegt, lässt sich eine dauerhafte Übertragung der Rechte an einem personenbezogenen Datum nicht mit der informationellen Selbstbestimmung vereinbaren. Durch die Möglichkeit des Rückrufs bei gewandelter Überzeugung bleibt gewährleistet, dass die Nutzung eines Datums nicht im Widerspruch zur Persönlichkeit des Betroffenen steht. Dennoch würde es sich zur Stärkung der Selbstbestimmung der Betroffenen anbieten, das Spannungsverhältnis zwischen dem Bedürfnis nach einer gesicherten Rechtsposition und der Vereinbarkeit der Nutzung mit den jeweiligen Interessen des Betroffenen zusätzlich durch eine zeitliche Geltungsdauer aufzulösen. Diese sollte weder zu kurz noch zu lang ausgestaltet sein.

Bei der datenschutzrechtlichen Einwilligung gibt es keine gesetzliche Vorschrift zu deren Gültigkeitsdauer, sodass diese prinzipiell zeitlich unbegrenzt wirksam ist. Bei der vertraglichen Einräumung von Nutzungsrechten ist es unproblematisch möglich, eine zeitliche Beschränkung festzulegen. Eine solche zeitliche Geltungsdauer würde maßgeblich die Selbstbestimmung fördern, da nach dem Ablauf der Geltungsdauer die Konditionen neu ausgehandelt werden müssen und die Unternehmen sich bei großem Interesse an den Daten vermutlich auf individuelle Vertragsgestaltungen mit einigen Zugeständnissen einlassen werden.

Bei einer Realisierung des Datenhandels mittels Nutzungslizenzen muss der Aspekt des Vertragsmanagements näher in den Blick genommen werden. Der Nutzer muss einen Überblick über abgeschlossene Verträge und alle vertragsrelevanten Informationen behalten. Auch die Vertragsarchivierung – also die langfristige Aufbewahrung vertragsrelevanter Dokumente – ist ein wesentlicher Aspekt. Auch in diesem Bereich könnten moderne Technologien eingesetzt werden. Zu denken ist an die elektronische Verwaltung der Lizenzen über speziell entwickelte Apps oder mittels eines Portals, vergleichbar dem Bürgerkonto. Auf diese Art kann sich der Betroffene die grundlegenden Vertragsdaten schnell vergegenwärtigen. Allerdings ist es auch möglich, einen Dritten mit der Verwaltungstätigkeit zu betrauen.

Wie bei der Durchsetzung von Urheberrechten könnten auch für datenschutzrechtliche Verfügungsrechte spezielle Wahrnehmungsgesellschaften

gegründet und mit der Verwaltung nach den individuellen Präferenzen der Betroffenen beauftragt werden. Ein solches Modell ließe sich nur umsetzen, wenn ein Herrschaftsrecht an personenbezogenen Daten anerkannt wird, da es einer Übertragung der Rechte auf den Datentreuhänder bedarf. Buchner schlägt vor, dass zentrale Datenverarbeitungsinstitutionen nicht nur Daten sammeln und nutzen, sondern zu aktiven Interessenvertretern der Betroffenen werden. Sie erhielten dann die personenbezogenen Daten vom Betroffenen selbst und könnten sie nach Maßgabe der individuellen Präferenzen des Nutzers auswerten, nutzen, an Dritte weitergeben und ihren Wert maximieren. Die Datenverarbeiter würden dann zugleich zu treuhänderischen Verwaltern der ihnen anvertrauten Informationen werden[121].

Das Recht des Betroffenen kann freilich nicht uneingeschränkt bestehen. Im Urheberrecht gibt es einige Ausnahmetatbestände bzw. Schrankenregelungen, die einen Ausgleich zwischen den Interessen des Urhebers und kollidierenden Interessen Dritter schaffen sollen. Unter bestimmten Voraussetzungen gewährt das Urheberrecht eine erlaubnisfreie bzw. eine vergütungsfreie Nutzung des Werks; es gibt zahlreiche Einschränkungen des prinzipiell dem Urheber zugewiesenen Nutzungs- und Verwertungsrechts zugunsten einzelner Nutzer, der Kulturwirtschaft und der Allgemeinheit. Auch im BDSG gibt es diverse Erlaubnistatbestände für eine Datenverarbeitung – solche Regelungen müssten bei einer Neugestaltung nach dem Vorbild des Urheberrechts fortbestehen.

Als Zwischenfazit kann festgehalten werden, dass sich auch im Bereich der Datenwirtschaft Nutzungsrechte mit dinglicher Wirkung einräumen ließen. Mit der dinglichen Wirkung ergäben sich die Vorteile einer gesicherten Rechtsposition auch gegenüber Dritten. Ferner entstünde eine Möglichkeit der Weiterübertragung von Rechten an Daten. Weiterhin dient es der Transparenz, dass bei einer vertraglichen Konzeption der Umfang des Nutzungsrechts bzw. die erlaubten Nutzungsarten und die Gegenleistung konkret bestimmt werden müssen. In der Tat geht es bei der Zuordnung der Verfügungsbefugnis über personenbezogene Daten zu der betroffenen Person auch darum, die marktmäßige Nutzung effektiv zu steuern. Die Vorteile

121 Buchner, Informationelle Selbstbestimmung im Privatrecht, S. 277ff.

gegenüber einem Dateneigentum liegen darin, dass die Verknüpfung von materiellen und ideellen Interessen besser erfasst wird.

IV. Schaffen von Vorteilen der Datenverarbeitung für den Nutzer

Die vorgestellten Konzepte des Dateneigentums und der vertraglichen Einräumung von Nutzungslizenzen wurden entwickelt, um den wirtschaftlichen Wert von Daten hervorzuheben und eine eindeutige Zuordnung zu schaffen. In der Praxis soll sich eine monetäre Beteiligung des Betroffenen an der Verwertung der auf ihn bezogenen Daten leichter realisieren lassen. Der Vorteil für den Nutzer muss sich jedoch nicht immer in Geld ausdrücken: in einem symbiotischen Verhältnis von Datenerheber und Nutzer könnten auch anderweitige Vorteile die Datenverwertung rechtfertigen.

Denkbar ist zum Beispiel, dass im Bereich der Smart Cars die erhobenen Fahrzeugdaten vom Automobilhersteller individuell ausgewertet und aufbereitet werden und darauf aufbauend dem Nutzer ein Bericht geliefert wird, der unter anderem darüber Aufschluss geben kann, welcher Kfz-Typ der ökonomisch sinnvollste für ihn ist[122]. Auf dieser Basis lassen sich in vielen Bereichen der modernen Datenverarbeitung ähnliche Konzepte realisieren. Denkbar wäre bspw. folgendes Angebot: Im Gegenzug für das Auslesen der Energiedaten eines „intelligenten" Zählers und die anschließende Verwendung für eigene Zwecke misst der Datenverarbeiter regelmäßig den Verbrauch aller Haushaltsgeräte, klärt über deren eventuelle Ineffizienz auf und legt eine Berechnung über die Amortisation einer Neuanschaffung vor. Ein derartiges Verhältnis besteht auch bereits bei den Fitness-Armbändern, bei denen sich mit der Aufbereitung und statistischen Auswertung für den Nutzer ebenfalls ein Überblick über seine Gesundheitsdaten und somit über gesundheitliche Defizite ergibt.

122 Reiners, ZD 2015, 51 (52).

V. Grenzen der Selbstbestimmung des Einzelnen

Es gibt immer wieder Stimmen, die den Datenhandel als unerwünschte Entwicklung betrachten und ihn unterbinden wollen[123]. In der Tat ist es problematisch, dass durch die Kommerzialisierung der Daten durch Einzelne die informationelle Selbstbestimmung anderer beschnitten werden kann. Schon Kant formulierte sinngemäß, dass die Freiheit des einen dort endet, wo die Freiheit des anderen beginnt[124]. In diesem Sinne fand die Ausübung von Grundrechten schon immer ihre Schranken dort, wo die Rechte anderer Grundrechtsträger berührt waren. So ist auch die informationelle Selbstbestimmung des Einzelnen nicht schrankenlos gewährleistet und im Hinblick auf die Einschränkbarkeit das Prinzip der Verhältnismäßigkeit von besonderer Relevanz[125]. Im Umgang mit personenbezogenen Daten gibt es diverse Beteiligte mit unterschiedlichsten Interessen. Alle Interessen müssen in einen schonenden Ausgleich gebracht werden, und es bedarf stets einer Abwägung.

1. Negative Auswirkungen einer Kommerzialisierung für Einzelne und die Allgemeinheit

Nicht verschwiegen werden soll, dass mit dem hier entwickelten Konzept eines Kommerzialisierungsrechts des Einzelnen an seinen personenbezogenen Daten auch neue Konfliktpotenziale entstehen können.

Ein Beispiel für negative Auswirkungen einer Kommerzialisierung durch Dritte ist das Hochladen eines Bildes z. B. auf Facebook, auf dem andere Personen zu sehen sind. So kann durch das Verhalten von Mitmenschen ein Eingriff in die eigene Privatsphäre erfolgen. Es stellt sich die Frage, ob insoweit die Freiheiten anderer beschränkt werden müssen. In der Tat muss ein schonender Ausgleich zwischen allen Interessen gefunden werden, und

123 Interview mit Evgeny Morozow: „Niemand sollte Daten besitzen. Luft gehört auch keinem. [...] Daher müssen wir die Daten vergemeinschaften, sie sozialisieren", abrufbar unter: http://bit.ly/1PnDXtg

124 Kant, Die Metaphysik der Sitten (1797), Teil I.

125 Vgl. Rede von Bundespräsident a.D. Prof. Dr. Roman Herzog anlässlich der Übernahme der Schirmherrschaft über das DIVSI, abrufbar unter: https://www.divsi.de/ueber-uns/schirmherr/.

die Schaffung eines Ordnungsrahmens hierfür wird als staatliche Aufgabe angesehen. Maßstab der Abwägung können dabei Kriterien wie das Interesse an der Veröffentlichung und die Sensibilität des personenbezogenen Datums sein. Für die konkrete Fragestellung, ob ein bestimmtes Bild hochgeladen werden darf, müssen dem Einzelnen Leit- bzw. Richtlinien an die Hand gegeben werden; insoweit wäre die Ausarbeitung eines Kodexes sinnvoll. Mittlerweile kann die Veröffentlichung von Bildern auf Facebook als sozialadäquat bezeichnet werden und dürfte bei einer Beschränkung auf den Freundeskreis noch zu einer privaten Nutzung zählen. Jedoch ist ungeklärt, ab wie vielen Facebook-Kontakten man noch von einem privaten Rahmen sprechen kann[126]. Insbesondere die Möglichkeit des „Teilens" durch Freunde wiederum mit ihren privaten Kontakten birgt die Gefahr, dass ein Bild einem großen Personenkreis zugänglich gemacht wird. Wenn ein zu großer Eingriff in die Privatsphäre erfolgt, sollte eine Veröffentlichung untersagt sein; es bliebe immer noch die Möglichkeit der Einholung einer Erlaubnis von der betroffenen Person.

Besonders schwierig ist die Situation zu beurteilen, wenn die Daten in die Hände eines Konzerns gelangen, ohne dass der Betroffene dem zugestimmt oder Kenntnis davon hat. Für diese Fälle existiert bereits eine Mitteilungspflicht im BDSG (§ 33), aber dieser wird in der Praxis vielfach nicht nachgekommen, und ihr musste von Seiten amerikanischer Konzerne bislang auch nicht nachgekommen werden. Daher ist in diesem Zusammenhang die geplante Einführung des Marktortprinzips sehr zu begrüßen.

Auch mit der Registrierung bei dem Dienst WhatsApp gibt der Nutzer Daten über andere Personen preis. Mit der Anmeldung wird standardmäßig auf die gesamten Adressbuchdaten des Smartphones zugegriffen. Bei einer aktuellen Version des Messenger-Dienstes für ein bestimmtes Betriebssystem gibt es nun die Möglichkeit, einzelne Kontakte gezielt auszuwählen. WhatsApp versichert, dass ausschließlich die Telefonnummern aus dem Adressbuch verwendet werden, da deren Verarbeitung zur Kommunikation

126 http://irights.info/artikel/inhalte-auf-facebook-veroffentlichen-was-muss-ich-beachten/11555; Koch in: Ahlberg/Götting, BeckOK UrhG, § 87c, Rn. 7.

mit den betreffenden Personen notwendig sei[127]. Unklar ist bislang, wie die Übermittlung einer fremden Telefonnummer zur Nutzung eines kommerziellen Dienstes rechtlich zu beurteilen ist. Jedoch ist eine Telefonnummer kein sensibles Datum, und das Unternehmen darf ohne die ausdrückliche Erlaubnis ohnehin keine Telefonwerbung vornehmen[128]. Dennoch wäre es wünschenswert, auch in diesem Bereich Rechtssicherheit bezüglich des Umgangs mit personenbezogenen Daten herzustellen.

Ein weiteres Problem ist, dass durch die massenhafte Datenerhebung auch einfacher Rückschlüsse über Personengruppen oder die eigene Person möglich sind. Aufgrund der technischen Entwicklungen sind heutige Statistiken und Rückschlüsse sehr viel präziser. Berühmtes Beispiel ist der Fall, in dem einem Mädchen im Teenageralter von einem Supermarkt Windelwerbung zugeschickt wurde[129]. Der Vater erboste sich, ob man sie zu einer Schwangerschaft verleiten wolle. Jedoch war das Mädchen tatsächlich bereits schwanger, und eine algorithmenbasierte Analyse des Kaufverhaltens hatte dies aufgedeckt. So kaufen schwangere Frauen bevorzugt parfümfreie Lotionen oder Nahrungsergänzungsmittel mit Spurenelementen.

Ob man sich gegen diese neuen Möglichkeiten der Datenanalyse wehren und sie unterbinden will, ist eine moralische und politische Frage, jedoch darf man nicht die positiven Effekte der modernen Datenanalyse aus den Augen verlieren. Im Jahr 2013 wurden in Deutschland 226 Mrd. Euro Umsatz in der IKT-Branche und 85 Mrd. Euro Umsatz in der Internetwirtschaft erzielt[130]. So wird allein im Bereich der Connected-Car-Dienstleistungen bis

---

127 https://www.datenschutzbeauftragter-info.de/whatsapp-und-datenschutz-antworten-auf-die-wichtigsten-fragen/.

128 Vgl. Gesetz zur Bekämpfung unerlaubter Telefonwerbung und zur Verbesserung des Verbraucherschutzes bei besonderen Vertriebsformen, abrufbar unter: http://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&start=//*%255B@attr_id=%27bgbl109s2413.pdf%27%255D.

129 Lorenzen, Big Data schafft den Zufall ab, abrufbar unter: http://www.wiwo.de/unternehmen/it/digitale-revolution-der-wirtschaft/algorithmen-was-heute-schon-geht/7865208-2.html.

130 Bundesministerium für Wirtschaft und Energie, Monitoring-Report Digitale Wirtschaft 2014, abrufbar unter: http://www.bmwi.de/BMWi/Redaktion/PDF/Publikationen/monitoring-report-digitale-wirtschaft-2014-langfassung,property=pdf,bereich=bmwi2012,sprache=de,rwb=true.pdf.

2019 mit weltweiten Umsätzen von 40 Milliarden Dollar gerechnet[131]. Auch der Einzelne ist vielfach fasziniert von dem Komfort und den Möglichkeiten durch moderne IK-Technologien, und häufig werden schon bei geringen Anreizen bereitwillig Daten preisgegeben. Grundsätzlich steht die Kommerzialisierung der personenbezogenen Daten im freien Ermessen der Betroffenen. Es besteht allerdings die Befürchtung, dass die Freiwilligkeit sich zu einem ökonomischen Zwang hin entwickelt[132]. Das Handeln des Individuums unterliegt diversen Sachzwängen, die von den Gesetzen des Marktes ausgehen. Beispielsweise wird die Nutzung von IK-Technologien, die vielfach nur gegen eine Einwilligung in die Datennutzung möglich ist, auch für das berufliche Fortkommen immer essenzieller. Nach einer Studie der Personalvermittlungsagentur Kelly Services werden von Arbeitgeberseite vermehrt Jobangebote über Soziale Medien wie die Networking-Plattform XING unterbreitet[133]. Jedoch gibt es auch andere ökonomische Zwänge, die gesellschaftlich anerkannt sind: Bei diversen Technologien wie dem Telefon oder dem Automobil ist unbestreitbar, dass es keine Möglichkeit gibt, sich deren Gebrauch zu entziehen, ohne spürbare negative Auswirkungen in Kauf nehmen zu müssen. Manchen gesamtgesellschaftlichen Entwicklungen kann sich der Einzelne nur schwerlich entziehen.

Mit der zunehmenden Marktmacht einzelner Unternehmen wie Google infolge der Datenwirtschaft stellt sich immer drängender die Frage, ob der Staat aus Gründen des Allgemeinwohls eingreifen muss. So gab es die Idee, Suchmaschinen von anderen kommerziellen Dienstleistungen abzukoppeln[134]. In diesem Kontext ist die Bevorzugung eigener Angebote durch Suchmaschinenbetreiber ein gravierendes Problem im Hinblick auf den Missbrauch einer marktbeherrschenden Stellung. Doch nicht nur im kommerziellen Bereich, sondern auch im Bereich der Informationsbeschaffung

131 Aktuelle Studie von Juniper Research abrufbar unter: http://www.juniperresearch.com/press/press-releases/connected-cars-to-be-20pc-of-global-car-market.

132 Reiners/Suckfüll, Datensouveränität im Rahmen einer Personal Data Economy, S. 10.

133 http://www.kellyservices.de/uploadedFiles/Switzerland_-_Kelly_Services%281%29/4-Resource_Center/KGWI%204%202013%20Soziale%20Medien%20und%20Technologie_DEU%281%29.pdf.

134 Entschließung des Europäischen Parlaments zur Stärkung der Verbraucherrechte im digitalen Binnenmarkt, abrufbar unter: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+MOTION+B8-2014-0286+0+DOC+XML+V0//DE.

ist wesentlich, dass ausreichend Auswahl für die Nutzer und Vielfalt der Informationsquellen gewährleistet ist. Es ist wichtig, dass der Suchvorgang und die Suchergebnisse frei von Verzerrung sind. Suchmaschinen haben sich zu „Gatekeepern" entwickelt; es bedarf allerdings eines adäquaten Zugangs zu netzgebundenen Informationen für jeden Einzelnen. Die Individualisierung von Suchergebnissen kontrolliert durch Google ist eine besorgniserregende Entwicklung, und mit der EuGH-Entscheidung zum Recht auf Vergessenwerden wird nun sogar eine grundrechtliche Abwägungsentscheidung auf den privaten Konzern übertragen[135]. Das Internet stellt mittlerweile eine bedeutende Infrastruktur dar und dient diversen Beteiligten als Handlungsplattform. Daher ist der Staat verpflichtet, einen diskriminierungsfreien Zugang sowie eine gleichberechtigte Nutzung für jedermann sicherzustellen.

Abschließend lässt sich festhalten, dass die informationelle Selbstbestimmung nicht das Recht gewährt, sich jeglicher Datenverarbeitung zu entziehen. Es ist die Fehlvorstellung entstanden, dass die Daten, die sich auf die eigene Person beziehen, dem Betroffenen „gehören" und dieser gänzlich frei über deren Verwendung entscheiden könne. Jedoch wird die informationelle Selbstbestimmung nicht schrankenlos gewährleistet. Auch andere Rechtssubjekte haben diverse (grundrechtlich verbürgte) Rechte zum Umgang mit den personenbezogenen Daten z. B. basierend auf der Meinungsfreiheit, Medienfreiheit, Berufsfreiheit, Kunstfreiheit etc. Mit der umfassenden Digitalisierung und Vernetzung werden Daten immer intensiver von immer mehr Beteiligten genutzt. Hierdurch ergibt sich ein gewisser Kontrollverlust über die Verwendung von personenbezogenen Daten. Es muss den Grundrechtsträgern weiterhin möglich sein, den Kern ihrer Privatsphäre zu schützen, aber im Rahmen einer Abwägung wird bei etlichen Daten ein gewisser Kontrollverlust und eine Datenverarbeitung ohne Einwilligung des Betroffenen im Rahmen gesetzlicher Erlaubnistatbestände legitim sein und nicht die informationelle Selbstbestimmung verletzen. Davon losgelöst und von besonderer Bedeutung zur Stärkung der informationellen Selbstbestimmung ist die Herstellung von Transparenz der Datenverarbeitung. Denn

135 EuGH v. 13.5.2014, Rs. C-131/12.

auch eine nicht zu unterbindende Datenverarbeitung sollte in Kenntnis des Betroffenen erfolgen, damit der Einzelne mit dem Wissen über alle Umstände frei planen, entscheiden und sich entfalten kann.

2. Geltung des Solidarprinzips

Als weiteres Beispiel negativer Folgeentwicklungen einer Kommerzialisierung personenbezogener Daten kann der Trend zu individualisierten Versicherungstarifen genannt werden, der durch präzisere Risikoabschätzungen und Risikobewertungen möglich wird. Der Lebensstil des Versicherten lässt sich mittels Daten über Blutdruck, Blutzucker, Fettspiegel oder über das Bewegungsverhalten ermitteln, und bei einer gesunden Lebensführung können z. B. im Bereich der Krankenversicherung Rabatte oder Prämien gewährt werden. Analysten sehen in den aggregierten Körper- und Bewegungsdaten enormes Potenzial und regen an, sie für verhaltensbasierte Tarife zu nutzen. Grundsätzlich ist es wünschenswert, wenn die Versicherten zu gesunder Ernährung und ausreichend Sport angehalten werden, jedoch besteht bei individuellen Verträgen das Risiko der Ausgrenzung Einzelner. Hier würde sich die Preisgabe von Daten unmittelbar auf die finanzielle Situation der Betroffenen auswirken. Als Folge müssten Hochrisikopatienten statt einer Durchschnittsprämie immense Summen für ihre Versicherung aufbringen, und es wäre nicht gewährleistet, dass sie sich überhaupt versichern könnten.

Ab einem gewissen Stadium dieser Entwicklung muss ihr unter Umständen Einhalt geboten werden, da sie nicht mehr mit dem Sozialstaatsprinzip vereinbar ist. Der Staat hat nach dem Sozialstaatsprinzip den verfassungsrechtlichen Auftrag, ein System der sozialen Sicherung aufzubauen, d. h., er darf niemanden ohne ein Minimum an sozialer Sicherung sich selbst seinem Einzelschicksal überlassen. Aus dem Sozialstaatsprinzip folgt das Solidaritätsprinzip, welches die moralische Grundlage der Sozialversicherung ist. Es wird eine Solidargemeinschaft gebildet, deren Mitglieder gegenseitig füreinander einstehen. Freiheit wird dadurch ermöglicht, dass gewisse Risiken und risikobehaftete Tätigkeiten von der Solidargemeinschaft toleriert und versichert werden. Gesetzliche Krankenkassen lehnen bislang Tarife bezogen auf den individuellen Gesundheitszustand ab und verweisen dabei auf

das Solidarprinzip und das Prinzip, dass der Beitrag einkommensabhängig ausgestaltet ist. Allerdings bietet auch eine gesetzliche Krankenversicherung bereits Rabatte bei der freiwilligen Übermittlung von Bewegungsdaten an[136].

VI. Zuordnungsregel für nicht-personenbezogene Daten

Es stellt sich die Frage, ob es auch eines Ausschließlichkeitsrechts für nicht personenbezogene Daten bedarf. Bislang gibt es im Bereich der Daten ohne Personenbezug keine rechtlichen Vorgaben in Bezug auf Rechte zur Nutzung und zur Verwertung. Während bei personenbezogenen Daten der Einzelne ein Interesse daran hat, die auf ihn bezogenen Daten im Sinne seines Persönlichkeitsrechts zu schützen, gibt es dieses Interesse bei nicht personenbezogenen Daten nicht. Daher kann hinsichtlich einer rechtlichen Zuordnung auch nicht an den Personenbezug angeknüpft werden.

Mit zunehmendem Wert der Daten als „Rohstoff" sind allerdings auch diese immer schützenswerter. Bislang entschied allein der faktische Besitz an Daten über ihre Verteilung. In der Regel hat derjenige, der Daten produziert oder erhebt, zunächst den Besitz an ihnen und kann sie anderen vorenthalten. Dennoch lässt sich die Verbreitung und Verwendung durch andere nicht gänzlich kontrollieren. Bei einer Beeinträchtigung in seinem Besitz stehen dem Einzelnen keine ebenso starken Abwehransprüche und Schutzansprüche zur Verfügung, wie dies bei einer dinglichen Zuweisung der Fall wäre. Unklar ist, an welche Kriterien man bei der Vornahme einer Zuordnung anknüpfen sollte.

Ob man letztlich die Verwertungsrechte an Daten mittels eines Ausschließlichkeitsrechts jemand Bestimmtem zuordnen will, ist auch eine politische Frage. In Bezug auf viele Daten wird es mehrere Rechtssubjekte geben, die ein berechtigtes Interesse an ihnen geltend machen. Zweifelhaft ist daher, ob eine eindeutige Zuordnung möglich und erstrebenswert ist oder ob es nicht vielmehr einer Ordnung bedarf, die bestimmt, wer in welcher

136 Schneider, Rabatte für Gesundheitsdaten: Was die deutschen Krankenversicherer planen, abrufbar unter: http://www.zdnet.de/88214397/gesundheitsdaten-per-fitness-tracker-die-deutschen-krankenversicherer-planen/.

Relation zum Umgang mit Daten befugt ist. In diesem Sinne wäre es zur Förderung der Wirtschaft und im Sinne der Rechtsklarheit wünschenswert, dass die Rechte in Bezug auf den Umgang und die Verwertung auch für nicht personenbezogene Daten klarer geregelt werden.

H. Fazit

Der wirtschaftliche Wert von Daten findet bislang in rechtlicher Hinsicht immer noch kaum Berücksichtigung. Im Zusammenhang mit der Datenverarbeitung stehen weiterhin ideelle Interessen im Vordergrund der rechtlichen Regelungen. Noch heute dient das Bundesdatenschutzgesetz zuallererst dem Schutz der freien Entfaltung der Persönlichkeit. Von Seiten der Unternehmen wird aber, wie diese Studie aufzeigt, schon längst und in zunehmendem Maße der wirtschaftliche Wert von personenbezogenen Daten mithilfe des Instruments der Einwilligung ausgeschöpft. Aufgezeigt wurde, dass die datenschutzrechtliche Einwilligung vollkommen ungeeignet ist, das hier faktisch bestehende Austauschverhältnis zu erfassen. Mit der zunehmenden Kommerzialisierung der Daten ist also längst ein Reformbedarf entstanden, weil das derzeitige Datenschutzrecht aktuellen Entwicklungen in der Datenwirtschaft aufgrund seiner Konzeption gar nicht gerecht werden kann.

Heute sollte der Einzelne als selbstbestimmtes Individuum entscheiden können, ab welchem Umfang eine Veröffentlichung und Verbreitung der auf ihn bezogenen Daten das ihm zuträgliche Maß überschreitet. Die Selbstbestimmung der Nutzer sollte das oberste Ziel sein. Hierfür ist Transparenz notwendig. Aber gerade diese erweist sich in der Realität als unzureichend. Überforderte Betroffene erteilen ihre Einwilligung, ohne den angebotenen, aufklärenden Text zur Kenntnis zu nehmen. Bei Intransparenz aber fehlt es an einer willentlichen Entscheidung in Kenntnis aller Konsequenzen.

Sind die Daten erst einmal in den Besitz von Unternehmen gelangt, können diese faktisch in zahlreichen Fällen mit ihrem Datenbestand nach Belieben verfahren. Der Nutzer hat keinen Einfluss auf die stattfindende Datenverarbeitung. Wie sich die Datensouveränität des Einzelnen in der Praxis herstellen lässt, ist eine schwer zu lösende Herausforderung. Die vorgestellten Ansätze wären ein vielversprechender Anfang.

Da Urheberrecht und Datenschutzrecht von ideellen und materiellen Interessen geprägt sind, lassen sich einige grundlegende Wertungen des Urheberrechts auf den Umgang mit personenbezogenen Daten übertragen. Insbesondere das Modell der Einräumung von Nutzungslizenzen mit

dinglicher Wirkung wird schon lange auch für den Bereich der Datenwirtschaft befürwortet. Mit der dinglichen Wirkung ergäben sich die Vorteile einer gesicherten Rechtsposition der Nutzer gegenüber Dritten. Auch entstünde für sie eine Möglichkeit der Weiterübertragung von Rechten an Daten. Eine vertragliche Ausgestaltung böte die Vorzüge, dass der Umfang des Nutzungsrechts bzw. die erlaubten Nutzungsarten und die Gegenleistung konkret bestimmt werden müssen. Zudem ließe sich eine zeitliche Geltungsdauer vereinbaren. Denkbar wäre auch zur Ausübung der Rechte, diese auf einen Datentreuhänder bzw. auf Wahrnehmungsgesellschaften zu übertragen.

Um die Selbstbestimmung der Nutzer effektiv sicherzustellen, bedarf es praxistauglicher Mechanismen. Hierbei steht insbesondere, wie eingangs angeführt, die Herstellung von Transparenz im Vordergrund. Diese ist bei stärkerer Selbstbestimmung der betroffenen Parteien hinsichtlich der Ausgestaltung des Datenverarbeitungsverhältnisses unbedingt notwendig. Erste Ansätze sind mit der Einführung eines Datenschutzbriefs oder eines Bürgerkontos (denkbar auch für den Bereich der Privatwirtschaft) erkennbar.

Deutschland benötigt einerseits eine Lockerung des Datenschutzrechts dergestalt, dass nicht jede Datenverarbeitung als unerwünscht betrachtet wird und auch ökonomische Interessen Berücksichtigung finden. Zudem ist eine Verschärfung dahingehend notwendig, dass es dem Einzelnen erleichtert wird, seine ideellen Interessen zu schützen.

Zur Herstellung von Rechtssicherheit für alle Beteiligten bedarf es klarer Regelungen über Nutzungs- und Verwertungsrechte an (personenbezogenen) Daten. Ziel muss sein, den Datenhandel rechtlich zu erfassen sowie die Nutzer-Selbstbestimmung zu fördern. Hauptproblem ist, dass im Bereich der digitalen Datenwirtschaft Politik und Gesetzgeber nicht angemessen auf seit Langem bekannte Entwicklungen reagieren. Es wird Zeit, dass rechtliche und praktische Konzepte zur Entwicklung von Daten zu einer Handelsware umgesetzt werden.

Literatur- und Quellenverzeichnis

Ahlberg, Hartwig/Götting, Horst-Peter (Hrsg.): Beck'scher Online-Kommentar zum Urheberrecht, Edition 9, München, Stand: 01.07.2015.

Astheimer, Sven/Balzter, Sebastian: Schwedische Arbeitnehmer lassen sich Chip implantieren – freiwillig, 25.2.2015, www.faz.net/aktuell/beruf-chance/arbeitswelt/rfid-chip-bueroangestellte-schweden-13438675.html.

Bartels, Gerrit: Nichts darf umsonst sein, Jaron Lanier und die Gratiskultur im Internet, in: Der Tagesspiegel, 12.5.2014, http://www.tagesspiegel.de/kultur/jaron-lanier-und-die-gratiskultur-im-internet-nichts-darf-umsonst-sein/9873822.html.

Baumann, Max-Otto: Datenschutzversagen, MERKUR Mai 2015, S. 86-92.

Berke, Jürgen: Telekom fordert vollständige Deregulierung des Marktes, 26.10.2013, www.wiwo.de/unternehmen/it/positionspapier-telekom-fordert-vollstaendige-deregulierung-des-marktes/8988344.html.

Boos, Carina/Roßnagel, Alexander: Nutzerunterstützung im Online-Versandhandel, MMR 2015, S. 215-220.

Bosesky, Pino/Deussen, Peter H./Quandt, Anne/Schulz, Sönke E./Strick, Linda: Datenhoheit in der Cloud, in: Schriften zur Modernisierung von Staat und Verwaltung, Band 18, Kiel 2013.

Bräutigam, Peter: Das Nutzungsverhältnis bei sozialen Netzwerken, MMR 2012, S. 635-641.

Buchner, Benedikt: Informationelle Selbstbestimmung im Privatrecht, Tübingen 2006; Die Einwilligung im Datenschutzrecht – vom Rechtfertigungsgrund zum Kommerzialisierungsinstrument, DuD 2010, S. 39-43.

Bundesministerium für Bildung und Forschung: Studie „Technikfolgenabschätzung – Ubiquitäres Computing und Informationelle Selbstbestimmung" (TAUCIS), Juli 2006, https://www.datenschutzzentrum.de/taucis/ita_taucis.pdf.

Bundesministerium für Wirtschaft und Energie (BMWi): Herausforderungen für eine moderne Industriepolitik, http://www.bmwi.de/DE/Themen/Industrie/Industriepolitik/moderne-industriepolitik.html; Industrie 4.0: Digitalisierung der Wirtschaft, http://www.bmwi.de/DE/Themen/Industrie/industrie-4-0.html; Monitoring-Report Digitale Wirtschaft 2014, http://www.bmwi.de/BMWi/Redaktion/PDF/Publikationen/monitoring-report-digitale-wirtschaft-2014-langfassung,property=pdf,bereich=bmwi2012,sprache=de,rwb=true.pdf.

Bundesverband Informationswirtschaft, Telekommunikation und neue Medien (BITKOM): Big Data und Geschäftsmodell-Innovationen in der Praxis: 40+ Beispiele, 9.2.2015, https://www.bitkom.org/Bitkom/Publikationen/Big-Data-und-Geschaeftsmodell-Innovationen-in-der-Praxis-40-Beispiele.html; Bitkom sieht Strafen im IT-Sicherheitsgesetz kritisch, 12.6.2015, https://www.bitkom.org/Presse/Presseinformation/Bitkom-sieht-Strafen-im-IT-Sicherheitsgesetz-kritisch.html.

Carr, Nicholas: The Limits of Social Engineering, 16.4.2014, http://technologyreview.com/review/526561/the-limits-of-social-engineering.

Chaos Computer Club: „E-Mail Made in Germany": Das Sommermärchen von der sicheren E-Mail, 9.8.2013, http://www.ccc.de/de/updates/2013/sommermaerchen; Datenbrief, 25.1.2010, http://www.ccc.de/datenbrief.

Clauß, Ulrich: So würde Europas „Schengen-Internet" funktionieren, 31.3.2014, http://www.welt.de/politik/deutschland/article126343060/So-wuerde-Europas-Schengen-Internet-funktionieren.html.

Datenschutzbeauftragter - INFO: WhatsApp und Datenschutz – Antworten auf die wichtigsten Fragen, 15.1.2015, https://www.datenschutzbeauftragter-info.de/whatsapp-und-datenschutz-antworten-auf-die-wichtigsten-fragen.

Dehmel, Susanne: Datenschutz in der global vernetzten Wirtschaft – ein europäischer Exportschlager?, ZD 2015, S. 197-198.

Deiß, Matthias: Datenklau per Funk – Sicherheitsrisiko an deutschen Flughäfen, 14.1.2010, www.rbb-online.de/kontraste/ueber_den_tag_hinaus/terrorismus/datenklau_per_funk.html.

Deutsche Wirtschafts Nachrichten: Digital-GEZ:Merkel denkt über staatliches Internet nach, 5.6.2015, http://deutsche-wirtschafts-nachrichten.de/2015/06/05/digital-gez-merkel-denkt-ueber-staatliches-internet-nach/.

Deutsches Institut für Vertrauen und Sicherheit im Internet (DIVSI): Daten – Ware und Währung, November 2014, https://www.divsi.de/wp-content/uploads/2014/11/DIVSI-Studie-Daten-Ware-Waehrung.pdf; Rede von Bundespräsident a.D. Prof. Dr. Roman Herzog anlässlich der Übernahme der Schirmherrschaft über das DIVSI, https://www.divsi.de/ueber-uns/schirmherr/.

DIE WELT: Datenklau-Opfer müssen noch ein paar Tage bangen, 4.4.2014, http://www.welt.de/wirtschaft/webwelt/article126583693/Datenklau-Opfer-muessen-noch-ein-paar-Tage-bangen.html; Hacker erbeuten unveröffentlichte Sony-Filme, 3.12.2014, http://welt.de/wirtschaft/webwelt/article134981981/Hacker-erbeuten-unveroeffentlichte-Sony-Filme.html.

Dix, Alexander: Nach Snowden: Noch eine Chance für Safe Harbor?, DSB 2015, S. 62-63.

Dorner, Michael: Big Data und „Dateneigentum", CR 2014, S. 617-628.

Dreier, Thomas/Schulze, Gernot: Kommentar zum Urheberrechtsgesetz, 5. Aufl., München 2015.

Europäische Kommission: Strategie für einen digitalen Binnenmarkt für Europa vom 06.05.2015, COM(2015) 192 final, http://ec.europa.eu/priorities/digital-single-market/docs/dsm-communication_de.pdf.

Europäisches Parlament: Entschließungsantrag des Europäischen Parlaments zur Stärkung der Verbraucherrechte im digitalen Binnenmarkt (2014/2973(RSP)) vom 24.11.2014, http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+MOTION+B8-2014-0286+0+DOC+XML+V0//DE; Legislative Entschließung des Europäischen Parlaments zu dem Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (allgemeine Datenschutzverordnung) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)) vom 12.03.2014, http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0212+0+DOC+XML+V0//DE.

Europarat: Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (Konvention Nr. 108) vom 1.10.1985, http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=108&CM=2&CL=GER.

Forkel, Hans: Lizenzen an Persönlichkeitsrechten durch gebundene Rechtsübertragung, GRUR 1988, S. 491-501.

Frankfurter Allgemeine Zeitung: Ein Internet nur für Deutschland, 10.11.2013, http://www.faz.net/aktuell/wirtschaft/netzwirtschaft/plaene-der-telekom-ein-internet-nur-fuer-deutschland-12657090.html.

Giurgiu, Andra: Die Modernisierung des europäischen Datenschutzrechts – Was unternehmen erwartet, CCZ 2012, S. 226-229.

Grapentin, Sabine: Datenschutz und Globalisierung – Binding Corporate Rules als Lösung?, CR 2009, S. 693-698.

Hoeren, Thomas: Dateneigentum, MMR 2013, S. 486-491.

Hoffmann, Christian: Die Gewährleistung der Vertraulichkeit und Integrität elektronischer Daten- und Dokumentensafes, Kiel 2012.

International Data Corporation (IDC): Data Growth, Business Opportunities, and the IT Imperatives, April 2014, http://germany.emc.com/leadersAhip/digital-universe/2014iview/executive-summary.htm.

ITWissen: Beschreibung „Peering", in: ITWissen. Das große Online-Lexikon für Informationstechnologie, http://www.itwissen.info/definition/lexikon/Peering-peering.html.

Juniper Research: Connected Cars to Represent 20% of the Global Car Market by 2019, http://www.juniperresearch.com/press/press-releases/connected-cars-to-be-20pc-of-global-car-market.

Kant, Immanuel: Ebeling, Hans (Hrsg.), Metaphysik der Sitten, Stuttgart 1990.

Kelly Services: Kelly Global Workforce Index 2013, Soziale Medien und Technologie, http://www.kellyservices.de/uploadedFiles/Switzerland_-_Kelly_Services%281%29/4-Resource_Center/KGWI%204%202013%20Soziale%20Medien%20und%20Technologie_DEU%281%29.pdf.

Lackes, Richard: Eintrag „Algorithmus", in: Gabler Wirtschaftslexikon, http://wirtschaftslexikon.gabler.de/Definition/algorithmus.html.

Leibholz, Gerhard/Rinck, Hans-Justus: Kommentar zum Grundgesetz, Rechtsprechung des Bundesverfassungsgerichts, Stand: 68. Ergänzungslieferung, Köln Juli 2015.

Lorenzen, Meike: Big Data schafft den Zufall ab, 1.3.2013, http://www.wiwo.de/unternehmen/it/digitale-revolution-der-wirtschaft/algorithmen-was-heute-schon-geht/7865208-2.html.

Mander, Jason: Mobile Messaging, Summary GWI Trends Q3 2014, http://de.slideshare.net/globalwebindex/gwi-trends-mobile-messaging-q3-2014.

Meier, Albrecht: Brüssel will Datenübermittlung nach USA neu regeln, 13.4.2015, http://www.tagesspiegel.de/politik/datenschutz-bruesesel-will-datenuebermittlung-nach-usa-neu-regeln/11629820.html.

Melan, Nevada/Wecke, Bertram: Umsatzsteuerpflicht von „kostenlosen" Internetdiensten und SmartphoneApps, DStR 2015, S. 22672269.

Monopolkommission: Auszug aus Hauptgutachten XX (2012/2013), Kapitel I – Aktuelle Probleme der Wettbewerbspolitik, http://www.monopolkommission.de/images/PDF/HG/HG20/1_Kap_1_A_HG20.pdf.

Morozov, Evgeny: „Mir ist egal, ob ich lustig bin", Interview der TAZ mit Evgeny Morozov, geführt von Johannes Gernert und Daniel Schulz, 31.1.2015, http://www.taz.de/1/archiv/digitaz/artikel/?ressort=hi&dig=2015%2F01%2F31%2Fa0027&cHash=171560451b3d7fc9f7949b174cfe2db9.

Peterson, Andrea: The White House's draft of a consumer privacy bill is out – and even the FTC is worried, 27.2.2015, https://www.washingtonpost.com/blogs/the-switch/wp/2015/02/27/the-white-houses-draft-of-a-consumer-privacy-bill-is-out-and-even-the-ftc-is-worried/.

Pisacane, Maximilian: Firmen unterschätzen Datenklau, 10.5.2007, http://www.handelsblatt.com/unternehmen/management/mittelstaendler-besonders-sorglos-firmen-unterschaetzen-datenklau/2806634.html.

Rat der Europäischen Union: Allgemeine Ausrichtung des EU-Rats zur Datenschutzgrundverordnung v. 15.6.2015, 9565/15, http://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/de/pdf.

Reiners, Wilfried: Datenschutz in der Personal Data Economy, ZD 2015, S. 51-55.

Reiners, Wilfried/Suckfüll, Hanns: Datensouveränität im Rahmen einer Personal Data Economy, 24.7.2013, http://www.apde-org.eu/media/pdf/Recht%20der%20Datensouveraenitaet%20DE_2.pdf.

Rogosch, Patricia Maria: Die Einwilligung im Datenschutzrecht, in: Frankfurter Studien zum Datenschutz, Band 40, Baden-Baden 2013.

Schaar, Peter: Privacy by design, in: Identity in the Information Society 2010, S. 267-274, http://www.bfdi.bund.de/SharedDocs/Publikationen/%22PrivacyByDesign%22.pdf?__blob=publicationFile.

Schliesky, Utz/Hoffmann, Christian/Luch, Anika/Schulz, Sönke/Borchers, Kim Corinna: Schutzpflichten und Drittwirkung im Internet. Das Grundgesetz im digitalen Zeitalter, Baden-Baden 2014.

Schmidt, Wolf: Ein Datenbrief fürs Handy, 6.7.2010, http://www.taz.de/!5139557/.

Schneider, Rainer: Rabatte für Gesundheitsdaten: Was die deutschen Krankenversicherer planen, 18.12.2014, http://www.zdnet.de/88214397/gesundheitsdaten-per-fitness-tracker-die-deutschen-krankenversicherer-planen/.

Schultz, Stefan: Sorge vor Kartell: Maas hätte gerne, dass Google geheime Suchformel offenlegt, 16.9.2014, http://www.spiegel.de/wirtschaft/unternehmen/google-heiko-maas-fordert-offenlegung-von-algorithmus-a-991799.html.

Schulz, Sönke E.: Wider die Aufnahme des Datenschutzes in das Grundgesetz, ZG 2010, S. 358-373.

Seidel, Ulrich: Das Grundrecht auf Datensouveränität, ZG 2014, S. 153-165.

Simitis, Spiros (Hrsg.): Bundesdatenschutzgesetz Kommentar, 8. Auflage, Baden-Baden 2014.

SPIEGEL ONLINE: Datenklau: Hacker stehlen Daten von 4,5 Millionen US-Patienten, 18.8.2014, http://www.spiegel.de/netzwelt/netzpolitik/us-krankenhaeuser-hacker-stehlen-daten-von-4,5-millionen-patienten-a-986804.html; Healthkit: IBM will Gesundheitsdaten von Apple-Nutzern auswerten, 14.4.2015, http://www.spiegel.de/wirtschaft/unternehmen/apple-healthkit-ibm-will-gesundheitsdaten-auswerten-a-1028426.html.

Statista: Marktanteile führender Suchmaschinen in Deutschland im Februar 2015 (sowie Vorjahresvergleich), http://de.statista.com/statistik/daten/studie/167841/umfrage/marktanteile-ausgewaehlter-suchmaschinen-in-deutschland/; Umsatz der Branche Datenverarbeitung, Hosting und damit verbundene Tätigkeiten in den USA von 2008 bis 2013 und Prognose bis zum Jahr 2018 (in Millionen US-Dollar), http://de.statista.com/prognosen/371852/datenverarbeitung-hosting-und-verbundene-taetigkeiten-in-den-usa--umsatzprognose; Marktanteile von Social Media Seiten nach Seitenabrufen weltweit von Januar bis Juli 2015, http://de.statista.com/statistik/daten/studie/241601/umfrage/marktanteile-fuehrender-social-media-seiten-weltweit.

Taeger, Jürger/Gabel, Detlev (Hrsg.): Kommentar, Bundesdatenschutzgesetz und Datenschutzvorschriften des TKG und TMG, 2. Auflage, München 2013.

tagesschau: Puzzlespiel im Bundestag – Hackerangriff dauert offenbar schon viel länger, 19.6.2015, http://www.tagesschau.de/inland/bundestag-hacker-angriff-101.html.

The Boston Consulting Group (BCG): The Value of Our Digital Identity, November 2012, http://www.libertyglobal.com/PDF/public-policy/The-Value-of-Our-Digital-Identity.pdf.

Tinnefeld, Marie-Theres/Buchner, Benedikt/Petri, Thomas: Einführung in das Datenschutzrecht, 5. Aufl., München 2012.

Verbraucherzentrale Bundesverband (vzbv): Facebook führt Nutzer in die Irre, 26.2.2015, http://www.vzbv.de/pressemitteilung/facebook-fuehrt-nutzer-die-irre.

Weidlich-Flatten, Eva: Verbraucherschutzverbände als Heilsbringer für den Datenschutz?, ZRP 2014, S. 196-198.

Weiser, Mark: The Computer for the 21st Century, in: Mobile Computing and Communications Review, Volume 3, Number 3, S. 3-11.

Wirtschaftswoche: Milliardenstrafe abgewendet, Google und die EU sind sich einig, 5.2.2014, http://www.wiwo.de/technologie/digitale-welt/milliardenstrafe-abgewendet-google-und-die-eu-sind-sich-einig/9436322.html.

Wragge, Alexander: Inhalte auf Facebook veröffentlichen: Was muss ich beachten?, 18.8.2015, http://irights.info/artikel/inhalte-auf-facebook-veroffentlichen-was-muss-ich-beachten/11555.

Xamit: Datenschutzbarometer 2009, http://www.xamit-leistungen.de/veroeffentlichungen/studien-und-tests/; Datenschutzbarometer 2013, http://www.xamit-leistungen.de/veroeffentlichungen/studien-und-tests/.

Zech, Herbert: Daten als Wirtschaftsgut – Überlegungen zu einem ,,Recht des Datenerzeugers¨, CR 2015, S. 137-146.

ZEIT ONLINE: Facebook manipulierte für Studie Nachrichtenstrom, 29.6.2014, http:/www.zeit.de/digital/internet/2014-06/facebook-nutzer-manipulation-studie; Gefeit vor der NSA? Deutsche Cloud-Anbieter werben mit Sicherheit, 18.3.2014, http://www.zeit.de/news/2014-03/18/computer-gefeit-vor-der-nsa-deutsche-cloud-anbieter-werben-mit-sicherheit-18143806.

Alle angegebenen Internetadressen wurden zuletzt am 20.10.2015 abgerufen.

Über DIVSI

Die Durchdringung von Staat und Gesellschaft mit IT nimmt immer weiter zu. In vielen Bereichen des täglichen Lebens ist das Internet heute nahezu unverzichtbar. Es wird daher künftig entscheidend sein, das Vertrauen der Menschen in das Internet zu fördern und zu sichern. Es geht darum, eine zeitgemäße Technologie sicher einsetzen zu können. Dabei wollen wir als Institut maßgeblich mithelfen.

Das Deutsche Institut für Vertrauen und Sicherheit im Internet (DIVSI) ...

- versteht sich als Forum, das einen offenen und transparenten Dialog zu mehr Vertrauen und Sicherheit im Internet gestaltet und mit neuen Aspekten belebt.
- fördert den interdisziplinären Dialog und die Vernetzung zwischen Wissenschaft, Wirtschaft, Gesellschaft und Politik.
- unterstützt Wissenschaft und Forschung und will so mithelfen, potenzielle Risiken bei der elektronischen Kommunikation und Transaktion zu untersuchen und zu analysieren.
- will durch Aufklärungsarbeit für eine Sensibilisierung auf Seiten der Nutzer zur Steigerung von Vertrauen und Sicherheit im Internet sorgen.

Das Deutsche Institut für Vertrauen und Sicherheit im Internet ist eine gemeinnützige Gesellschaft der Deutsche Post AG.

DIVSI-Kernbegriffe

Vertrauen ist eine wichtige Triebfeder menschlichen Handelns. Das gilt im alltäglichen Leben ebenso wie für spezielle Aktivitäten im Internet. Konkret kann Vertrauen dabei zweierlei bedeuten: Vertrauen in eine Sache oder Vertrauen in eine Person. Neben der Fähigkeit, mit etwas vertraut zu sein, bringt der Begriff also auch die menschliche Empfindung zum Ausdruck, Vertrauen zu haben. Beides ist entscheidend dafür, wie wir das Internet nutzen. Aus diesem Grund ist Vertrauen für DIVSI ein Kernbegriff im Diskurs über Chancen und Risiken des Internets.

Sicherheit ist ein Grundbedürfnis aller Menschen. In unterschiedlicher Ausprägung bestimmt es unser individuelles Handeln und Nutzungsverhalten. Wie sicher die Nutzung des Internets tatsächlich ist, können die wenigsten Menschen beurteilen. Das Sicherheitsempfinden einzelner User hängt zum einen von der Technologie und zum anderen von einem Konsens über sicheres Agieren im Internet ab. Dem Thema Datenschutz kommt dabei eine besondere Bedeutung zu. An einem bestimmten Punkt kann ein „verordnetes" Maß an Sicherheit zur Einschränkung individueller Freiheiten führen. Eine freie und demokratische Gesellschaft muss daher stets die Balance zwischen Sicherheit und Freiheit wahren.

Über das Lorenz-von-Stein-Institut für Verwaltungswissenschaften

Das Lorenz-von-Stein-Institut ist eine der Christian-Albrechts-Universität zu Kiel angegliederte wissenschaftliche Einrichtung, die selbstständig Forschung und Lehre auf dem Gebiet der Verwaltungswissenschaften erbringt. Das Institut betreibt Zweckforschung für die öffentliche Verwaltung, erstellt Sachverständigengutachten, bietet Fort- und Weiterbildung für Angehörige der Verwaltungen und forscht noch heute über das Werk und Wirken Lorenz von Steins in der Vergangenheit, Gegenwart und Zukunft. Gemeinsam mit dem Deutschen Institut für Vertrauen und Sicherheit im Internet führt das Lorenz-von-Stein-Institut auch ein Forschungsprojekt unter dem Titel „Ist das Grundgesetz zur Bewältigung der Herausforderungen des digitalen Zeitalters geeignet?" durch, das die Auswirkungen der Digitalisierung auf die verfassungsrechtlichen Grundlagen des Rechtssystems analysiert. Unter Leitung eines aus drei Professoren bestehenden, interdisziplinär zusammengesetzten Vorstandes arbeiten am Institut derzeit fünf wissenschaftliche Mitarbeiter. Das Institut unterhält eine eigene Bibliothek und betreibt einen wissenschaftlichen Verlag.

Die Autorin

Johanna Jöns ist Diplom-Juristin (Universität Kiel) und wissenschaftliche Mitarbeiterin am Lorenz-von-Stein-Institut für Verwaltungswissenschaften.

DIVSI Publikationen im Überblick

Studien

- **DIVSI Milieu-Studie zu Vertrauen und Sicherheit im Internet**, 2012, Aktualisierung 2013
- **DIVSI Meinungsführer-Studie: Wer gestaltet das Internet?**, 2012
- **DIVSI Entscheider-Studie zu Vertrauen und Sicherheit im Internet**, 2013
- **DIVSI Studie zu Freiheit versus Regulierung im Internet**, 2013
- **DIVSI U25-Studie**, 2014
- **DIVSI Studie zu Bereichen und Formen der Beteiligung im Internet**, 2014
- **Braucht Deutschland einen Digitalen Kodex?**, 2014
- **Wissenwertes über den Umgang mit Smartphones**, 2014
- **Daten – Ware und Währung**, 2014
- **DIVSI U9-Studie: Kinder in der digitalen Welt**, 2015
- **Beteiligung im Internet – Wer beteiligt sich wie?**, 2015
- **Das Recht auf Vergessenwerden**, 2015
- **Big Data**, 2016

Diskussionsbeiträge

- Völz/Janda: **Thesen zur Netzpolitik – Ein Überblick**, 2013
- Heckersbruch/Öksüz/Walter/Becker/Hertel: **Vertrauen und Risiko in einer digitalen Welt**, 2013
- Wewer: **Digitale Agenda 2013–2017: Netzpolitik im neuen Deutschen Bundestag**, 2013
- Meckel/Fieseler/Gerlach: **Der Diskurs zur Netzneutralität**, 2013
- Völz/Janda: **Netzpolitik in Deutschland – Wahlprogramme, Koalitionsvereinbarung, Regierungserklärung**, 2014
- Schubert: **Vertrauensmessung in der digitalen Welt**, 2014
- Baumann: **Privatsphäre als neues digitales Menschenrecht? Ethische Prinzipien und aktuelle Diskussionen**, 2015

Bücher

- Fischermann/Hamann: **Zeitbombe Internet**, Gütersloher Verlagsgruppe, 2012
- Bull: **Netzpolitik – Freiheit und Rechtsschutz im Internet**, Nomos Verlag, 2013
- Schliesky/Hoffmann/Luch/Schulz/Borchers: **DIVSI-Perspektiven: Schutzpflichten und Drittwirkung im Internet – Das Grundgesetz im digitalen Zeitalter**, Nomos Verlag, 2014
- Schliesky/Schulz: **DIVSI-Perspektiven: Die digitale Dimension der Grundrechte – Das Grundgesetz im digitalen Zeitalter**, Nomos-Verlag, 2015
- Paschek: **DIVSI-Perspektiven: Leadership in der digitalen Welt**, Nomos-Verlag, 2015

Unter **www.divsi.de** stehen die Studien und Diskussionsbeiträge kostenlos zum Download zur Verfügung.

DIVSI Deutsches Institut für Vertrauen und Sicherheit im Internet

www.divsi.de