Typoskript i. S. d. § 38 Abs. 2 UrhG
aus: Hill/Martini/Wagner (Hrsg.), Die digitale Lebenswelt gestalten, Baden-Baden 2015, S. 9-56

Wie werden und wollen wir morgen leben? – Ein Blick in die Glaskugel der digitalen Zukunft

Mario Martini

Übersicht

I. Sphären des digitalen Alltags der Zukunft 3
1. Mobilität 3
2. Arbeitswelt und Verteilung ihrer digitalen Dividende 5
a) Das Internet der Dinge als Quellcode einer neuen digitalen Revolution 5
aa) Funktionslogik des Internets der Dinge 5
bb) Standardisierung als Wettbewerb konkurrierender Systeme 6
cc) Verletzlichkeit der Systeme in integrierten Wertschöpfungsketten 7
b) Die Digitalisierung – Geburtsstunde einer neuen sozialen Frage? 7
aa) Veränderungen der Bedarfsstruktur 7
bb) Verteilung der digitalen Dividende 9
3. Privater Lebensraum 10
II. Der Nutzer im Zwiespalt zwischen convenience und surveillance 12
1. Digitaler Schattenriss 13
2. Das Privacy Paradox 14
3. Sorge vor einem digitalen Kapitalismus und Totalitarismus 16
4. Reaktionsmuster: zwischen digitaler Entschlackungskur und Schutzstrategien für die digitale Unversehrtheit 18
III. Der Status quo der Rechtsordnung und Entwicklungsoptionen de lege ferenda 19
1. Funktionswandel und Bew(ä/e)hrung der Grundrechte im digitalen Raum 19
2. Regulierungsbemühungen der Europäischen Union und Hoffnungen auf ein Völkerrecht für die digitale Welt 20
a) Die Datenschutz-Grundverordnung ante portas 21
b) Ein Internet-Völkerrecht zwischen Macht und Ohnmacht 23
3. Multi-Stakeholder-Ansatz und Selbstregulierung im Digitalisierungskontext 25

Seit der industriellen Revolution hat sich keine größere technologische und soziale Innovation vollzogen als die digitale Transformation. In Windeseile ist das Internet nicht allein zur zentralen (räumlich und zeitlich entgrenzten) technischen Infrastruktur der globalen Kommunikation, sondern auch zum Schwungrad industrieller Entwicklung avanciert. Seine disruptive Kraft setzt längst überkommene wirtschaftliche Geschäftsmodelle, Alltagsabläufe und Lebensentwürfe einem tief greifenden sozialen, technischen und kulturellen Wandlungsprozess aus.

Innovationsschübe gehören zur Biografie einer modernen Gesellschaft wie die Pubertät zur Entwicklung eines Menschen. Von früheren Entwicklungssprüngen der Menschheit, etwa der Erfindung des Buchdrucks oder der Eisenbahn, unterscheidet sich die digitale Revolution aber in einem wichtigen Aspekt: Während diese nur einzelne Lebensbereiche (mit Rückstrahlungen auf die Gesellschaft insgesamt) betrafen, legt die digitale Revolution eine Innovationsschicht über alle Lebens- und Arbeitsbereiche – von der Konsum- über die Arbeitswelt bis hin zur Partnersuche. Die digitale Revolution läutet auch einen Kulturwandel ein, der die Grundregeln unseres gesellschaftlichen Miteinanders einer Bewährungsprobe aussetzt. Bislang gesellschaftlich anerkannte »rote Linien« sozialer Normen, etwa das Tabu einwilligungslosen Fotografierens Dritter, lassen sich durch neue technische Möglichkeiten, wie etwa »Google Glass«,[1] unbemerkt übertreten. Die Technik verschiebt die Grenzen des Machbaren; das Machbare läuft der gesellschaftlichen Diskussion über das Wünschenswerte voraus und fordert unsere Gesellschaft zu einer Suche nach der ethischen Signatur der künftigen elektronischen Welt heraus: Wie wird und wie soll in der digitalen Welt das Verhältnis zwischen Privatheit und Öffentlichkeit ausgestaltet sein? Wird die Digitalisierung aller Lebensbereiche eine neue Blüte demokratischer Kultur in räumlich entgrenzten Gemeinschaften auslösen oder eher einer neuen Kultur der Überwachung, eines informatorischen Panoptikums, den Boden bereiten, in der – wie *Foucault*[2] es ausdrückte – die Macht bei denen liegt, die schweigen und beobachten, nicht bei denen, die sprechen und über sich Auskunft geben? Wer steuert und kontrolliert künftig die digitalen Ströme, auf die wir im Zeitalter des Internets angewiesen sind? Wie werden und wie wollen wir also morgen leben?

Mit diesen Herausforderungen lässt sich in zweierlei Weise umgehen: fatalistisch wie *Albert Einstein*, der gesagt haben soll: »Ich denke niemals an die Zukunft. Sie kommt früh genug«, oder optimistisch mit Neugierde und Gestaltungswillen wie *Alan Kay*: »Die Zukunft kann man am besten voraussagen, wenn man sie selbst gestaltet.« Der Wunsch, die Zukunft zu gestalten, verdient bei nüchterner Betrachtung einen stärkeren Impuls als kontemplatives Abwarten. Denn sie ist es, in der wir leben werden. Das *Comte*'sche Leitmotiv »Sehen, um vorauszusehen« ist Teil des Gebots einer rationalen Handlungswahl. Will die Gesellschaft nicht von der Faktizität technischer Entwicklungen überrollt werden, muss sie frühzeitig den Blick auf die Möglichkeiten und Grundfragen des digitalen Alltags der Zukunft richten. Das setzt eine Erschließung der technischen Grundlagen und Perspektiven voraus, auf deren Folie Visionäre die Parameter der Zukunft skizzieren und ein zweites Maschinenzeitalter[3] ausrufen.

Eine okkulte Kristallkugel, welche die Details des Lebens im Jahre 2025 sichtbar macht, steht dabei niemandem zu Gebote. Einige Entwicklungen zeichnen sich aber bereits heute klar ab – und mit ihnen zahlreiche Herausforderungen für die digitale Gesellschaft. Der Computerpionier *Alan Turing* hat sie mit den Worten beschrieben: »Wir können nur eine kurze Distanz in die Zukunft blicken, aber dort können wir eine Menge sehen, was getan werden muss.«

---

1 Die Aktivierung der Aufnahmefunktionen durch unauffällige Gesten oder ein Augenzwinkern ist weder für Gesprächspartner und noch weniger für Passanten erkennbar.

2 Der Gefangene solle niemals wissen, ob er zu irgendeinem Zeitpunkt beobachtet wird; aber er müsse sicher sein, dass er immer beobachtet werden kann. *Foucault*, Überwachen und Strafen: die Geburt des Gefängnisses, 14. Aufl., 2013 S. 258 f.

3 *Brynjolfsson/McAfee*, The second machine age, 2014.

I. Sphären des digitalen Alltags der Zukunft

Schenkt man den technischen Prophezeiungen Glauben, wird der Alltag der Zukunft vor allem eines sein: smart. Wir leben in Smart Homes einer Smart City, deren gesamte Verkehrsinfrastruktur digital vernetzt und der autonomen Steuerung von Smart Cars anvertraut ist.

Die Welt von morgen ist gespickt mit Sensoren. Sie begleiten den Einzelnen auf dem Weg zur Arbeit in der U-Bahn, im Auto, im Supermarkt und beim Sport. Sie dienen als physische digitale Zapfstellen der Internetkommunikation.[4] Die Vorboten der damit verbundenen vollständigen digitalen Vermessung sind bereits fester Alltagsbestandteil der »Digital Natives« von heute. Ihre sich abzeichnenden Fortschreibungen laden ein zu einem soziologisch-juristischen Erkundungsgang in die verschiedenen Sphären unserer künftigen digitalen Lebenswelten der Mobilität (1.), der Arbeitswelt (2.) sowie des privaten Lebensraums (3.).

1. Mobilität

Lange Zeit war das Automobil der Inbegriff für Individualität und Freiheit. Weder produzierte es noch konsumierte es digitale Daten. Der technologische Fortschritt unterwirft diesen Befund einem Wandel. In aktuellen Mittelklasse-PKW sind heute mehr als 20 Daten erzeugende und datenverarbeitende Steuergeräte verbaut und miteinander vernetzt – angefangen bei der elektronischen Zündung, über Tankstands- und Öldruckmesser bis hin zu komplexen Systemen wie ABS, Airbags und Fahrerassistenzsystemen. Unter ihren Kühlerhauben verbirgt sich mehr Steuerungstechnik als in den amerikanischen Mondraketen der sechziger Jahre.

In den nächsten 10 Jahren werden sich Autos weit stärker verändern als in den vergangenen 50 Jahren zuvor. Die Fahrzeugindustrie steht vor einem historischen Umbruch, der das Verhältnis zwischen Mensch und Auto neu definieren wird: Die Vision eines digitalen Autopiloten auf Rädern ist der alltagstauglichen Umsetzung sehr nahe. Seiner ursprünglichen griechischen Wortbedeutung macht das Auto der Zukunft alle Ehre. Es wird ein Rechenzentrum auf Rädern sein, das – gespickt mit Minikameras, Radartechnik und Sensoren – dem Fahrzeugführer wie von Geisterhand die Steuerung abnimmt.[5] Es reagiert auf Gesten und Augenbewegungen seiner Passagiere; die Fenster können die Insassen als Bildschirm nutzen, um während der Fahrtzeit im Internet zu recherchieren, ein geschäftliches Videotelefonat zu führen oder sich durch einen Film unterhalten zu lassen.

Das autonome Fahrzeug denkt mit. Wird morgens um 7:30 Uhr der Kofferraum beladen und werden die Gurte des Fahrersitzes sowie der beiden Rücksitze angelegt, weiß der Autopilot: Fahrziel ist die Schule. Er nimmt selbsttätig den besten Weg – samt Abstecher zum Bäcker. Auf der Grundlage der gespeicherten Daten sowie via Eye-Tracking stellt der Smart Car selbstverständlich auch die gewünschte Sitzstellung, Klimatisierung sowie Musik ein.

Seine Annehmlichkeiten sollen den Menschen die beim herkömmlichen Fahren verlorene Zeit für andere Verwendungen schenken. Aufmerksamkeit und Fahrleidenschaft sind nicht mehr vonnöten. In seinem Prototyp des selbstfahrenden Autos hat Google deshalb mit radikaler Konsequenz nicht einmal mehr ein Lenkrad oder Pedale verbaut. Der »Computer auf Rädern« ist fortlaufend mit der Datenzentrale seines Herstellers verbunden. Dorthin sendet es auch seine Standort- und telemetrischen Daten.

---

4 Das Smartphone büßt dann seine Schaltstelle als Funkzentrale für alle persönlichen Daten ein Stück weit ein. An seine Seite tritt in einigen Bereichen eine Vielfalt von an das Internet gebundenen Alltagsgeräten.

5 Vgl. dazu etwa *Köhler/Wollschläger*, Die digitale Transformation des Automobils, 2014; *Rubinyi*, The Car in 2035, 2014.

Ebenso wie das Automobil der Zukunft automatisierte Entscheidungen trifft und mit seiner Umgebung vernetzt ist, verhält es sich auch mit der smarten Verkehrssteuerung von morgen: Bordcomputer und Motor kommunizieren nicht nur mit allen Bauteilen des digitalen Autopiloten, sondern auch mit anderen am Verkehr teilnehmenden Fahrzeugen, warnen diese etwa vor Glatteis oder einem unvermittelten Stauende. In die Fahrbahn eingelassene Sensoren zählen Fahrzeuge, messen Geschwindigkeiten und organisieren den öffentlichen wie individuellen Personenverkehr. Die digitale Steuerung der Verkehrssysteme minimiert dadurch den Risikofaktor »Mensch« und senkt so Unfallgefahren, die der Preis für die bisherige »freie Fahrt für freie Bürger« waren. Gegenwärtig gehen 90 % aller Unfälle auf Fahrfehler zurück. Die Automatisierung wird diese Zahl drastisch reduzieren. Die Vision vom unfallfreien Straßenverkehr wird womöglich Realität.

Zugleich ebnen Automatisierung und Vernetzung einer effizienten Ausnutzung der Verkehrsinfrastruktur unter den Bedingungen erhöhter allgemeiner Mobilität den Weg. Der Verkehrsfluss in der Smart City[6] kennt keine Staus und keine langen Wartezeiten an Bushaltestellen oder Bahnhöfen. Denn die digitale Koordination über die verschiedenen Verkehrssysteme hinweg optimiert Verkehrsabläufe in einem antizipatorischen System, dessen technische Möglichkeiten schon heute die Fantasie der Stadtplaner beflügelt. Die automatisierte Verkehrssicherung gestattet es, die Sicherheitsabstände zwischen Fahrzeugen zu reduzieren, dadurch den Verkehrsfluss zu verbessern, insbesondere ein Vielfaches des bisher üblichen Fahrzeugdurchsatzes zu erreichen, und manche Fläche, die bislang die Verkehrsinfrastruktur eingenommen hat, anderen Zwecken zugänglich zu machen.

Die Automatisierung kann aber nicht nur wie ein Bremsklotz auf die Freude am Fahren wirken. Sie ist auch grundrechtssensibel, fordert sie doch eine absolute Transparenz der Fahrzeugnutzung. Mobilitätsdaten lassen sich nicht nur zur Funktionsprüfung, sondern auch zur Erstellung von Bewegungs- und Handlungsprofilen nutzen. Smart Cars und Smart Cities projizieren das Bild des gläsernen Autofahrers bzw. Fahrgasts an die Zukunftsleinwand, dessen autonome Verfügungsgewalt über seine Daten den Effizienzvorteilen digitaler Mobilität Platz macht.[7]

Mit der autonomen Steuerung tritt der Mensch auch einen Teil seiner ethischen Steuerungsmacht an den Algorithmus ab, der die Handlungsanweisungen trifft. Eine automatisierte Verkehrswelt lässt keinen Platz mehr für individuelle Entscheidungen am Lenkrad. Das gilt auch für Dilemmaentscheidungen – etwa die Entscheidung, ob das Fahrzeug dann, wenn unvermittelt ein Kind auf die Fahrbahn läuft, eher das Leben des Kindes, unbeteiligter Dritter oder der Fahrzeuginsassen aufs Spiel setzt. Die digitale Programmierung ethischer Dilemmaentscheidungen braucht einen Wertekompass für Entscheidungsregeln und Präferenzmuster. Damit verbindet sich auch eine Chance: Während bislang Konfliktsituationen und Unfallszenarien der Intuition und Reaktionskraft menschlicher Entscheidungen überantwortet waren, sind sie nun einer Steuerung zugänglich. Ihre Steuerung darf entsprechend auch nicht alleine der ethischen Wertung und den Interessen von Ingenieuren und Informatikern überlassen bleiben. Sie ist auf einen normativen Rahmen angewiesen, der gesellschaftlichen Präferenzen und Wertmuster in einer Welt automatisierter Entscheidungen zum Durchbruch verhilft. Das ethische Setting der Algorithmen muss den gesellschaftlichen Wertvorstellungen entsprechen – nicht umgekehrt.

---

6 Vgl. zum Begriff und zum ökonomischen Potenzial etwa *VDE*, VDE-Trendreport 2014 - Schwerpunkt: Smart Citys, 2014, S. 4 f.

7 Zu den damit verbundenen datenschutzrechtlichen Herausforderungen siehe den Überblick bei *Buchner*, DuD 2015, 372 ff.; *Cichy*, PinG 2 (2014), 200 ff.; *Hansen*, DuD 2015, 367 ff.; *Kinast/Kühnl*, NJW 2014, 3057 ff.; *Hornung/Goeble*, CR 2015, 265 (269 ff.); *Kremer*, RDV 2014, 240 (243 ff.); *Rieß/Agard*, PinG 2015, 98 (99 ff.); *Roßnagel*, DuD 2015, 353 ff.; *Rammo/Holzgräfe*, Datenschutz bei vernetzten Autos – elektronische Fahrtenbücher, in: Taeger (Hrsg.), Big Data & Co, 2014, S. 351 ff.; zur Verfügungsbefugnis über Fahrzeugdaten *Hornung*, DuD 2015, 359 ff.; *Kraus*, Telematik – wem gehören Fahrzeugdaten?, in: Taeger (Hrsg.), Big Data & Co, 2014, S. 377 (379 ff.).

Mit der algorithmischen Programmierung eng verknüpft sind bislang ungeklärte Haftungsfragen, die sich mit möglichen technischen Fehlern automatisierter Fahrzeugsysteme verbinden, so etwa: Wer haftet im Falle eines Auffahrunfalls, der durch das Funktionsdefizit eines sich selbst steuernden Fahrzeugs entstanden ist: der Fahrzeughalter, der Hersteller oder gar die Allgemeinheit?[8] Wie auch bei anderen technischen Entwicklungen, die Gefahren induzieren, welche die Gesellschaft aber als beherrschbar einstuft, wird eine allgemeine Gefährdungshaftung eine rechtstechnisch sinnvolle Zurechnungslösung etablieren: Derjenige, der durch die Nutzung technischer Systeme ein Risiko setzt, haftet dann ohne Rücksicht auf ein Verschulden für den Schaden, den die Nutzung des technischen Systems im Einzelfall hervorgerufen hat.

2. Arbeitswelt und Verteilung ihrer digitalen Dividende

a) Das Internet der Dinge als Quellcode einer neuen digitalen Revolution

Nicht nur auf der Straße, sondern auch in den Werkhallen der Zukunft realisiert sich die Vision der vollendeten Automatisierung: Die Smart Factory stellt die Produkte weitgehend autonom her. Alle Maschinen sind via IP-Adresse vernetzt. Der klassische Produktionsprozess bestand bislang aus weitgehend voneinander abgeschichteten Produktionswelten. Diese greifen in der Smart Factory ineinander. Zwischen den Wertschöpfungsstufen ergießt sich ein reicher Daten- und Informationsstrom.

aa) Funktionslogik des Internets der Dinge

In dem Internet der Dinge, einem Machine-to-machine-Internet,[9] das sich aus in physikalische Objekte integrierten Computersystemen zusammensetzt, verfügen alle Gegenstände über einen eigenen RFID-Chip. Sie koordinieren und steuern sich wechselseitig: Die digitale Lagerverwaltung meldet, welche Produkte benötigt werden. Die Maschinen signalisieren, welche Bauteile sie für die Zusammensetzung brauchen und bestellen selbsttätig Fertigungsmaterial. Anlagen reagieren autonom auf Störungen und Umweltveränderungen, simulieren verschiedene Produktionsszenarien und entscheiden sich auf der Grundlage eines Ergebnisabgleichs ihrer Rahmendatenanalyse für das geeignetste Verfahren.

Sensoren erfassen sämtliche Funktionsdaten über den Zustand von Anlagen, durchsuchen die Werkmaschinen auf Muster, die drohende Störungen erkennen lassen, und ermöglichen dadurch eine präventive Wartung. In der Smart Factory denken nicht nur Menschen, sondern auch Maschinen: Die Maschinen werden intelligent; sie konfigurieren, optimieren und regulieren sich durch stete wechselseitige Rückkopplung selbst, ohne dass es eines programmierenden Eingreifens von außen bedarf. Der Mensch bleibt der Dirigent in dem Wertschöpfungskonzert der Produktion. Das Orchester aber besteht aus einem konzertanten Zusammenspiel von Mensch und Technik.

Statt durch zentrale Steuerung wird die Produktion über dezentrale autonome Selbstorganisationseinheiten organisiert. So entsteht eine effiziente Interaktion zwischen Produkt und Produktion sowie zwischen Produzent und Verbraucher, die Arbeitsabläufe und Fertigungsstrukturen beschleunigt und

---

8 Zu den haftungsrechtlichen, strafrechtlichen und zulassungsrechtlichen Implikationen *Lutz*, NJW 2015, 119 ff.

9 Im angelsächsischen Raum firmiert das »Internet der Dinge« daher auch unter dem Begriff »Industrial Internet«. Zu den datenschutzrechtlichen Herausforderungen siehe auch *Artikel-29-Datenschutzgruppe*, Opinion 8/2014 on the Recent Developments on the Internet of Things, WP 223, 2014.

flexibilisiert. Die Smart Factory ermöglicht dadurch Fertigung in kleinsten Losgrößen, schafft Geschäftsmodelle, die den gesamten Lebenszyklus von Produkten abdecken und verkürzt damit die Reaktionszeit auf Marktveränderungen.[10] Die horizontale Integration in globale Wertschöpfungsnetzwerke senkt die Instandhaltungskosten, erhöht die Produktivität sowie die Qualität und die Transparenz des Produktionsprozesses. Die verbesserte Effizienz der Betriebsabläufe schont Ressourcen, reduziert damit die Umweltbelastung und verleiht Innovationen im Idealfall über alle Produktionslebenszyklen hinweg einen Schub.

In diesen Entwicklungen liegt der Quellcode einer vierten industriellen Revolution, die nach dem Vorbild der vorangegangenen industriellen Revolutionen[11] Basisinnovationen mit langwelligen Konjunkturzyklen auszulösen verspricht. Mit ihrem disruptiven Potenzial läutet sie ein neues Zeitalter der Produktion ein, indem sie eine Brücke zwischen den Möglichkeiten der digitalen IT-Welt und der analogen Produktionslandschaft schlägt.

bb) Standardisierung als Wettbewerb konkurrierender Systeme

Die vollständige Vernetzung aller Produktionsprozesse setzt eine Standardisierung der Schnittstellen und Normung der technischen Standards voraus, um eine babylonische Sprachverwirrung zwischen den Maschinen und Plattformen zu verhindern. Standardsetzung entpuppt sich hier in besonderer Weise als Wettlauf konkurrierender Systeme: Wer die Standards definiert, liefert den Grundriss für die Architektur der digitalen Plattform der Zukunft. Er hat in dem Rennen um die Datenhoheit einen entscheidenden Wettbewerbsvorteil.[12] Die Startplatzierungen dafür werden heute verteilt.

---

10 Davon profitieren besonders Industriezweige mit sehr kurzen Produktionszyklen, wie die Verpackungsindustrie oder die Handyherstellung. 3D-Druck ergänzt bzw. ersetzt dabei konventionelle Fertigungstechnologien, erleichtert insbesondere die Fertigung von Ersatzteilen und die Individualisierung der Produktion, indem er auf der Grundlage detailscharfer Computervorlagen komplexe Komponenten schichtweise zu Fertigungsteilen aufbaut, ohne dass diese von Menschenhand geschweißt, gefräst oder gegossen werden bzw. lange Transportwege aus dem Herstellungsland in Kauf genommen werden müssen – von der Plastikfigur über das Ersatzteil des Staubsaugers bis hin zur einer zweistöckigen Villa (vgl. etwa *Ankenbrand*, Eine Villa aus dem 3D-Drucker, FAZ vom 6.3.2015, S. 22; zu den immaterialgüterrechtlichen Implikationen *Nordemann/Rüberg/Schaefer*, NJW 2015, 1265 ff.; *Solmecke*, Rechtliche Aspekte des 3D-Drucks, in: Taeger (Hrsg.), Big Data & Co, 2014, S. 283 ff.). Das senkt zum einen die Produktions-, zum anderen die Vorhaltekosten für (später nicht unbedingt benötigte) Bauteile und verkürzt die Absatzwege sowie Fertigungszeiten. Die Technologie macht sogar Bio-Printing-Verfahren vorstellbar, welche in Massenverfahren Produkte herstellen, die organischen Bestandteilen äquivalent sind. Bio-Printing reproduziert dann aus zuvor gezüchteten Zellen organisches Gewebe, aus dem nach heutigen Visionen eine Niere, eine Leber oder sogar ein Herz entstehen kann.

11 Erst zogen Wasser- und Dampfkraft in die Fabriken ein (Industrie 1.0 ab 1784) und ersetzten menschliche und tierische Arbeitskraft durch Maschinen. Mit ihrer Elektrifizierung, der arbeitsteiligen Massenfertigung auf Fließbändern sowie der Verbesserung der Logistik durch den verstärkten Eisenbahnbau rollte ab 1870 die zweite industrielle Revolution vom Band (Industrie 2.0). Dann kam die automatisierte Steuerung durch Computer und Software hinzu (Industrie 3.0 ab 1970). Die Industrie 4.0 verbindet diese Produktionsansätze nun miteinander zu einer übergreifenden digitalen Kommunikationseinheit.

12 Dazu und zum Zusammenspiel von technischen Standards und Patentrechten *Ullrich*, GRUR 2007, 817 ff.

cc) Verletzlichkeit der Systeme in integrierten Wertschöpfungsketten

Jede Schnittstelle in einer Welt der Industrie 4.0, über welche die Maschinen sowie Produkte miteinander kommunizieren, eröffnet zugleich eine potenzielle Angriffsfläche, mit deren Hilfe sich Dritte Zugänge zu sensiblen Informationen verschaffen können. Diese gilt es, vor unerwünschten Zugriffen zu schützen. Die Angreifbarkeit von Fertigungsdaten, Betriebsgeheimnissen und ganzen Wertschöpfungsketten ist die empfindliche Kehrseite vollständiger Vernetzung.

Die Produktionsprozesse der Smart Factory sind verwundbar durch jegliche Form des Angriffs aus dem Cyberspace, sei es Industriespionage, sei es nachrichtendienstliche Überwachung, seien es Sabotageakte. Längst sind es insbesondere nicht mehr nur kriminelle Gruppen, die Schadsoftware mit der Zielsetzung programmieren, in Computersysteme eindringen und dort wirtschaftlichen Schaden anrichten zu können. Immer häufiger sind es Konkurrenzunternehmen, die den Vorsprung des Technologieführers und anderer Wettbewerber einzuholen und deren Know-how abzugreifen versuchen. Um sich darauf Zugriff zu verschaffen, genügt der Angriff auf ein einziges Objekt entlang des Produktionsprozesses.

Nicht alleine eigene, sondern auch fremde Infrastrukturen können zum Waffenlager von Cyberangriffen werden. Die Störung eines Systems kann eine Kette von Reaktionen in fremden Systemen auslösen. Die wachsende Zahl von Angriffspunkten wirksam zu schützen, ist entsprechend eine der zentralen Herausforderungen digitaler Industriepolitik: Alle Industriesektoren haben ein vitales Interesse an der Absicherung ihrer Wertschöpfungsnetzwerke gegen den unberechtigten Zugriff von außen.[13] Die Wehrfähigkeit der Sicherheitsarchitektur ist ein Schlüsselfaktor für die Verantwortbarkeit der neuen technologischen Produktionsmöglichkeiten. Nicht zuletzt hängt von dem Vertrauen in die Sicherheit die Bereitschaft zu ihrem Einsatz ab. Bedrohungen zu erkennen und sie zu bekämpfen, bevor ein Schaden entstehen kann, darf daher auch in einer Welt vernetzter Maschinen nicht nur eine Vision bleiben. Die Herstellung von Sicherheit gleicht dabei immer mehr dem Kampf gegen eine Hydra, deren Köpfe so schnell nachwachsen, wie die bereits erkannte Gefahr gebannt wird.

b) Die Digitalisierung – Geburtsstunde einer neuen sozialen Frage?

Die Fabrik der Zukunft senkt die Grenzkosten für die Herstellung von Waren und Dienstleistungen drastisch. Sie macht insbesondere Arbeiten entbehrlich, die durch einen hohen Grad an Routine oder körperlicher Anstrengung gekennzeichnet sind. Eine Welt, in der Menschen nicht mehr eintönige, die körperliche Gesundheit gefährdende Arbeiten verrichten müssen, wird vorstellbar. Die entsprechenden Zeitressourcen und Fähigkeiten stehen für kreative, dem Menschen mit seinen besonderen Begabungen und seiner intellektuellen Kapazität zugänglichere Tätigkeiten zur Verfügung.

aa) Veränderungen der Bedarfsstruktur

Die vernetzte Welt überträgt digitalen Sklaven lästige und unangenehme Tätigkeiten einer Wohlstandsgesellschaft. Sie stellt aber auch dem einfachen Arbeiter der bisherigen Mittelschicht nicht mehr ohne Weiteres die überkommenen Strukturen bisheriger Arbeitsplätze in gewohnter Form und Menge zur Verfügung. Die Zahl der in der Fertigung oder Dienstleistungserbringung benötigten Mitarbeiter sinkt

---

13 Vgl. auch zum Datenschutz im Internet der Dinge: *Artikel-29-Datenschutzgruppe* (Fn. 9), S. 1 ff. sowie zu den haftungsrechtlichen und produktsicherheitsrechtlichen Herausforderungen *Bräutigam/Klindt*, NJW 2015, 1137 (1138 ff.).

rapide. Einfache Fertigungsprozesse – im Grundsatz alle Tätigkeiten, die wenig soziale oder kreative Intelligenz bzw. keine komplexe Analyse ihrer Umgebung erfordern – können Maschinen und ihre technischen Assistenzsysteme übernehmen. Sicher: Die kognitive und haptische Flexibilität eines Arbeiters an der Werkbank lässt sich durch algorithmengesteuerte Roboter nicht ohne Weiteres vollständig ersetzen. Aber die Industrie 4.0 wird sie ergänzen. Die Bedien- und Programmierbarkeit, Einsatztauglichkeit und Fehlerresistenz moderner Roboter verbessern sich stetig. Während sie noch vor nicht allzu langer Zeit bereits an einfachsten motorischen Aufgaben scheiterten, sind sie inzwischen in der Lage, komplexe Aufgaben zuverlässig zu erfüllen. Die Verbreitung der Robotertechnologie im Alltag steht vor einem Durchbruch. Die Einführung von Mindestlöhnen verleiht dieser Entwicklung zusätzlichen Schub: Sie verschiebt die Renditekurve zusätzlich zugunsten der maschinellen Produktion von morgen.

Nachhaltige Umbrüche sagen Experten insbesondere dem Dienstleistungssektor voraus. Dort kommt der Robotik sogar ein noch größeres Potenzial zu als in der Industrie.[14] Digitale Assistenzsysteme, welche die Robotik dank ihrer technischen Entwicklungssprünge der jüngeren Zeit und drastisch sinkender Herstellungskosten (die teilweise ein Hundertstel der früheren Kosten betragen) hervorbringt, finden ihre Einsatzfelder insbesondere als Helfer im Haushalt, bei der Pflege älterer Menschen und in der Logistik. Sie stehen rund um die Uhr zur Verfügung, machen keine Pausen, vergessen ihre einstudierten Aufträge und Arbeitsrhythmen nicht, begehen bei ihren automatisierten Entscheidungen keine Flüchtigkeitsfehler, brauchen keinen Urlaub, fallen nicht krankheitsbedingt aus und organisieren sich nicht in Interessenvereinigungen, Betriebsräten und Gewerkschaften.

Dem Exklusivbereich menschlicher Entscheidung bleiben damit langfristig nur noch die Vorbereitung und Überwachung der elektronischen Steuerung, das Lösen komplexer Probleme sowie wichtige Strukturentscheidungen in laufenden Prozessen vorbehalten – jeweils unterstützt durch digitale Agenten, welche die Fülle der Daten auswerten und Vorschläge unterbreiten. Nicht das Abarbeiten eines Auftrags, sondern die Steuerung laufender Produktionsprozesse wird zukünftig als besondere menschliche Leistung gefragt sein. Das Anforderungsniveau an diese spezielle Mitarbeiterequipe und der Bedarf an Berufen, die auf eine besondere soziale und kreative Intelligenz ihrer Ausübenden angewiesen sind, werden tendenziell steigen. Das gilt etwa für diejenigen Tätigkeitsbereiche, deren Kerngehalt darin besteht, auf andere Menschen und ihre Bedürfnisse einzugehen, sie zu betreuen oder ihnen in einer individuellen Problemlage helfend zur Seite zu stehen. Diese Leistungen und Fähigkeiten sind durch eine Automatisierung des Geistes[15] am schwersten ersetzbar.

Empathie hat bisher noch keine Maschine erlernen können. Wenn sich Prozesse in kurzen Abständen ändern, ist der Mensch (jedenfalls bislang noch) flexibler als ein programmierter Roboter. Anderes gilt demgegenüber für diejenigen Entscheidungen, welche auf der Grundlage einer umfassenden Datenanalyse und Datenauswertung rekonstruierbar sind, etwa die Aufgaben von Kassierern, Buchhaltern und Kreditanalysten.[16] Diese Arbeitnehmergruppen werden den Kampf um ihren Arbeitsplatz im Zweifel gegen Maschinen verlieren.

---

14 Das *McKinsey Global Institute* geht davon aus, dass das potenzielle jährliche Marktvolumen der Robotik in Höhe von 1,7 bis 4,5 Billionen USD mit mehr als 0,8 bis 2.6 Billionen USD allein im Gesundheitssektor verortet ist, vgl. *Manyika/Chui/Bughin et al.*, Disruptive technologies: Advances that will transform life, business, and the global economy, 2013, S. 68.

15 *Kurz/Rieger*, Arbeitsfrei, 2015, S. 241.

16 Siehe auch die umfassende Auflistung bei *Frey/Osborne*, The Future of Employment, 2013, 57 ff.

bb) Verteilung der digitalen Dividende

In der Tiefe ihrer Einschnitte für die Arbeitswelt unterscheidet sich die digitale von der industriellen Revolution. Während letztere vergleichsweise hoch bezahlte handwerkliche Tätigkeit durch Fließbandarbeit ersetzte, die mehr Arbeiter, aber weniger Qualifikationen erforderte, wird die Industrie 4.0 die arbeitenden Menschen selbst entbehrlich machen.

Zugleich ging nahezu jeder Produktivitätsfortschritt und jede Innovation in der Menschheitsgeschichte bisher in der Regel mit einem Bedarf an neuen Arbeitskräften einher. So wird auch die digitale Revolution eine Vielzahl neuer Tätigkeitsfelder entstehen lassen – so wie sie bereits den Beruf des Datenanalysten oder Unternehmen für Klingeltöne von Mobilfunkgeräten geschaffen hat. Andere überkommene Tätigkeitsfelder werden sich wandeln und unter veränderten Bedingungen mit neuen Aufgaben fortbestehen – ähnlich wie sich in den letzten Jahrzehnten etwa das Arbeitsfeld der Sekretärin radikal gewandelt hat und nach der technischen Vorstellungswelt der siebziger Jahre heute als Beruf eigentlich nicht mehr in gleichem Umfang existieren dürfte. Denn viele ihrer tradierten Arbeitsfelder, etwa das Abtippen von Texten oder die Buchung von Reisen, lassen sich heute unter Inanspruchnahme digitaler Assistenzsysteme deutlich schneller erledigen. Dafür sind die an Sekretärinnen gestellten Anforderungen an das Terminmanagement und die Büroorganisation sowie Ablaufkoordination in einer dynamischer werdenden Welt gestiegen, welche sie weiterhin zu einer vielfach unentbehrlichen Hilfe im Arbeitsalltag machen.

Die Bedeutung der Arbeit als Kostenfaktor in der Produktionskette wird aber tendenziell (weiter) fühlbar abnehmen; die Prämie für qualifizierte Arbeit sinkt ebenso wie die Lohnquote, also der Anteil des Volkseinkommens, der auf die Beschäftigten entfällt, und der Anteil der Lohn- an den Herstellungskosten. Standortentscheidungen werden in Zukunft weitaus weniger als früher von dem Zugang zu Arbeitskräften an der Produktionsstätte, sondern stärker von anderen Standortfaktoren, wie etwa der Nähe zum Absatzmarkt, den steuerlichen und sonstigen regulatorischen Rahmenbedingungen sowie der verfügbaren Infrastruktur, abhängig sein.

Nicht nur die Anspruchslosigkeit und Leistungsstabilität von Robotern reduzieren den Wert steter Bindungen zwischen Arbeitnehmer und Arbeitgeber. Auch Arbeitsmodelle werden individueller, Zeitsouveränität gewinnt an Bedeutung. An die Stelle der überkommenen Präsenz- tritt eine Ergebniskultur. Crowdworking-Modelle erlauben eine situative Mitwirkung Externer, die zum kreativen Potenzial und Erfahrungswissen des fest angestellten Mitarbeiters in Konkurrenz treten.[17] Die Transaktionskosten, die das Aushandeln von Verträgen und die Suche nach geeigneten Arbeitskräften auslösen und als solche die Existenz der Arbeitnehmer-Arbeitgeber-Beziehung in Unternehmen ökonomisch erklären,[18] sinken drastisch.

Die Industrie 4.0 löst damit die Geschäftsgrundlage des alten Verteilungskonsenses und der ihm innewohnenden Richtigkeitsvermutung auf. Während sich in der Vergangenheit Arbeitgeber und Arbeitnehmer auf der Grundlage tarifvertraglicher Vereinbarungen die Produktivitätsfortschritte teilten, wird der einfache Arbeiter mithilfe der wirtschaftlichen Drohung einer Arbeitsniederlegung seinen Anteil am wirtschaftlichen Gesamtertrag der Gesellschaft nicht mehr in gleicher Weise einfordern können. Seine Arbeitsleistung wird zur Herstellung der Produkte nicht mehr benötigt. Entsprechend ist ihm der erzielte Produktivitätsfortschritt der Zukunft nicht mehr zurechenbar. In der Gesellschaft der Industrie 4.0 stellt sich mithin die Frage nach der gerechten Verteilung der im wirtschaftlichen Wertschöpfungsprozess erzielten Wohlstandsgewinne und Vermögen neu.

---

17 Vgl. dazu den Beitrag von *Tapper* in diesem Band.

18 *Coase*, Economica 4 (1937), 386 ff.

In den USA erzählt man sich scherzhaft-ironisch die Geschichte von der Begegnung eines Unternehmensvorstandes und eines Gewerkschaftschefs in der modernen, hochautomatisierten Fabrikhalle der Zukunft. Mit herablassendem Sprachduktus fragt der Vorstand den Gewerkschafter: »Wie willst du meine Roboter dazu bringen, für deine Gewerkschaft zu streiken?«. Der Gewerkschafter kontert schmunzelnd: »Wie willst du deine Roboter dazu bringen, deine Autos zu kaufen?«

Dass auch heute schon in den USA die Ungleichheit der Einkommen tendenziell wächst, passt womöglich zu dem Bild dieses Zukunftsszenarios: Der Reallohn der Masse der Beschäftigten stagniert, während der Anteil der am besten verdienenden Bevölkerungsschichten am Bruttosozialprodukt stetig zunimmt.[19] Viele sehen einen intellektuellen Kapitalismus heraufziehen[20] – und damit die Wiederkehr aristokratischer Gesellschaftsstrukturen vorangegangener Jahrhunderte, die es einer kleinen Schicht von Menschen erlaubt, einen erheblichen Teil der volkswirtschaftlichen Ressourcen auf sich zu vereinen.[21]

Die Ballung wirtschaftlicher Macht in den Händen Weniger macht den Staat auf der einen Seite durch diese Gruppe erpressbar. Auf der anderen Seite wächst dem Staat als Verteilzentrum des gesellschaftlichen Produktivitätsfortschritts eine zentrale, immer wichtiger werdende Gestaltungsrolle zu. Handeln Arbeitnehmer und Arbeitgeber das Verteilungsergebnis nicht mehr wie bisher im Interessenkampf aus, muss der Staat noch stärker als früher mit seinen Instrumenten steuerlichen Zugriffs auf den wirtschaftlichen Ertrag die Rolle des verteilenden Akteurs einnehmen, wenn er die wirtschaftliche Machtasymmetrie zwischen beiden Gruppen ausgleichen will.

Dazu genügt im Zweifel weder eine bloße kosmetische Korrektur noch ein einfaches Facelifting des überkommenen Steuermodells. Um die Staatsfinanzierung beim Sprung in die autonomisierte digitale Gesellschaft vor einer Bauchlandung zu bewahren, wird vielmehr vermutlich ein grundlegender Umbau der Steuer- und Sozialsysteme erforderlich sein, der auch denjenigen, deren körperliche Arbeitsleistung die digitale Gesellschaft nicht mehr benötigt, eine Teilhabe an der wirtschaftlichen Wertschöpfung und am gesellschaftlichen Leben ermöglicht. Die digitale Rationalisierung menschlicher Arbeit und das damit einhergehende Wegbrechen der Lohn- und Einkommenssteuererträge als einer zentralen Säule der Finanzierung unseres Gemeinwesens wird ein Nachdenken über die Besteuerung der menschliche Arbeitskraft substituierenden Leistung von Robotern auslösen sowie der alten Diskussion um das Modell der Vermögensteuer neue Nahrung geben.

3. Privater Lebensraum

Die Wohnung der Zukunft wird gespickt sein mit intelligenten Sensoren. Diese verinnerlichen die Muster, nach denen die Bewohner ihren Alltag bestreiten, und passen auf dieser Grundlage die Raumbedingungen autonom an deren Bedürfnisse an: Das elektronische Schaltsystem regelt rechtzeitig vor Eintreffen des Wohnungsinhabers Beleuchtung, Temperatur sowie den Funktionsstatus der Haushaltsgeräte. Es erkennt, welche Räume beheizt werden müssen. Alle wichtigen Funktionsgeräte – vom Fernseher über die Musikanlage und den Geschirrspüler bis zur Heizung und zur Photovoltaikanlage – sind mit einer eigenen IP-Adresse ausgestattet und über diese miteinander verbunden. Der Kühlschrank hat den Lieblingskäse, der schon fast aufgebraucht war, selbsttätig nachbestellt. Der Koch-Roboter bereitet die

---

19 *Stiglitz*, Der Preis der Ungleichheit, 2012, S. 29 ff.

20 Vgl. etwa *Kaku*, Die Physik der Zukunft, 6. Aufl, 2013, S. 471 ff.

21 Vgl. dazu etwa *Piketty*, Le capital au XXIe siècle, 2013, der mit seinem Werk sehr viel Aufmerksamkeit auf sich gezogen und eine neue gesellschaftspolitische Verteilungsdebatte ausgelöst hat. Siehe auch *Frey/Osborne* (Fn. 16), 14 ff.; *Brynjolfsson/McAfee*, Race against the machine, 2012.

Cremesuppe und den Hauptgang nach dem Rezept und entsprechend den Künsten eines Dreisternekochs selbsttätig zu. Intelligente Gebäudetechnik steigert die Eigenverbrauchsquote und den effizienten Einsatz von Wasser und Strom. Die »smarte« Waschmaschine reguliert die Wassertemperatur so, dass die Enzyme bei der jeweils gewaschenen Kleidung ideal wirken können. Dazu tritt die »smarte« Kleidung via Chip mit dem Prozessor der Waschmaschine in Verbindung. Das digitale Haushaltssystem lässt den Waschgang selbstverständlich zu einem Zeitpunkt starten, zu dem der Strom besonders günstig ist. Energieversorger passen ihre Kraftwerke auf der Grundlage einer Zusammenführung technisch generierter Nutzungsdatenprognosen und einer dezentralen, auf der Auswertung von Wetterdaten beruhenden Kraftwerkssteuerung regenerativen Energieträgern an.

Die digitale Ökonomie wird im Zweifel weniger durch individuelles Eigentum und damit verbundenen Ausschließlichkeitsrechte an jedem genutzten Alltagsgegenstand, etwa dem Auto, Haushaltsgeräten oder Maschinen, geprägt sein als durch eine Ökonomie des Teilens und des Besitzes (sog. Share Economy), die auf einem Pay-per-use-Ansatz aufbaut.[22] Eine Kultur des Teilens löst ein Stück weit die kapitalistische Kultur des Eigentums ab.[23] Sie ermöglicht, jeden gekauften in einen kurzfristig zu geringen Transaktionskosten leihbaren Gegenstand zu verwandeln und beflügelt damit die effiziente Nutzung knapper Ressourcen in einer globalisierten Welt.

Das Lernen wird sich in Zukunft nicht mehr unbedingt in den festen Lernrhythmen und Umgebungen des Klassenraums vollziehen, sondern radikalen Wandlungen der Individualisierung unterworfen sein. Personalisierte Lernprogramme (Customized Learning Programs) aggregieren in Echtzeit Lernaufgaben, welche auf den Entwicklungs- und Wissensstand sowie den augenblicklichen Aufenthaltsort und Handlungskontext des Schülers maßgeschneidert abgestimmt sind. Die schablonenartige Modularisierung von Lerninhalten entlang traditioneller Lehrpläne, die sich persönlichen Lernfortschritten und Ausgangspunkten des Wissens nicht anpassen, gehört im Zweifel der Vergangenheit an.[24] Ein individuell gestaltetes, weitgehend von Ort und Zeit entgrenztes »Lebenslanges Lernen« tritt an seine Stelle.

Das Buch, mit dem der Mensch von morgen seinen Tag ausklingen lässt, schreibt sich in einem interaktiven Koproduktionsprozess zwischen dem Autor und seinen Lesern fort. In diesen kreativen Entwicklungsvorgang ist der Verleger als elektronischer Mittler zwischengeschaltet. Seine Lesegeräte analysieren, welche Stellen besonders gerne gelesen werden und wo sich die Aufmerksamkeit des Lesers verliert: Dass Amazon die Rolle der reinen Verkaufsplattform abstreift und selbst zum Verleger geworden ist, ist insofern wohl auch kein Zufall, sondern ein Vorbote dieser Entwicklung. Mit seinen Milliarden von Kundendaten und der Analyse der individuellen Lesegewohnheiten via Kindle lässt sich das kollektive Leseverhalten effizient und zuverlässig ermitteln. Während der Leser in den literarischen Welten eines E-Books umherstreift, schaut ihm Big Brother über die Schulter. Das Buch mutiert dadurch von einer Erkenntnis- zur Überwachungsquelle. So erschließt sich die Welt der Algorithmen Stück für Stück auch die letzte Bastion menschlicher Erlebniswelten, die ihr bislang weithin verschlossen war: die Gefühlswelt. Eine ganze Wissenschaftsdisziplin – Affective Computing – begibt sich mit dem Anspruch, die menschlichen Emotionen auf der Grundlage von Daten aufzuspüren und auszuwerten, an die Datenanalyse.

Auch vor dem kulturellen Genuss im Theater wird diese Entwicklung in Zukunft wohl nicht haltmachen: In Spanien haben die Betreiber des »Teatreneu« den Vorhang für diesen Trend geöffnet: Sie haben die Rückseite eines jeden Sitzplatzes mit speziellen Tablets ausgestattet, die in der Lage sind, den

---

22 Dazu Weg bereitend *Weitzman*, The share economy, 1984.

23 Siehe dazu allgemein *Rifkin*, Die Null-Grenzkosten-Gesellschaft, 2014.

24 Zu diesen Visionen zukünftigen Lernens: *Bauer*, Lernen gestern – heute – morgen, in: Ludwig/Narr/Frank et al. (Hrsg.), Lernen in der digitalen Gesellschaft – offen, vernetzt, integrativ, 2013, S. 128, (128 ff).

Gesichtsausdruck seines Betrachters zu analysieren. Die Gäste erhalten kostenfreien Eintritt; für jedes von dem Tablet erkannte Lachen müssen sie aber 0,30 EUR zahlen (max. 24 EUR, was 80 Lachern entspricht).[25]

Ähnlich wird die Werbung der Zukunft auf Grundlage intelligenter Sensoren, die unsere emotionale Befindlichkeit registrieren und Werbeaussagen entsprechend zuschneiden, als emotionales Targeting flächendeckend personalisiert sein. All dies ist heute bereits alles andere als Science-Fiction. Das Sprichwort »Zukunft ist etwas, das meistens schon da ist, bevor wir damit rechnen«, wird womöglich auch insoweit seine Lebensnähe unter Beweis stellen.

Heute noch Zukunftsmusik, aber wohl nur noch eine Frage der Zeit ist demgegenüber gegenwärtig noch das Auslesen von Gedanken durch die Analyse von Gehirnströmen. Entwicklungen der Neurotechnologie lassen die Vorstellung, dass der Mensch der Zukunft mit Hilfe von Computer-Hirn-Schnittstellen Gegenstände, etwa Prothesen, Bildschirmeingabehilfen, Roboterarme oder Alltagsgegenstände, alleine durch die Kraft seiner Gedanken steuern oder die Gedanken Dritter lesen kann, nicht mehr als Utopie erscheinen. Ein alter Menschheitstraum scheint Wirklichkeit werden zu können.[26] Netzhaut- und Cochlea-Implantate könnten Sinnesorgane ersetzen und Signale in das Gehirn von Parkinson- oder Epilepsiepatienten lenken, Wearables oder eingepflanzte Chips den Blutdruck und Blutzuckerspiegel von Insulinpatienten messen und den gesamten Gesundheitszustand des Körpers überwachen; als unheilbar erkrankt diagnostizierte Organe lassen sich auf der Grundlage der Fortschritte der Gewebetechnologie und Bioinformatik nachzüchten. Sogar die Vorstellung von der Unausweichlichkeit des Todes gerät womöglich ins Wanken.[27]

II. Der Nutzer im Zwiespalt zwischen convenience und surveillance

Der digitale Epochenwandel wirkt nachhaltig auf unsere überkommenen Vorstellungen von Privatheit ein. Die mit ihm einhergehende massenhafte elektronische Datenerfassung organisiert eine Buchführung des gesamten Lebens, die sich dem Vergessen zu entziehen und den Einzelnen einer ständigen Überwachung zu unterwerfen droht.

Zwar entfaltet sich Persönlichkeit seit jeher in der Interaktion mit anderen. Der Mensch ist auf den Austausch mit anderen angewiesen, um Privatheit erfahren und sich als Homo socialis entwickeln zu können. Schon dadurch ist er notwendig auch den Augen der Öffentlichkeit und fremden Einflusssphären ausgesetzt. Das schließt einen Anspruch auf besonderen Schutz der Daten aber nicht aus. Ohne den verdunkelnden Rückzugsraum der Privatheit kann der Einzelne dem gleißenden Licht der Öffentlichkeit auf Dauer nicht standhalten und seine Eindrücke nicht verarbeiten. In welchem Umfang er sich in der öffentlichen Wahrnehmung oder alleine in seinem Forum internum bewegt, entscheidet er aber grundsätzlich selbst. Diese Autonomie konstituiert den Wert der Privatheit.

In der digitalen Welt ist Datenautonomie demgegenüber immer weniger erfahrbar, ebenso wie die Grenzen zwischen Privatem und Öffentlichem immer weniger präzise abgrenzbar sind. Die massenhafte elektronische Datenerfassung eröffnet tiefe Einblicke in unser digitales Alter Ego. Verloren sich ehedem die Spuren des Guten und Sündigen im Sand der Zeit, sind sie nun auf Servern eingebrannt. Alltagsgegenstände werden zu Bewegungsmeldern, die viel über die Lebensgewohnheiten ihrer Nutzer zu erzäh-

---

25 Siehe *Schulz*, Billige Witze, http://sz-magazin.sueddeutsche.de/texte/anzeigen/42640/Billige-Witze (3.4.2015).

26 Vgl. zu einem solchen Blick in die Zukunft etwa *Kaku*, Die Physik des Bewusstseins, 2014, S. 120 ff.; *Kaku* (Fn. 20), S. 86 ff.

27 Vgl. dazu *Kaku* (Fn. 20), S. 222 ff.

len wissen. Das Gerät, von dem die Menschen glaubten, es trüge die digitale Freiheit in sich, das Smartphone, sowie der Smart Car[28] werden zur digitalen Fußfessel. Die smarte Wohnung,[29] einst Refugium der Privatsphäre, leuchtet den digitalen Schatten aus, den der Bewohner an seine Wände malt.[30] Die Smart Factory[31] perfektioniert die alltägliche Überwachung des Mitarbeiters im Interesse einer Erhöhung seiner Produktivität. Jede Entscheidung, jeder Handgriff ist digital nachvollziehbar. Die hochentwickelten Sensoren und Aktoren zur Optimierung von Arbeitsabläufen werden zum Seismographen jeder menschlichen Regung und damit auch zum Spion. Sie machen das Leben erfassbar, entschlüsselbar und berechenbar (unten 1.). In den smarten Lebenswelten der Zukunft bleibt so kaum etwas geheim – weder, welcher Mitarbeiter wie lange Pause gemacht hat, noch, zu welchen Zeiten die Produktivität des Mitarbeiters von den erwünschten Kennzahlen um welche Prozentzahl abweicht. Während der Homo digitalis diesem Wandel mit Pragmatismus begegnet (unten 2.), greift insbesondere in der intellektuellen Elite zusehends die Sorge vor einem digitalen Totalitarismus um sich (unten 3.). Die Suche der Gesellschaft nach sachgerechten Reaktionsmustern auf die Herausforderungen des digitalen Wandels hat gerade erst begonnen; aber sie eilt (unten 4.).

1. Digitaler Schattenriss

Das Internet als Nervensystem des 21. Jahrhunderts eröffnet uns ungeahnte Möglichkeiten der Kommunikation und des Wissensaustauschs. Die Daten, die es vorhält, lassen sich dadurch auch zu einem Puzzle mit kontextübergreifendem Muster zusammensetzen, das ein detailgetreues Gesamtbild unserer Persönlichkeit erzeugt. Die algorithmische Einhegung des Menschen perfektioniert die Berechenbarkeit menschlichen Verhaltens. Die neue digitale Welt setzt uns einer Observation aus, die unser Verhalten auf Schritt und Tritt analysiert, und droht dadurch die Vision von einem über alles wachenden metaphysischen Panoptikum Realität werden zu lassen. Sensoren und Datenerfassungsgeräte bilden die »Augen und Ohren« eines »weltumspannenden lebenden Organismus«,[32] der jede Regung und jede Tätigkeit systematisch erfasst und permanente Selbstoptimierung als zivilisatorischen Auftrag versteht.

Darin liegt ein für die Erforschung sozialen Verhaltens ähnlicher Quantensprung, wie es die Erfindung des Mikroskops für die Bakteriologie war. Sein Erkenntnispotenzial beflügelt bei manchem die Fantasie einer Zukunft, in der ein besseres Verständnis der Gesetzmäßigkeiten menschlichen Zusammenlebens eine bessere Gesellschaft formt.[33] Umgekehrt bereitet das Entschlüsseln menschlicher Handlungsmuster aber auch einem manipulativen, gesellschaftliche Entwicklungen gefährdenden Gebrauch dieses neuen Wissens das Feld. Ungeachtet ihrer neoliberalen Logik und kybernetischen Idee können die Vermessungsmöglichkeiten der digitalen Welt nämlich die Grundlagen der Freiheit und der Chance zu Selbstentfaltung sowie Entwicklung zerstören, die sich zu verteidigen behaupten. Die Steuerungstechnologie der smarten digitalen Welt vermittelt durch ihre Grundeinstellungen unausgesprochen auch einen Definitionsanspruch für richtiges Autofahren, richtiges Heizverhalten und Energiesparen. Die

---

28 Dazu I. 1., S. 3 ff.

29 Dazu I. 3., S. 10 ff.

30 Zu den damit verbundenen datenschutzrechtlichen Implikationen im Einzelnen *Raabe/Weis*, RDV 2014, 231 (233 ff.); *Rüdiger*, RDV 2014, 253 (255 ff.).

31 Dazu I. 2., S. 5 ff.

32 *Pentland*, Society's Nervous System: Building Effective Government, Energy, and Public Health Systems, 2010, S. 2.

33 So die optimistische Hoffnung des MIT-Datenwissenschaftlers *Alex Pentland* im SPIEGEL-Interview Can We Use Big Data to Make Society Better?, Spiegel online vom 26.5.2014, abrufbar unter www.spiegel.de/international/zeitgeist/scientist-alex-pentland-argues-big-data-can-be-used-to-improve-society-a-970443.html (28.1.2015).

Möglichkeit sozialer Überwachung löst – wie jedes soziale Paradigma – einen formenden Druck auf das Subjekt aus: Sie kann durch die sublime Form der Kontrolle, die sie ausübt, zugleich zum Konformismus erziehen. Wer ubiquitäre Beobachtung vermutet, passt sich an die antizipierten Erwartungen der Außenwelt an. Das prämiert die Flucht in die Anonymität und drängt Diversität, Individualität sowie den beständig neu auszuhandelnden Kompromiss zwischen widerstreitenden Interessen aus den Lebensentwürfen der Menschen zurück. Oft ist es gerade die gezielte Übertretung der Grenzen des Konformen und Normalen, die gesellschaftlichem Wandel den Antrieb verleiht. Ohne Innovation droht das Gemeinwesen zu stagnieren, der Fortschritt zu erlahmen. Eine Rechtsordnung, »in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß«, hielt das BVerfG daher dereinst für mit dem informationellen Selbstbestimmungsrecht unvereinbar.[34]

Aber ist diese Forderung noch zeitgemäß? Oder muss man schlicht dem Bundesdatenschutzbeauftragten a. D. *Bull* beipflichten, der prophezeit, es werde nicht gelingen, den Internetnutzern zu garantieren, gleichzeitig sichtbar und doch unsichtbar zu sein?[35]

2. Das Privacy Paradox

Die Geschäftsmodelle digitaler Ökosysteme fußen auf einer Monetarisierung ihrer Inhalte. Die zahlreichen Annehmlichkeiten, mit denen digitale Anwendungen das Leben leichter machen, erkaufen die Nutzer um den Preis lückenloser Speicherung und Auswertung ihres Verhaltens sowie eines Kontrollverlustes über die autonome Verwendung von Daten. Der Nutzer ist nicht länger nur Kunde, er ist auch das Produkt, das der Anbieter zu verwerten trachtet. Die Daten sind die Gegenleistung für die Dienstleistung, in deren Genuss sie den Einzelnen bringt.[36] Die digitale Welt scheint beseelt von dem Ansinnen, die sprudelnden Datenquellen als Wirtschaftsgut in Geldströme umzuwandeln – wie König *Midas*, der alles, was er anfasste, in Gold zu verwandeln vermochte.

Die Nutzer der technischen Innovationen reagieren auf die Prämissen der digitalen Ökonomie mit einem ambivalenten Verhalten. Einige begreifen das Internet als bewusste Chance der Selbstvermarktung und Selbstinszenierung, die keine Scheu vor einem Eindringen in Residualsphären der Privatheit kennt; der Übergang zwischen obsessiver Preisgabe der Privatheit und unbedachter Selbstentblößung ist dabei bisweilen fließend. Andere erkennen die Risiken für ihre Privatsphäre, die mit der schönen neuen Dienste-Welt des Web 2.0 Einzug in ihren Alltag halten, sehr klar, nehmen diese aber in Kauf, da sie auf die Funktionalität der Dienste nicht verzichten wollen.[37] Denn – bei allem diffusen Unbehagen gegenüber der Informationsmacht des Datenkapitalismus – spenden diese substanziellen Nutzen, der das Alltagsleben in erfahrbarer Weise annehmlicher macht.[38] Diesen individuellen, kurzfristig erzielbaren Nutzungsvorteil gewichten die Betroffenen höher als abstrakte Gefahren für die individuelle Persönlichkeitsentfaltung oder langfristige kollektive Privacy-Gefährdungen.

---

34 BVerfGE 65, 1 (43).

35 *Bull*, NVwZ 2011, 257 (263).

36 40 % derjenigen, die täglich Google in Anspruch nehmen, sind sich empirischen Analysen zufolge dieses Tauschgeschäftes nicht bewusst. *Köcher*, Folgenlose Ängste, FAZ vom 20.6.2014, S. 8.

37 70 % der Internetnutzer finden es nicht in Ordnung, wenn Unternehmen in größerem Umfang Daten über ihre Kunden sammeln und auswerten. Um ihren Datenschutz im Internet besorgte Nutzer nehmen die Suchmaschine Google aber in nahezu gleichem Umfang in Anspruch wie solche Nutzer, die sich um die Sicherheit ihrer Daten keine Sorgen machen. Vgl. die Ergebnisse der empirischen Analyse bei *Köcher* (Fn. 36), S. 8.

38 Diese These unterschreiben bei empirischen Befragungen zwei Drittel der Internetnutzer *Köcher* (Fn. 36), S. 8.

Ein Experiment, das der Informatikprofessor *Alessandro Acquisti* in den USA zusammen mit Kollegen durchgeführt hat, illustriert diese Grundhaltung:[39] Sie verteilten an zwei Gruppen von Studienteilnehmern nach einem Zufallsverfahren zwei unterschiedlich werthaltige Einkaufsgutscheine: Die eine Gruppe erhielt einen Einkaufsgutschein im Wert von 10 USD, die andere Gruppe im Wert von 12 USD – allerdings mit der Besonderheit, dass die Einkäufe (nach dem Vorbild des Bonussystems »Payback«) protokolliert und in allen ihren Datenfacetten ausgeleuchtet werden. Die beiden Gruppen durften dann jeweils ihre Einkaufsgutscheine mit den Mitgliedern der anderen Gruppe tauschen. Lediglich 9 % der Besitzer von 12 USD-Gutscheinen wollte ihren Gutschein gegen einen 10 USD-Gutschein tauschen. Demgegenüber war die Hälfte der 10 USD-Gutscheinen-Besitzer bereit, ihren Gutschein gegen einen 12 USD-Gutschein auszuwechseln. Die Gutscheine, die einen geringfügigen ökonomischen Vorteil mit einer umfassenden Datenauswertung verknüpften, waren also deutlich beliebter. Mit dem in der Verhaltensökonomik bekannten sog. Besitzeffekt (engl. Endowment-Effect)[40] alleine lässt sich dieses Ergebnis nicht erklären. Die Mehrheit der Teilnehmerinnen und Teilnehmer maß ihrer Privatsphäre beim Einkauf offenkundig einen geringeren Wert als 2 USD zu. Die Gratifikation der Nutzung überwiegt die wahrgenommene Gefährdung. Vergegenwärtigt man sich die geringen Beträge, zu denen Kunden auch in realitas ihre Kundenprofile via Kundenkarten an Payback und andere Bonussystem-Anbieter zur kommerziellen Verwertung veräußern, überrascht dieses Ergebnis nicht.

Erstaunen löst vor dieser Folie allerdings der empirische Befund aus, dass weiterhin über zwei Drittel der Internetnutzer dem Datenschutz und der Datensicherheit bei Online-Diensten in Umfragen eine hohe Wichtigkeit zumessen.[41] Im Rahmen einer im Juni 2014 veröffentlichten Studie sprachen sich beispielsweise 92 % der Befragten dafür aus, den Kauf und Verkauf von Daten ohne explizite Zustimmung durch Gesetze zu verbieten; nur 12 % der befragten Deutschen gaben an, für Vorteile wie mehr Komfort bei Online-Diensten ihren Datenschutz einschränken zu wollen.[42]

Zwischen dem abstrakten Bewusstsein und der Wertschätzung der Nutzer für einen besonderen Schutz der Persönlichkeit auf der einen Seite und seiner konkreten Wahrnehmung im Einzelfall auf der anderen Seite klafft eine bemerkenswerte Lücke. Insbesondere bei Nutzern sozialer Netzwerke, wie Facebook, lässt sich nur ein schwacher Zusammenhang zwischen den Einstellungen zu Privatsphäre und Datensicherheit und ihrem tatsächlichen Kommunikationsverhalten beobachten. Dieses Phänomen ist unter dem Begriff »Privacy Paradox« bekannt geworden. Darin machen sich nicht nur eine kognitive Dissonanz und ein Kontrollverlust beim Umgang mit komplexen Interaktionszusammenhängen bemerkbar. Vielmehr schwingt darin auch ein gerüttelt Maß an Wahrnehmungsveränderung mit: Menschen messen den neuen Kommunikationsräumen als Medium der Selbstinszenierung und -erprobung einen hohen Stellenwert bei. Die Monetarisierung des eigenen Datenportfolios als Datenagent, der die unbekümmerte Seele eigener Privatheit gegen ökonomischen Wert eintauscht, ist für sie keine besorgniserregende Entwicklung, sondern Teil eines logischen Prozesses der Entprivatisierung.[43] Was dem einen als Linsengericht kurzfristiger Nützlichkeit erscheint, der den langfristig zu zahlenden Preis eines Verlustes der Privatheit nicht rechtfertigt, ist für den anderen ein rationales Kalkül einer neuen Wahrnehmung von Privatheit entlang des Pfads individuell empfundener Präferenzen. Die Veränderungen legen auch Zeugnis dafür ab, dass sich seit der Geburtsstunde verfassungsrechtlicher Privatheitsverbürgungen die

---

39 Vgl. *Acquisti/John/Loewenstein*, Journal of Legal Studies 42 (2013), 249 ff.

40 Er beschreibt das Phänomen, dass Menschen für die Aufgabe eines Gutes, das sie bereits besitzen, einen höheren Preis verlangen, als sie für den Erwerb des Gutes zu zahlen bereit wären; *Thaler*, Journal of Economic Behavior and Organization 1 (1980), 39 (43 ff.).

41 *Initiative D21* (Hrsg.), eGovernment Monitor 2014, 2014, S. 18.

42 Damit sind Deutsche der Umfrage zufolge deutlich skeptischer als der weltweite Durchschnitt, vgl. den EMC-Datenschutzindex für Deutschland, online abrufbar unter http://germany.emc.com/campaign/privacy-index/germany.htm (28.4.2015).

43 *Heller*, Post Privacy, 2011.

Grenzlinie zwischen Privatheit und Öffentlichkeit deutlich verschoben hat; den Wert der Privatsphäre nehmen viele Menschen heute anders wahr als frühere Generationen: Während in den 80er Jahren lautstarke Proteste gegen die geplante Volkszählung ertönten und Bürger diese schließlich massenhaft boykottierten, erleben Digital Natives die ungleich detailschärferen Profilsammlungen von Facebook & Co. als elementaren Teil ihrer Identität und Persönlichkeitsentfaltung. Für sie negiert die Selbstdarstellung im Internet nicht die Freiheit, sie macht von ihr Gebrauch. Der gesellschaftliche Stellenwert von Privatheit erfährt so einen Kulturwandel. Entsprechend hält denn auch nur jeder fünfte deutsche Internetnutzer staatliche Eingriffe ins Internet für notwendig. 11 % halten die Regulierungsbemühungen bereits für zu weitgehend.[44]

Zugleich agiert lediglich die Hälfte der Bevölkerung nach eigenen Angaben in Sachen Datenschutz hinreichend informiert und souverän.[45] Nach wie vor sind sich viele Google-Nutzer des Umstands nicht bewusst, dass die Gegenleistung für die nur scheinbar kostenlosen Suchdienste, Usability-Tools und sozialen Medien des Web 2.0-Giganten ihre persönlichen Daten sind.[46] Womöglich ist das Privacy Paradox aber auch Ausdruck eines systematischen Wahrnehmungsfehlers bei der Risikobewertung, der auch aus anderen Zusammenhängen bekannt ist: Menschen schätzen einen individuellen, kurzfristig erzielbaren Nutzungsvorteil mitunter als deutlich höher ein als objektiv vorhandene, aber bloß kollektiv oder abstrakt beschreibbare Risiken. Darüber hinaus gewichten sie objektiv vorhandene Risiken für sich selbst mitunter deutlich geringer ein, als sie tatsächlich sind.

Womöglich ist die Wahrnehmungsveränderung aber auch Zeichen einer Prioritätenverschiebung, einer Verschiebung der Präferenzen bei der Anwendung komplexer Technologien von Eigenverantwortung, Beherrschbarkeit und Freiheit hin zu Komfort und Effizienz – entsprechend der Prophezeiung des Gedichts »Die Abnehmer« von *Erich Fried* aus dem Jahre 1964: »Einer nimmt uns das Denken ab (…), einer nimmt uns die großen Entscheidungen ab (…). Das ganze Leben nehmen sie uns dann ab.«. Die Segnungen des digitalen Zeitalters drohen uns dadurch zugleich zu voraufklärerischer Unmündigkeit zu treiben, die uns zu Mündeln einer Datenherrschaft macht. Die Warnung *Immanuel Kants* vor dem süßen Gift der Bequemlichkeit und der Naivität scheint heute aktueller denn je: »Faulheit und Feigheit sind die Ursachen, warum ein so großer Teil der Menschen (...) gerne zeitlebens unmündig bleiben; und warum es anderen so leicht wird, sich zu deren Vormündern aufzuwerfen. Es ist zu bequem, unmündig zu sein.«[47] Wir nehmen die Segnungen von Facebook, Google & Co. mit der gleichen Begeisterung und geradezu götzenhaften Verehrung auf, mit der die Azteken ihre spanischen Eroberer begrüßten. Deren Freude hat bekanntlich nicht lange gehalten.[48] Komfort und Sicherheit verdrängen dadurch ein Stück weit auch Freiheit und Selbstbestimmung.

3. Sorge vor einem digitalen Kapitalismus und Totalitarismus

Die Dynamik des Wertewandels, Privatheit im Alltag wahrzunehmen, hat allerdings mit der Aufdeckung des NSA-Skandals an Fahrt verloren, vielleicht sogar einen Richtungswechsel erfahren. *Edward Snowdens* Enthüllungen haben erste Kratzer in die Karosserie des Grundvertrauens der modernen Informationsgesellschaft in das Netz als »Raum der Freiheit« geritzt. Kaum hat das Internet, z.B. während des

---

44 *Köcher* (Fn. 36), S. 8.

45 Vgl. *DIVSI*, Milieu-Studie zu Vertrauen und Sicherheit im Internet, 2012, S. 15.

46 Vgl. *Köcher* (Fn. 36), S. 8.

47 *Kant*, Berlinische Monatsschrift 1784, 481 (481 f.).

48 Kritisch gegenüber einer digitalen Fortschrittseuphorie angesichts anderer weltweiter Probleme, die es zu vorrangig zu lösen gelte, *Kreibich*, APuZ 2015, 20 (20 f.).

»Arabischen Frühlings«, unter Beweis gestellt, die Geburtsstunde einer Emanzipation der Bürger in einer offenen Demokratie einläuten und die verfestigten Machtstrukturen totalitärer Regime durch digital organisierten Protest aufbrechen zu können, wird seine Kraft zur Subversion der Privatheit besonders sichtbar.

Die Einblicke in unser Leben, welche unsere digitalen Spuren großen Internetkonzernen gewähren, und die fortgeschrittenen Möglichkeiten, die ihnen zentralen Zugriff zur Auswertung digitaler Daten eröffnen, ohne dass dem Einzelnen eine vollständige Kontrolle über diese Vorgänge möglich ist, machen die Privatheit für Formen eines Missbrauchs angreifbar. Zahlreiche Internetnutzer stehen betroffen und stellen fest, dass viele Äpfel am Baum der digitalen Erkenntnis faule Stellen aufweisen oder ganz und gar zernagt sind. Die Sorge vor einem informationellen bzw. technologischen Totalitarismus[49], in dem sich die Grenzen zwischen staatlicher Überwachung und Wirtschaft, privater und staatlicher Verfügungsmacht, zusehends verflüchtigen, geht um – einem Totalitarismus, der (anders als bisherige totalitäre Herrschaftsformen) keine Uniformen benötigt, da die Uniformität bereits informationell unter Kontrolle ist.[50]

»Google weiß«, so hat es der Vorstandsvorsitzende der Axel Springer SE *Matthias Doepfner* ausgedrückt, »über jeden digital aktiven Bürger mehr, als sich *George Orwell* in seinen kühnsten Visionen in '1984' je vorzustellen wagte«.[51] Das Unternehmen sitze auf dem gesamten gegenwärtigen Datenschatz der Menschheit wie der in einen Drachen verwandelte Riese Fafner im »Ring des Nibelungen«.[52]

Unsere Gesellschaft droht so – wie der Staat im Verhältnis zu den Banken in der Finanzkrise 2008 – Petabyte für Petabyte zur Geisel in der Hand der Internetkonzerne zu werden. Die ehemalige EU-Kommissarin für die digitale Agenda *Neelie Kroes* hat die Enthüllungen von *Edward Snowden* deshalb als die Lehmann-Insolvenz des Internets bezeichnet.[53] In jeder Krise, die ein Offenbarungseid auslöst, steckt zugleich auch eine Chance: Sie öffnet die Augen für eine Bedrohungslage, die dem System immanent ist, sich seine Nutzer bislang aber nicht ausreichend vergegenwärtigt haben.

Der Cyberspace ist seit jeher ein Spannungsfeld zwischen Freiheit und Sicherheit. Als vernetzter öffentlicher Raum verdankt das Internet seine Kinderstube nicht zuletzt dem Kalten Krieg, es war Spielwiese militärischer Entwicklungsideen und staatlicher Überwachung. Es entwickelt sich zugleich immer stärker zu einer notwendigen Voraussetzung effektiver Teilhabe am sozialen Leben. So ist auch die Regulierung sozialer Kommunikation zu einer Schicksalsfrage einer freiheitlich-demokratischen Informationsgesellschaft geworden.[54] Im schlimmsten Fall kann ein um sich greifendes Misstrauen der Nutzer die Uhr des technologischen Fortschritts anhalten oder gar ein Stück weit zurückdrehen.

Viele sehen unter diesen Vorzeichen die sozialen Bedingungen für ein demokratisches Gemeinwesen, namentlich die individuelle Entfaltungsfreiheit und Selbstbestimmung, und damit die Souveränität des demokratischen Gesellschaftsvertrages infrage gestellt.[55] Längst gehe es »nicht mehr um die Sicherung von Verfügungsmacht über die eigene Person, sondern um deren Rückgewinnung – daher um den Entzug von Information«.[56] *Shoshana Zuboff* sieht sich an die Fabel von den Fröschen erinnert, die glücklich

---

49 *Schulz*, Technologischer Totalitarismus - Warum wir jetzt kämpfen müssen?, FAZ vom 6.2.2014, S. 25; ähnlich *Welzer*, Vorsicht, Datensammler, FAZ vom 23.4.2014, S. 9.

50 *Welzer* (Fn. 49), S. 9.

51 *Doepfner*, Offener Brief an Eric Schmidt: Warum wir Google fürchten, FAZ vom 16.4.2014, S. 9.

52 *Doepfner* (Fn. 51), S. 9.

53 *Kroes*, Ich bin nicht naiv, und Europa darf es auch nicht sein, FAZ vom 24.3.2014, S. 9.

54 *Schirrmacher*, Der verwettete Mensch, in: Geiselberger (Hrsg.), Big Data, 2013, S. 273(279); *Weichert*, Big Data – eine Herausforderung für den Datenschutz, in: Geiselberger (Hrsg.), Big Data, 2013, S. 131(138).

55 *Welzer* (Fn. 49), S. 9; *Zuboff*, Die Google-Gefahr: Schürfrechte am Leben, FAZ vom 30.4.2014, S. 9.

56 *Welzer* (Fn. 49), S. 9.

in ihrem Märchenteich planschen, während die Temperatur des Wassers langsam ansteigt, ohne dass die Frösche es bemerken. Als sie der Gefahr gewahr werden, ist es zu spät. Als Frösche in den digitalen Gewässern seien die Menschen heute einer absolutistischen Macht eines neuartigen Monopols ausgesetzt – dieses sei zwar in seiner Rhetorik dem Ethos des öffentlichen Webs verpflichtet, habe seiner Operationslogik aber längst den Rücken zugekehrt.[57]

In der Bevölkerung bildet sich unterdessen im Gefolge des NSA-Überwachungsskandals einerseits das Bewusstsein für die Erforderlichkeit einer Datenhygiene und einer besonderen Achtsamkeit im Umgang mit eigenen Daten heraus. Andererseits lässt sich auch zunehmend eine Akzeptanz der Bevölkerung für staatliche Überwachungsmaßnahmen beobachten. Welcher Aspekt sich stärker Bahn bricht, hängt vor allem davon ab, wie sehr das Sicherheitsbedürfnis der Menschen – insbesondere im Gefolge von terroristischen Anschlägen – in ihre obersten Bewusstseinsschichten vordringt. Zwischen Überwachungsängsten und Kriminalitätsfurcht besteht eine Korrelation.

4. Reaktionsmuster: zwischen digitaler Entschlackungskur und Schutzstrategien für die digitale Unversehrtheit

Als Teil einer Abstimmung mit den Füßen entwickelt sich vielerorts eine Ausstiegskultur, die dem »Totalitarismus in Kapuzenshirts«[58], wie der Google-Dataismus sinnbildlich umschrieben wird, abschwört. Sie rät zur digitalen Entschlackungskur, welche den mittel- und langfristigen Nebenwirkungen digitaler Omnipräsenz und der Echtzeitideologie sozialer Kommunikation durch Entsagung die Grundlage weiterer Wucherung entzieht. Soziale Medien identifiziert sie als Spielautomaten, die nach dem Vorbild einer Las-Vegas-Spielhölle darauf angelegt sind, unserem Hang zur Selbstinszenierung, der in sozialen Netzwerken bisweilen in digitalen Exhibitionismus abzugleiten droht, in einem digitalen Verkündigungsparadies Raum zu geben. Internetaussteigern bieten bereits entsprechende Apps, die zur digitalen Diät anhalten, ihre Diente an.[59] *Hans Magnus Enzensberger* ruft in der FAZ sogar dazu auf, das eigene Smartphone auf die Müllhalde technischer Innovationen zu verbannen. Zehn Gebote für den Widerstand gegen die »digitale Nachstellung« hat er formuliert: »Waren oder Dienstleistungen via Internet sollte man meiden.«[60] »Dem Aberwitz, alle denkbaren Gebrauchsgegenstände, von der Zahnbürste bis zum Fernseher, vom Auto bis zum Kühlschrank über das Internet zu vernetzen, ist nur mit einem totalen Boykott zu begegnen.«[61]

Ist der Entschluss, sich gegenüber dem Rest der Gesellschaft zu desynchronisieren,[62] aber die richtige Antwort auf die Herausforderungen ubiquitärer Digitalisierung? In einer digitalen Welt keine digitalen Fußspuren zu hinterlassen, ist eine anachronistisch anmutende Vorstellung. Sie verliert das gesamtgesellschaftliche Nutzen- und Innovationspotenzial des Internets aus dem Auge. Den Chancen der Technik gänzlich abzuschwören, erweist sich als genauso wenig sinnvoll, wie Geldautomaten zu meiden, weil

---

57 *Zuboff* (Fn. 55), S. 9.

58 *Welzer* (Fn. 49), S. 9.

59 *Morozov*, Achtung, Achtsamkeit!, FAZ vom 17.2.2014, S. 35.

60 *Enzensberger*, Wehrt Euch!, FAZ vom 1.3.2014, S. 9, Regel 8.

61 *Enzensberger* (Fn. 60), Regel. 6.

62 In diesem Sinne *Enzensbergers* Forderungen stützend *Welzer* (Fn. 49), S. 9. Auch *Frank Schirrmacher* publizierte in den vergangenen Jahren Streitschriften gegen die grenzenlose Digitalisierung des gesellschaftlichen Lebens; er warnt darin vor einer Gesellschaft, in der die Menschen durch eine psychologische Steuerung ihrer Bedürfnisse nach den Erfordernissen des Marktes im Ergebnis einer kollektiven Regentschaft von Computern und Gleichungen unterworfen sind. Vgl. etwa *Schirrmacher*, Ego, 2013.

dort leicht Übergriffe auf Kunden möglich sind, oder das Autofahren zu unterlassen, weil es zu Verkehrsunfällen kommen kann. Der Forderung nach einem Boykott der technischen Möglichkeiten im digitalen Universum fehlt der Weitblick für die Gestaltungsmöglichkeiten einer Zukunft, in der die Technologie sich den Interessen und Bedürfnissen der Menschen unterwirft. Eine dystopische Vision ist keine unaufhaltbare Gesetzmäßigkeit. Eine Kapitulation vor den Herausforderungen, die der digitale Lebenswandel mit sich bringt, wäre auch eine Kapitulation des Rechts und der Möglichkeiten demokratischer Kontrolle vor einer digitalen Autokratie. Nicht zuletzt wäre der öffentliche Raum des Internets als Ort der Kommunikation und des globalen Diskurses für eine neue Form lebendiger, deliberativer Demokratie weitgehend verloren. Ziel sollte vielmehr eine Erschließung des Reservoirs der Chancen und eine Domestizierung der Gefahren digitaler Technologien sein. Geboten ist eine Suche nach Schutzmechanismen, welche die digitale Unversehrtheit des Einzelnen, im Cyberspace hinreichend schützen. Anders als die körperliche Integrität des Art. 2 Abs. 2 S. 1 GG ist sie nicht jederzeit spürbar, aber nicht minder verwundbar. Sie ruft die Leitfrage auf den Plan: Wie kann der Einzelne in der digitalen Welt die Hoheit über seine Daten gegenüber übermächtig scheinenden Datenkollektoren sichern? Dazu gilt es, sich der rechtlichen Grundlagen zu vergewissern, auf denen unser Schutz der Privatheit im digitalen Zeitalter aufsetzt.

III. Der Status quo der Rechtsordnung und Entwicklungsoptionen de lege ferenda

1. Funktionswandel und Bew(ä/e)hrung der Grundrechte im digitalen Raum

Unserer Rechtsordnung attestieren manche bislang eine völlige »Schweigespirale«[63] gegenüber der digitalen Revolution. *Juli Zeh* etwa mahnt deshalb prononciert einen digitalen Code civil an: »Während andere unkörperliche Gegenstände wie Forderungen schon lange nach klaren Regeln am Geschäftsverkehr teilnehmen, gibt es im digitalen Bereich nicht einmal Begriffe, um die vielfältigen wirtschaftlichen und rechtlichen Beziehungen zu beschreiben.«[64] Sie fordert ein Grundrecht, das »personenbezogene Daten unter die alleinige Verfügungsgewalt des Einzelnen stellt«.[65]

Zentrale Wegmarken rechtlicher Begleitung des Persönlichkeitsschutzes geraten bei diesen prononcierten Thesen freilich aus dem Blickfeld: Bereits vor 30 Jahren hat das BVerfG im Volkszählungsurteil eben dieses Recht, das informationelle Selbstbestimmungsrecht, aus der Verfassung herausgelesen. Personenbezogene Daten stellt die Datenschutzrichtlinie 95/46/EG der Europäischen Union schon seit 1995 unter besonderen Schutz. Das BDSG hat sich als die nationale Magna Charta der informationellen Selbstbestimmung im Grundsatz bewährt. Auch die Fortschreibung des verfassungsrechtlichen Schutzes des Homo digitalis im Lichte veränderter Interessen- und Gefährdungslagen ist nicht lediglich ein Zukunftsszenario. Einen ersten Takt hat das BVerfG im Jahr 2008 mit seiner Entscheidung zur Online-Durchsuchung angestimmt: Es hat das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme aus den Einzelverbürgungen der Verfassung heraus komponiert.[66] Doch das war wohl erst die Ouvertüre. Die prinzipielle Entwicklungsoffenheit des allgemeinen Persönlichkeitsrechts[67] wird fraglos auch in Zukunft weitere taktgebende Impulse zur Konturierung des Persönlichkeitsschutzes in Zeiten der Digitalisierung und dynamische Anpassungen erforderlich machen, um den sich abzeichnenden Herausforderungen gerecht zu werden.

---

63 *Zeh*, Schützt den Datenkörper!, FAZ vom 11.2.2014, S. 34.

64 *Zeh* (Fn. 63), S. 34.

65 *Zeh* (Fn. 63), S. 34.

66 BVerfGE 120, 274.

67 Dazu *Schliesky/Hoffmann/Luch et al.*, Schutzpflichten und Drittwirkung im Internet, 2014, S. 80 ff.; *Lang*, in: Epping/Hillgruber (Hrsg.), BeckOK GG, 24. Edition, 2015, Art. 2 GG, Rn. 34.

Richtig aber ist, dass das gegenwärtige Datenschutzrecht auf das digitale Zeitalter nicht gut vorbereitet ist. Es hält zwar ein systematisches und durchaus strenges Rüstzeug für den Umgang mit Privatheit vor. Das BDSG stammt jedoch eher aus der Zeit von Aktenordnern und Karteikarten als von Web 2.0 und Big Data. Dass die Bodenschätze der Moderne in den Datensätzen des Menschen verborgen liegen können und dass die Gesellschaft ihre Erkenntnisse aus kontinuierlich zirkulierenden Datenströmen schöpft, welche eine automatische Auswertung von Informationen aus unterschiedlichsten Lebensbereichen in Echtzeit möglich machen, lag außerhalb der Vorstellungswelt der Schöpfer des BDSG. Auf die Wandlungen, die der Umgang mit Informationen und Privatheit in der Internet-Ära erfahren hat, antwortet es nicht mit einem zeitgerechten, konsistenten Schutzkonzept, das die besonderen Gefährdungen der Privatheit einerseits und das wirtschaftliche Wertschöpfungspotenzial andererseits zu einem Ausgleich bringt.

Im digitalen Zeitalter ist der Datenschutz ebenso eine zentrale Infrastrukturressource selbstbestimmter Kommunikation, wie die Qualität der Datenverarbeitung sich immer sichtbarer zu einer wichtigen Quelle der Wertschöpfung entwickelt. Vordringliche politische Aufgabe ist es, dem digitalen Wandel einen Rahmen zu geben, der dem gesellschaftlichen Konsens über einen verantwortungsvollen Umgang mit persönlichen Daten entspricht.

Inwieweit es dazu einer Erweiterung des Grundrechtskatalogs und – als Reaktion auf die Verlagerung von Grundrechtsgefährdungen in den privaten Sektor – einer kodifikatorischen Intensivierung der Gewährleistungs- und Drittwirkungsfunktion der Grundrechte bedarf, ist Gegenstand einer kontroversen politischen und rechtswissenschaftlichen Diskussion.[68] Angesichts der dem Grundgesetz bislang aufgrund seiner Stabilität und Flexibilität[69] attestierten Zukunftstauglichkeit und der Sensibilität verfassungsrechtlicher Ergänzungen[70], sollte allerdings vor einem Ruf nach einer digitalen Verjüngungskur der Verfassung zunächst das Entwicklungspotenzial der gegebenen Grundrechte und Grundrechtsfunktionen ausgelotet werden. Die hierfür relevanten Vermessungsareale sind einerseits die Entwicklungs- und Anwendungsspielräume des einfachgesetzlichen Rechts, andererseits die Aktivierungspotenziale der Emanzipation bzw. Stärkung der Verbraucher und des Wettbewerbs.

2. Regulierungsbemühungen der Europäischen Union und Hoffnungen auf ein Völkerrecht für die digitale Welt

Das World Wide Web kennt keine Demarkationslinien. Die Entgrenzung des Internets von Raum und Zeit stellt die Steuerungskraft der nationalen Rechtsordnung auf eine Bewährungsprobe. Mit seiner Flexibilität hält wirksame staatliche Vollzugskontrolle nur bedingt Schritt. Sein virtueller Raum erleichtert Ausweichmanöver, etwa durch die Verlagerung von Unternehmensniederlassungen ins Ausland.[71] Die

---

68 Vgl. dazu bspw. *Schliesky/Hoffmann/Luch et al.* (Fn. 67), S. 98 ff.

69 *Oppermann*, JZ 2009, 481 (491).

70 Dazu mit bspw. *Greve*, Drittwirkung des grundrechtlichen Datenschutzes im digitalen Zeitalter, in: Franzius/Lejeune/Lewinski et al. (Hrsg.), Beharren, Bewegen: Festschrift für Michael Kloepfer zum 70. Geburtstag, 2013, S. 665 (666 ff.); *Schulz*, ZG 2010, 358 ff.

71 Die Unternehmensniederlassung ist u.a. zentraler geographischer Anknüpfungspunkt für die Anwendbarkeit des deutschen Datenschutzrechts. Nur, wenn die inländische Datenerhebung, Verarbeitung und Nutzung auch durch eine im Inland gelegene Niederlassung erfolgt, findet das BDSG Anwendung (§ 1 Abs. 5 S. 1 und 2 BDSG). Der so eröffneten Möglichkeit des Forumshoppings hat der EuGH allerdings jüngst deutlich die Schranken aufgezeigt. Seit der Google-Entscheidung (EuGH, Urt. v. 13.5.2014 – C-131/12 –, EuZW 2014, 541 (544, Rn. 46 ff.) weist er auch einer Niederlassung, die zwar selbst keine Daten erhebt und verarbeitet, dafür aber untrennbar in die Geschäftstätigkeit des Gesamtunternehmens

damit einhergehende Erosion rechtlicher Regulierungsmacht nationalstaatlicher Akteure erfährt durch die parallele Machtkonzentration in der digitalen Wirtschaft und die überragende Marktstellung globaler Internetkonzerne des Silicon Valley[72] eine zusätzliche Brisanz.

a) Die Datenschutz-Grundverordnung ante portas

Unter diesen strukturellen Rahmenbedingungen entspricht es mehr denn je einem sachgerechten Regelungsansatz, dem drohenden Wirkungsverlust rechtlicher Steuerungskraft – zumindest innerhalb der EU – durch eine harmonisierte und damit schlagkräftigere europäische Rechtsetzung entgegenzuwirken. Die geplante Datenschutz-Grundverordnung[73] stellt sich dieser Herausforderung.[74] Indem sie für die Anwendbarkeit europäischen Datenschutzrechts nicht an den Ort anknüpft, an dem die Datenverarbeitung stattfindet, sondern an den Ort, an den sich die angebotene Leistung richtet (Marktortprinzip), schließt sie datenschutzrechtliche Fluchtwege, die digitalen Global Playern bislang eine Cream-Skimming-Strategie sowie ein unionales Datenschutz-Dumping ermöglichten.[75] Wenn ein Internetkonzern in einem Mitgliedstaat der EU seine Leistungen anbietet, dann muss es auch europäischen Datenschutzstandards genügen.

Die Datenschutz-Grundverordnung eröffnet damit die Chance, die aus dem analogen Zeitalter stammende Datenschutzregulierung an die Herausforderungen moderner Informationstechnologie anzupassen. Ihr Regelungsauftrag ist ein Drahtseilakt: Sie muss das Potenzial wirtschaftlicher Wertschöpfung gegen die Grundrechtserwartungen der Bürger ausbalancieren. Beide stehen in einem natürlichen Zielkonflikt. Die Grundverordnung kämpft mit einem Grundphänomen des Datenschutzes, das sich in der digitalen Welt noch stärker als in der analogen bemerkbar macht: Datenschutz ist mitunter Sand im Getriebe wirtschaftlicher Innovation. Entsprechend genießt Datenschutz in der Wirtschaft häufig umso höhere Wertschätzung, je abstrakter er bleibt.

---

eingebunden ist, eine datenschutzrechtliche Mitverantwortlichkeit zu. Er stellt dafür – auch auf der Grundlage der alten Datenschutzrichtlinie 95/46/EG – nicht auf den Sitz der Niederlassung des Mutterunternehmens ab (im Falle von Google Inc. wäre dies Mountain View in Kalifornien, USA). Vielmehr lässt der EuGH es ausreichen, dass das Unternehmen in dem betreffenden Staat eine Niederlassung hat, »wenn diese die Aufgabe hat, in dem Mitgliedstaat für die Förderung des Verkaufs der angebotenen Werbeflächen der Suchmaschine, mit denen die Dienstleistung der Suchmaschine rentabel gemacht werden soll, und diesen Verkauf selbst zu sorgen.« EuGH, a. a. O., 544, Rn. 54.

72 Der Suchmaschinen-Marktanteil von Google in Deutschland lag nach Zahlen des Statistischen Bundesamtes vom März 2014 bei 91,2 %, vgl. http://de.statista.com/statistik/daten/studie/222849/umfrage/marktanteile-der-suchmaschinen-weltweit/ (27.1.2015). Googles Betriebssystem »Android« für mobile Geräte erreicht in Deutschland Anfang 2015 eine Marktdurchdringung von 77 % (vgl. http://www.giga.de/smartphones/iphone-6/news/kantar-ios-mit-steigendem-marktanteil
-in-deutschland/ [27.1.2015]). Youtube – Googles Videoportal – ist nicht nur der mit Abstand beliebteste Social-Video-Dienst im Netz (vgl. http://de.statista.com/statistik/daten/studie/209190/umfrage/beliebteste-videoportale-in-deutschland/ [27.4.2015]), sondern birgt auch die weltweit größte Sammlung an Videomaterial. Nest Labs – eine der neuesten Errungenschaft der Google Einkäufer – attestieren Experten eine goldene Zukunft im Smart-Metering-Markt.

73 Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung) vom 25.1.2012, KOM(2012), 11 endg.; Legislative Entschließung des Europäischen Parlaments vom 12.3.2014 zu dem Vorschlag für eine Datenschutz-Grundverordnung.

74 Dazu etwa *Albrecht*, ZD 2013, 587 ff.; *Jaspers*, DuD 2012, 571 ff.; vgl. zum kompetenzrechtlichen Rahmen *Pötters*, RDV 2015, 10

75 Zu dem ersten Schritt, den hat der EuGH in seiner (dogmatisch durchaus gewagten) Google-Entscheidung in diese Richtung unternommen hat, siehe Fn. 71.

Will das Datenschutzrecht den spezifischen Freiheitsbedrohungen digitaler Technologien zielgenau entgegenwirken, sollte es seinen Regulierungsfokus stärker als bisher vom personenbezogenen Einzeldatum wegbewegen und auf den strukturellen Gefährdungsgrad der Datenverarbeitungsprozesse, insbesondere mithilfe algorithmischer Auswertung von Datensätzen und Datenzusammenhängen, richten.[76] Das personenbezogene Datum erfüllt bislang eine wichtige Filterfunktion für das datenschutzrechtliche Kontrollregime: Sobald eine Person identifizierbar ist, greift das datenschutzrechtliche Verbotsprinzip (§ 4 Abs. 1 BDSG). Diese Dichotomie bläht das Datenschutzrecht als Kommunikationsregulierungsrecht freilich bisweilen über seinen Zielgehalt hinaus auf. Es bedarf einer risikobasierten Feinjustierung, die stärker als bisher Aspekte der Folgenabschätzung, insbesondere des Gefährdungsgrades für die Persönlichkeit im Einzelfall, in das datenschutzrechtliche Prüfungsregime integriert.[77]

Wichtigen normativen Flankenschutz kann dem Datenschutzrecht eine Harmonisierung mit dem Wettbewerbs- und Kartellrecht der Europäischen Union verleihen.[78] Als Schutzinstrument des europäischen Wirtschaftsordnungsrechts »mit Biss« hält es im Grundsatz ein wirksames Instrumentarium vor, um gegen ein wettbewerbsbeschränkendes Machtungleichgewicht vorzugehen.[79] Der immense Zeitaufwand kartellrechtlicher Prüfungen wirkt allerdings einer zeitnahen, der Dynamik des Digitalisierungs- und Onlinemarktes gerecht werdenden Sanktionierung von Wettbewerbsverstößen vielfach strukturell entgegen; das leistet damit einer Verfestigung der Monopolstrukturen tendenziell Vorschub.[80] Ein Regulierungsweg, der die Wachsamkeit und Beobachtungsgenauigkeit der direkten Wettbewerber sowie der Verbraucherschutzverbände für einen wirksamen Datenschutz bündelt und fruchtbar macht, ist deshalb um einiges erfolgsversprechender. Der Gesetzesentwurf der Bundesregierung für ein Gesetz zur Stärkung der Durchsetzungsmacht des Datenschutzrechts durch ein Verbandsklagerecht[81] unternimmt einen Schritt in diese Richtung.

Die Überlegung, die Internetnutzer an den milliardenschweren Gewinnen der Konzerne des digitalen Morgenlandes durch eine Verbürgung eines Dateneigentums und eines Vergütungsanspruchs zu beteiligen,[82] hat grundsätzlich Charme, sind die wertvollen Dienstleistungen, welche Diensteanbieter vermitteln, doch auch das Produkt des Datenstocks, den die Nutzer einbringen. Allerdings sind die Kollateralschäden eines solches Shareholder-value-Konzepts größer als sein Nutzen. Denn es setzt kontraproduktive Anreize, treibt damit im Ergebnis den Teufel mit dem Beelzebub aus. Die Kapitalisierung personenbezogener Daten bereitet nämlich einer Kommerzialisierung der Persönlichkeit den Boden, welche immaterielle Grundwerte der Gesellschaft einer Ökonomisierungslogik unterwirft. Sie lässt ökonomisches Kalkül in gesellschaftliche Handlungsräume eindringen, die sich einer Erfassung durch wirtschaftliche

---

76 Vgl. dazu insbesondere *Schneider/Härting*, ZD 2011, 63 (64 f.); *Härting*, AnwBl 2012, 716 ff.; *Schneider/Härting*, CR 2014, 306 (308 f.).

77 In diese Richtung gehen Erwägungsgrund Nr. 66a, 70 S. 4 - Nr. 74a, Art. 33 Datenschutz-Grundverordnung.

78 Siehe dazu auch *Monopolkommission*, Hauptgutachten XX 2012/2013 – Kap. 1: Google, Facebook & Co. – eine Herausforderung für die Wettbewerbspolitik, 2014, S. 62 ff. (Rn. 20 ff.) u. S. 66 ff. (Rn. 39 ff.).

79 U.a. Abstellungsverfügungen, einstweilige Maßnahmen und Vorteilsabschöpfungen. Diese Reaktionsmöglichkeiten spiegeln sich aufgrund der Überprägung des nationalen Kartellrechts durch das Unionskartellrecht vollständig im GWB wider.

80 Beispiele dafür liefern die EU-Wettbewerbsverfahren gegen Microsoft Nr. 39530 (Microsoft – Tying) und Intel Nr. 37990 (Intel Corporation). Dazu *Schultz*, EU-Strafe für Microsoft: Machtlos gegen die Web-Giganten, Spiegel online vom 6.3.2013.

81 Entwurf eines Gesetzes zur Verbesserung der zivilrechtlichen Durchsetzung von verbraucherschützenden Vorschriften des Datenschutzrechts, BR-Drucks. 55/15; dazu etwa *Gola/Wronka*, RDV 2015, 3 (6 ff.); *Weidlich-Flattern*, ZRP 2014, 196 ff.; *Zinke*, Eine Erweiterung der Verbandsklagebefugnisse auf datenschutzrechtliche Verstöße stärkt den Datenschutz in Zeiten von Big Data, in: Taeger (Hrsg.), Big Data & Co, 2014, S. 161 ff.

82 Vgl. dazu etwa *Tene/Polonetsky*, Northwestern Journal of Technology and Intellectual Property 11 (2013), 239 ff.; *Dorner*, CR 2014, 617 (626); *Zech*, C&R 2015, 137 ff. jeweils m. w. N.

Metrik gerade entziehen sollen. Führt man sich vor Augen, für welche geringen ökonomischen Gegenwerte Menschen bereit sind, ihre Persönlichkeit ausleuchten zu lassen,[83] stellt eine wirtschaftliche Partizipation des Nutzers an den wirtschaftlichen Erträgen, die Massendatenauswertungen von Persönlichkeitspräferenzen ermöglichen, schnell einen Persilschein aus, den inkommensurablen Wert der Persönlichkeit mit den Füßen wirtschaftlicher Macht zu treten[84] – mit Folgen, die beispielhaft das Verhalten des reichen Römers *Lucius Veratius* macht, der sich – nach der Erzählung »Ohrfeigen gegen Barzahlung« von *Aulus Gellius* im 2. Jahrhundert n. Chr.[85] – gleichsam einen Sport daraus machte, seine Mitmenschen im Vorübergehen zu ohrfeigen, da die 25 Asse, die das römische Recht für derartige Erniedrigungen als wirtschaftliche Sanktion vorsah, für ihn als kühlen wirtschaftlichen Rechner eine Einladung zum Handeln war.

b) Ein Internet-Völkerrecht zwischen Macht und Ohnmacht

Je weniger Internetdienstleistungen an nationalen Grenzen Halt machen und je stärker sich eine weltwirtschaftlich und menschenrechtlich sensible digitale Machtumverteilung auf Internetkonzerne abzeichnet, umso deutlicher tritt der Bedarf nach einer wirksamen weltumspannenden Regulierung zutage. Zwar steht die Weiterentwicklung des Völkerrechts hin zu einer Allgemeinen Erklärung digitaler Menschenrechte weit oben auf der Tagesordnung vieler freiheitlich-demokratischer Staaten[86], Staatenverbünde und NGOs. Strategiepapiere wie die »International Strategy for Cyberspace: Prosperity, Security and Openness in a Networked World« der USA[87], das »IBSA Joint Statement, Open Consultations on Enhanced Cooperation«[88] Indiens, Brasiliens und Südafrikas sowie die »Council of Europe Strategy 2012-2015 Internet Governance«[89] liefern erste Blaupausen für ein völkerrechtliches Internetregelwerk. Das regulatorische Augenmerk gilt dabei insbesondere der Internetwirtschaft, der Internetsicherheit und den Menschenrechtsgewährleistungen digitaler Technologienutzung, allen voran der Garantie des Privatsphärenschutzes. Verfahrensrechtlich sind sie eingebettet in den Grundsatz territorialer Gerichtsbarkeit, die Verpflichtung zu zwischenstaatlicher Kooperation und das Prinzip akteurs-übergreifender Kollaboration.[90]

Allerdings gibt die Erfahrung mit der Wirkmacht des Völkerrechts wenig Anlass zur Hoffnung auf eine gesteigerte Durchschlagskraft in der digitalen Welt. Der kleinste gemeinsame Nenner bestimmt typischerweise das Tempo, in dem die völkerrechtliche Regulierung voranschreitet. Mit dem dynamischen

---

83 Dazu S. 15 mit Fn. 39.

84 Im Hinblick auf die Welt der industriellen Fertigung stellt sich die Sachlage anders dar und sind andere Wertungen angezeigt. Dort baut das Geschäftsmodell vieler Hersteller auf der exklusiven Auswertung über den gesamten Produktlebenszyklus der Anlage auf. Nicht der Verkauf der Anlage als solcher, sondern vor allem ihre Wartung bildet dort vielfach den Ankerpunkt des Gewinns. Entsprechend ist die Sicherung des ausschließlichen Verwertungsrechts an den Daten, welche die Anlage generiert, eine zentrale Geschäftsgrundlage des Unternehmens.

85 *Aulus Gellius*, Noctes Atticae 20, 1, 13.

86 Totalitäre Staaten begegnen der Kommunikationsmacht des Internets demgegenüber durch massive tatsächliche Eingriffe in die Netzfreiheit, insbesondere durch Internetzensur, Verbot unliebsamer Plattformen und Verlangsamung oder gar zeitweilige Abschaltung des Internets.

87 Online abrufbar unter www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf (27.4.2015).

88 Online abrufbar unter http://unpan1.un.org/intradoc/groups/public/documents/un-dpadm/unpan043559.pdf (27.4.2015).

89 Internet Governance – Council of Europe Strategy 2012-2015, CM (2011)175 final.

90 Vgl. *Uerpmann-Wittzack*, German Law Journal 1 (2010), 1245 ff.

technologischen Wandel und seinen wachsenden Regelungsbedürfnissen hält das nicht hinreichend Schritt. Die Verständigung auf ein niedrigeres als das nationale Datenschutzniveau ist dann nicht selten der Preis der völkerrechtlichen Annäherung. Die Vorstellung, hohe deutsche und europäische Datenschutzstandards in Konkurrenz mit den US-amerikanischen Unternehmen Facebook, Google & Co. aus dem Silicon Valley etablieren zu können, entpuppt sich im Zweifel als regulatorischer Tagtraum.

Dies ist auch der Ausgangspunkt eines Kulturkampfes um die Hegemonie von Privacy-Idealen und Grundvorstellungen. Er bricht sich paradigmatisch in den Protesten und öffentlichen Debatten Bahn, die am Rande der Verhandlungen um das Freihandelsabkommen der EU mit den USA (Transatlantic Trade and Investment Partnership [TTIP][91]) stattfinden. Die Auseinandersetzung um das »Chlorhühnchen« steht stellvertretend für die Strukturentscheidung, ob sich ein wirtschaftsliberales US-amerikanisches oder ein stärker Verbraucherschutzidealen verpflichtetes europäisches Grundverständnis durchsetzt.

Im Hintergrund stehen dabei auch unterschiedliche Leitvorstellungen zum Verhältnis von Privatheit und Öffentlichkeit, welche diesseits und jenseits des Atlantiks bislang den Umgang mit personenbezogenen Informationen prägen. Während diese in der analogen Welt noch friedlich koexistierten, prallen sie in der digitalen Welt als gesellschaftliche und ökonomische Gegenentwürfe und unterschiedliche Rechtstraditionen unmittelbar aufeinander.

Während nach deutschem Grundverständnis Privatheit die umfassende Kontrolle über persönliche Daten – sowohl gegenüber staatlichen als auch privaten Stellen – und die autonome Verfügungsbefugnis Teil der Persönlichkeitsentfaltung und des Selbstbestimmungsrechts als einer selbst definierten Abgrenzung zwischen öffentlichem Raum und privater Rückzugsbasis ist, [92] begibt sich nach US-amerikanischem Grundverständnis derjenige, der die Öffentlichkeit sucht, weitgehend seines Schutzes vor Auswertung und Nutzung seiner Daten. Entsprechend der sog. »Third-party doctrine«[93] verliert, wer einem Dritten freiwillig Informationen offenbart, das berechtigte Vertrauen in einen Schutz der Privatheit: »With third parties, like telephone companies, banks, or even other individuals, the government can acquire that information from the third-party absent a warrant without violating the individual's Fourth Amendment rights.«[94] Der vierte Verfassungszusatz, welcher einen begrenzten verfassungsrechtlichen Schutz auf Privatsphäre gewährleistet[95], findet in diesen Fällen schon keine Anwendung.[96] Jedes Datum, das öffentlich zugänglich ist, darf jeder Private und jede Behörde beliebig sammeln, sei es der Blick in den öffentlich einsehbaren privaten Garten, sei es der Eintrag auf einer Homepage.[97] In allen anderen

---

91 Informationen dazu hält die Europäische Kommission unter http://ec.europa.eu/trade/policy/in-focus/ttip/index_de.htm (27.4.2015) bereit.

92 Entsprechend greift nach deutschem Verständnis nicht erst die Verwertung, sondern bereits die Speicherung von Daten, also die potenzielle Gefährdung von Privatheit, in das informationelle Selbstbestimmungsrecht ein. Vgl. BVerfGE 120, 378 (399 ff.).

93 Supreme Court – United States v. Miller, 425 U.S. 435 (1976); Supreme Court – Smith v. Maryland, 442 U.S. 735 (1979). Die Third-party doctrine steht jedoch angesichts ihrer wahrgenommenen Uferlosigkeit in der Kritik. Die obersten Gerichte einzelner Bundesstaaten übernehmen sie nicht; vgl. *Henderson*, Cath. U. L. Rev. 55 (2006), 373 (395).

94 *Executive Office of the President*, Big Data: Seizing Opportunities, Preserving Values, 2014, S. 33.

95 Vgl. z.B. Supreme Court – Katz v. United States, 389 U.S. 347 (1967).

96 *Kerr,* The case for the third-party doctrine, 107 Mich. L. Rev. (2009) 561 (563).

97 Auch das deutsche Datenschutzrecht gesteht verantwortlichen Stellen für allgemein zugängliche Quellen ein Auswertungs- und Nutzungsprivileg zu. Für private Stellen ist die Privilegierung grundsätzlich vorbehaltlos – sowohl bei der Nutzung für eigene Geschäftszwecke (§ 28 Abs. 1 S. 1 Nr. 3 BDSG) als auch bei der geschäftsmäßigen Datenspeicherung zum Zwecke der Übermittlung (§ 29 Abs. 1 S. 1 Nr. 2 BDSG) sowie bei der geschäftsmäßigen Datenerhebung und -speicherung für Zwecke der Markt- oder Meinungsforschung (§ 30a Abs. 1 S. 1 Nr. 2 BDSG). Öffentliche Stellen bleiben insoweit jedoch immer an die Erforderlichkeit zur Wahrnehmung einer öffentlichen Aufgabe gebunden (vgl. für öffentliche Stellen des

Fällen reicht der Schutz so weit, wie eine Person eine begründete Erwartung auf Privatheit hegen darf (»reasonable expectation of privacy«). Datenschutz ist in den USA insofern nicht durchgängiger, sondern punktueller Freiheitsschutz.[98] Privatheit ist dort primär der Schutz vor dem Einfluss staatlicher Stellen auf die individuelle Entfaltungsfreiheit – eben nicht der Schutz vor anderen Privaten, seien es auch Internet-Großkonzerne.

Allerdings wächst auch in den Vereinigten Staaten das Bewusstsein dafür, dass Bürger der Herauslösung von Daten aus dem jeweiligen Kontext und einem Missbrauch ihrer aus Massendatenbeständen auslesbaren personenbezogenen Informationen durch andere Private nicht schutzlos gegenüber stehen sollten. Die Möglichkeiten einer Personalisierung der Preisbildung sowie sämtlicher Online-Dienstleistungen und das damit einhergehende Diskriminierungspotenzial lösen einen Prozess des Nachdenkens über das dem Datenschutz traditionell skeptisch gegenüberstehende amerikanische Grundmodell aus. Die Regierung von Präsident Obama hat dementsprechend im Jahr 2012 ein umfassendes Konzept für den Verbraucher-Privatsphärenschutz unter Digitalisierungsbedingungen vorgelegt.[99] Es formuliert u.a. eine »Consumer Privacy Bill of Rights«, die sieben Grundsätze des fairen Umgangs mit personenbezogenen Informationen umschließt: individuelle Kontrollrechte, Transparenz, Kontextbindung, Sicherheit, Genauigkeit und Begrenzung der Datenerhebung sowie -verarbeitung und Verantwortlichkeit der Unternehmen.[100] Die Umsetzung des Gesetzesvorschlags in dem von einer Republikaner-Mehrheit dominierten Kongress gilt jedoch als unwahrscheinlich.[101]

3. Multi-Stakeholder-Ansatz und Selbstregulierung im Digitalisierungskontext

Je unwegsamer, schwerfälliger und wirkungsärmer (völker-)rechtliche Durchsetzungsmechanismen sind, umso eher können private Akteure einen Weg ebnen, zeitgerecht auf Governance-Defizite des Internets zu reagieren. Ein prominentes Beispiel – mit Licht- wie Schattenseiten (insbesondere der Gefahr amerikanischer Fremddominanz und Unabhängigkeitsgefährdung)[102] – bildet die Vergabe von Namen und Adressen im Internet einschließlich der Koordination des Domain Name Systems (DNS) und der Zuteilung von IP-Adressen.[103] Für sie zeichnet die 1998 in Kalifornien als Non-Profit-Organisation gegründete Internet Corporation for Assigned Names and Numbers (ICANN) verantwortlich.[104] Ihre Willensbildung ist einem konsensorientierten Abstimmungsprozess mit der Gemeinschaft der Internetnutzer und Stakeholder unterworfen; das Verfahren legt die Satzung der ICANN fest.

Bundes: § 13 Abs. 1 und § 14 Abs. 1 BDSG). Darüber hinaus beschränkt sich die Privilegierung ausschließlich auf allgemein zugängliche Quellen, erstreckt sich aber nicht generell auf bei Dritten verfügbare Daten. Insoweit greift grundsätzlich eine strikte Zweckbindung. Zum Grundrechtsschutz im Hinblick auf allgemein zugängliche Daten siehe insbesondere BVerfGE 120, 378 (399); BVerfG (1. Kammer des Ersten Senats), NVwZ 2007, 688 (690 f.);

98 *Masing*, RDV 2014, 3 (5); vgl. auch den Kurzüberblick über die US-amerikanischen Regelungen *Hense/Rengers*, Social CRM, in: Taeger (Hrsg.), Big Data & Co, 2014, S. 219 (224 ff.).

99 *The White House*, Consumer Data Privacy in a Networked World, 2012.

100 *The White House* (Fn. 99), S. 47 f.

101 *Singer*, White House Proposes Broad Consumer Data Privacy Bill, New York Times vom 27.2.2015, http://www.nytimes.com/2015/02/28/business/white-house-proposes-broad-consumer-data-privacy-bill.html?_r=0 (20.3.2015).

102 Vgl zu ihr etwa *Voegeli*, Die Regulierung des Domainnamensystems durch die Internet Corporation for Assigned Names and Numbers (ICANN), 2006, S. 59 ff. und 103 ff.

103 Vgl. die Standard-Registry-Vereinbarung der ICANN unter http://newgtlds.icann.org/en/applicants/agb/agreement-approved-09jan14-en.pdf (27.8.2014).

104 Als zivilrechtliche Organisation koordiniert sie ihre internationale Zusammenarbeit mit anderen Organisationen, insbesondere den regionalen Internet Registries, über zivilrechtliche Verträge, die auch die zur Finanzierung der ICANN von

In ihrer Neigung zu privater Selbstregulierung[105] als Handlungsinstrument hat die Internet-Wirtschaft eine Vielzahl privater Regelwerke und Standards mit nachhaltiger praktischer Relevanz für den Digital Commerce hervorgebracht.[106] Sie avancieren – entsprechend dem Vorbild der »lex mercatoria« – als Gesamtkomplex zusehends zu einer »lex digitalis«. Die Einbindung privaten Sachverstands bürgt für Sachnähe und Flexibilität; mit ihr kann eine höhere Akzeptanz und Vollzugseffizienz korrespondieren.[107] Diesem Regelungsgedanken hat sich auch die Selbstverpflichtungsregelung des § 38a BDSG verschrieben. Nachhaltigen Niederschlag in der Rechtspraxis hat sie bislang jedoch nicht gefunden.[108] Bislang füllen alleine die Verhaltensregeln des Gesamtverbands der Deutschen Versicherungswirtschaft den Regelungsgedanken eines Codes of Conduct i. S. d. § 38a BDSG inhaltlich aus.[109]

Angesichts der infrastrukturellen, wirtschaftlichen und gesellschaftlichen Bedeutung des Internets als Interaktions-, Vertriebs-, Dienstleistungs- und Kulturplattform für das Gemeinwesen scheidet eine vollständige Überantwortung seiner globalen Regulierung an Private allerdings aus.[110] Die Implementierung hinreichender Datenschutzstandards in Zeiten von Big Data ist zu sensibel, um sie alleine in die Hände des freien Spiels der Marktkräfte zu legen. Die Instrumente können gesetzliche Vorgaben nur ergänzen, sie aber nicht ersetzen. Regulierte Selbstregulierung kann immerhin eine Facette eines Multi-Stakeholder-Ansatzes sein, der staatliche Akteure, Privatwirtschaft und Zivilgesellschaft in internationalen Gremien gemeinsam über regulatorische Maßnahmen entscheiden lässt und dadurch ihre jeweiligen Eigenrationalitäten für das gemeine Wohl zur Entfaltung bringt. Um diese Kräfte zu beflügeln, hat das Generalsekretariat der Vereinten Nationen im Jahre 2006 das Internet Governance Forum (IGF) eingerichtet. Es bringt Politiker, Regierungsbeamte, Internetaktivisten, Branchenvertreter, Wissenschaftler und Technologieexperten zusammen; ihm wird in Zukunft eine noch wichtigere Rolle zuwachsen.[111] Parallel zu dieser top-down initiierten Gremienarbeit lassen sich auch vielfältige zivilgesellschaftliche und bottom-up veranlasste Initiativen für die Entwicklung einer internationalen Internet Governance beobachten, wie beispielsweise die Idee eines Digitalen Kodex des Deutschen Instituts für Vertrauen und Sicherheit im Internet (DIVSI)[112]. Sie zielt darauf, mithilfe der disziplinierenden Kraft der Selbstregulierung dem unternehmerischen Handeln digitaler Unternehmen Handlungsleitplanken setzen. Das Zusammenspiel

---

den Registries zu zahlenden Gebühren regeln. Vgl. die Statuten der ICANN online unter https://www.icann.org/resources/pages/bylaws-2012-02-25-de (20.12.2014).

105 Zum Konzept regulierter Selbstregulierung als Instrument des Wirtschaftsrechts siehe insbesondere jüngst *Weiß*, Der Staat 53 (2014), 555 (559 ff.) m. w. N. sowie grundlegend die Beiträge bei Berg (Hrsg.), Regulierte Selbstregulierung als Steuerungskonzept des Gewährleistungsstaates, 2001.

106 Vgl. zu Konzepten der nationalen Werbewirtschaft *Himmels*, Behavioural Targeting im Internet, 2013, S. 76 ff. mit Blick auf den Bundesverband Digitale Wirtschaft e. V., der ein nationales Konzept der Selbstregulierung entwickelt hat.

107 Ausführlich dazu *Himmels* (Fn. 106), S. 71 ff. Ihr weiteres Argument, dass dadurch grenzüberschreitende Abläufe nicht mehr an unterschiedlichen nationalen Regeln gemessen werden müssten, überzeugt freilich nicht. Zum einen hat auch grenzüberschreitende Selbstregulierung mit Effizienzverlusten zu kämpfen. Zum anderen bleibt das Bedürfnis nationaler normativer Mindeststandards unberührt. Für ihre Durchsetzung kann das Wettbewerbsrecht ein wirksames Instrument bilden.

108 Art. 38 der Datenschutz-Grundverordnung knüpfte daran an und schreibt den Regelungsgedanken des § 38a BDSG bzw. des Art. 27 Abs. 2 der Datenschutzrichtlinie 95/46/EG in ihrem Entwurf auf unionaler Ebene (in sehr ähnlicher Weise) fort. Vgl. zu § 38a BDSG bspw. *Kranig/Peintinger*, ZD 2014, 3 (4 ff.); *Vomhof*, PinG 2014, 209 (210 ff.).

109 Zu ihrem Inhalt: *Ritzer*, Verhaltensregeln (Code of Conduct) im Datenschutz – Gestaltungsmöglichkeiten für Unternehmen in Verbänden, in: Taeger (Hrsg.), Big Data & Co, 2014, S. 501 (504 ff.); *Petri*, in: Simitis (Hrsg.), BDSG, 7. Aufl., 2011, § 38a, Rn. 1 ff.

110 *Himmels* (Fn. 106), S. 95.

111 Die EU avisiert in ihrer Digitalen Agenda eine gezielte Förderung des IGF durch Schärfung seines Profils und Verteidigung des Multi-Stakeholder-Ansatzes, vgl. dazu https://ec.europa.eu/digital-agenda/en/international/action-98-support-internet-governance-forum (20.12.2014).

112 Vgl. https://www.divsi.de/projekte/digitaler-kodex/ (20.12.2014).

beider Initiativstränge – top-down und bottom-up – verspricht ein fruchtbares Ringen um die Etablierung international abgestimmter, gemeinwohlorientierter Spielregeln für die Codierung der digitalen Lebenswelt von morgen.

Eine zentrale Aufgabe des nationalen Rechts in diesem Regelungskonzert wird es sein, dem Selbstdatenschutz und der digitalen Souveränität der Bürger eine wahrnehmbare Stimme zu geben. Seine Mission ist es, entsprechend den Idealen der Aufklärung, die digitale Unversehrtheit des Einzelnen – als Pendant zum staatlichen Schutz der körperlichen Integrität – zu gewährleisten und die freiheitliche Rechtskultur unveräußerlicher und einklagbarer Bürgerrechte in die Rechtspraxis der digitalen Zukunft zu transformieren. Nur, wenn es gelingt, den Impetus des technisch Möglichen in die Bahnen des gesellschaftlich Sinnvollen zu lenken, verbessern die Segnungen der digitalen Revolution im Ergebnis die Lebensqualität – und verhindern, dass das Leben in Smart Houses in Smart Cities einem digitalen Panoptikum im *Foucault*'schen Sinne gleicht. Anderenfalls entpuppen sich die technologischen Diener der Gegenwart womöglich als die Fußfesseln unserer Freiheit und Privatheit.

Literaturverzeichnis

Acquisti, Alessandro/John, Leslie/Loewenstein, George, What is privacy worth?, Journal of Legal Studies 42 (2013), S. 249–274.

Albrecht, Jan Philipp, Die EU-Datenschutzgrundverordnung rettet die informationelle Selbstbestimmung!, Ein Zwischenruf für einen einheitlichen Datenschutz durch die EU, ZD 2013, S. 587–591.

Ankenbrand, Hendrik, Eine Villa aus dem 3D-Drucker, FAZ vom 6.3.2015, S. 22.

Artikel-29-Datenschutzgruppe, Opinion 8/2014 on the Recent Developments on the Internet of Things, WP 223, Brüssel, 2014.

Bauer, Zorah Mari, Lernen gestern – heute – morgen, Der Paradigmenwechsel des Lernens, in: Ludwig, Luise/Narr, Kristin/Frank, Sabine u.a. (Hrsg.), Lernen in der digitalen Gesellschaft – offen, vernetzt, integrativ, Berlin, 2013, S. 128–133.

Berg, Winfried (Hrsg.), Regulierte Selbstregulierung als Steuerungskonzept des Gewährleistungsstaates, Ergebnisse des Symposiums aus Anlass des 60. Geburtstages von Wolfgang Hoffmann-Riem Bd. 4, Berlin, 2001.

Bräutigam, Peter/Klindt, Thomas, Industrie 4.0, das Internet der Dinge und das Recht, NJW 2015, S. 1137–1142.

Brynjolfsson, Erik/McAfee, Andrew, Race against the machine, How the digital revolution is accelerating innovation, driving productivity, and irreversibly transforming employment and the economy, Lexington, Mass., 2012.

Brynjolfsson, Erik/McAfee, Andrew, The second machine age, Work, progress, and prosperity in a time of brilliant technologies, 2014.

Buchner, Benedikt: Datenschutz im vernetzten Automobil, DuD 2015, S. 372–377.

Bull, Hans Peter, Persönlichkeitsschutz im Internet, Reformeifer mit neuen Ansätzen, NVwZ 2011, S. 257–263.

Cichy, Patrick, Das Verletzte Fahrzeug – eine Bedrohung für die Privatsphäre?, PinG 2 (2014), S. 200–202.

Coase, Ronald H., The Nature of the Firm, Economica 4 (1937), S. 386.

DIVSI, Milieu-Studie zu Vertrauen und Sicherheit im Internet, Hamburg, 2012.

Doepfner, Mathias, Offener Brief an Eric Schmidt: Warum wir Google fürchten, FAZ vom 16.4.2014, S. 9.

Dorner, Michael, Big Data und „Dateneigentum", Grundfragen des modernen Daten- und Informationshandelns, CR 2014, S. 617–628.

Enzensberger, Hans Magnus, Wehrt Euch!, FAZ vom 1.3.2014, S. 9, www.faz.net/aktuell/enzensbergers-regeln-fuer-die-digitale-welt-wehrt-euch-12826195.html6 (23.12.2014).

Epping, Volker/Hillgruber, Christian (Hrsg.), Beck'scher Online-Kommentar GG, 24. Edition, 2015.

Executive Office of the President, Big Data: Seizing Opportunities, Preserving Values, 2014.

Foucault, Michel, Überwachen und Strafen: die Geburt des Gefängnisses, 14. Aufl., 2013.

Franzius, Claudio/Lejeune, Stefanie/Lewinski, Kai von/Meßerschmidt, Klaus/Gerhrad, Michael, Rossi, Matthias/Schilling, Theodor/Wysk, Peter (Hrsg.), Beharren, Bewegen: Festschrift für Michael Kloepfer zum 70. Geburtstag, Berlin, 2013.

Frey, Carl Benedict/Osborne, Michael A., The Future of Employment, How susceptible are jobs to computerisation?, Oxford, 2013.

Geiselberger, Heinrich (Hrsg.), Big Data, Das neue Versprechen der Allwissenheit, Berlin, 2013.

Gola, Peter/Wronka, Georg, Datenschutzrecht im Fluss, RDV 2015, S. 3–10.

Greve, Holger, Drittwirkung des grundrechtlichen Datenschutzes im digitalen Zeitalter, in: Franzius, Claudio/Lejeune, Stefanie/Lewinski, Kai von u.a. (Hrsg.), Beharren, Bewegen: Festschrift für Michael Kloepfer zum 70. Geburtstag, Berlin, 2013, S. 665–677.

Härting, Niko, Datenschutzrecht: Verbotsprinzips und Einwilligungs Fetisch, Warum die alten Rezepte versagen. Plädoyer aus Sicht eines Anwalts, AnwBl 2012, S. 716–720.

Hansen, Marit: Das Netz im Auto & das Auto im Netz, Herausforderungen für eine datenschutzgerechte Gestaltung vernetzter Fahrzeuge, DuD 2015, S. 367–371.

Heller, Christian, Post Privacy, Prima leben ohne Privatsphäre, München, 2011.

Henderson, Learning from all fifty states, How to apply the fourth amendment and its state analogs to protect third party information from unreasonable search, Cath.U.L.Rev. 55 (2006,), S. 373.

Hense, Peter/Rengers, Katja, Social CRM, Regulatorische Rahmenbedingungen für innovative Big-Data-Anwendungen in den USA, Singapur und Australien, in: Taeger, Jürgen (Hrsg.), Big Data & Co, Neue Herausforderungen für das Informationsrecht, Edewecht, 2014, S. 219–236.

Himmels, Sabine, Behavioural Targeting im Internet, Datenschutz durch lauterkeitsrechtlich gestuetzte Selbstregulierung?, Frankfurt, 2013.

Hornung, Gerrit: Verfügungsrechte an fahrzeugbezogenen Daten, Das vernetzte Automobil zwischen innovativer Wertschöpfung und Persönlichkeitsschutz, DuD 2015, S. 359–366.

Hornung, Gerrit/Goeble, Thilo, „Data ownership" im vernetzten Automobil, Die rechtliche Analyse des wirtschaftlichen Werts von Automobildaten unter Beitrag zum besseren Verständnis der Informationsordnung, CR 2015, S. 265–273.

Initiative D21 (Hrsg.), eGovernment Monitor 2014, Berlin, 2014.

Jaspers, Andreas, Die EU-Datenschutz-Grundverordnung, DuD 2012, S. 571–575.

Kaku, Michio, Die Physik der Zukunft, Unser Leben in 100 Jahren, 6. Aufl, Reinbek bei Hamburg, 2013.

Kaku, Michio, Die Physik des Bewusstseins, Über die Zukunft des Geistes, Reinbek, 2014.

Kant, Immanuel, Beantwortung der Frage: Was ist Aufklärung?, Berlinische Monatsschrift 1784, S. 481 ff.

Kerr, Orin S., The case for the third-party doctrine, 107 Michigan Law Review (2009), p. 561–601.

Kinast, Karsten/Kühnl, Christina, Telematik und Bordelektronik – Erhebung und Nutzung von Daten zum Fahrverhalten, NJW 2014, S. 3057–3060.

Köcher, Folgenlose Ängste, FAZ vom 20.6.2014, S. 8.

Köhler, Thomas R./Wollschläger, Dirk, Die digitale Transformation des Automobils, 5 Mega-Trends verändern die Branche (Connected Car; das Internet der Dinge; Big Data und Analytics; Cloud Computing; das autonome Fahrzeug), Pattensen, 2014.

Kranig, Thomas/Peintinger, Stefan, Selbstregulierung im Datenschutzrecht, Rechtslage in Deutschland, Europa und den USA unter Berücksichtigung des Vorschlags zur DS-GVO, ZD 2014, S. 3–9.

Kraus, Michael, Telematik – wem gehören Fahrzeugdaten?, in: Taeger, Jürgen (Hrsg.), Big Data & Co, Neue Herausforderungen für das Informationsrecht, Edewecht, 2014, S. 377–390.

Kreibich, Rolf, Von Big zu Smart - zu Sustainable?, APuZ 2015, S. 20–26.

Kremer, Sascha, Connected Car - intelligente Kfz, intelligente Verkehrssysteme, intelligenter Datenschutz?, RDV 2014, S. 240–252.

Kroes, Neelie, Ich bin nicht naiv, und Europa darf es auch nicht sein, FAZ vom 24.3.2014, S. 9.

Kurz, Constanze/Rieger, Frank, Arbeitsfrei, Eine Entdeckungsreise zu den Maschinen, die uns ersetzen, München, 2015.

Ludwig, Luise/Narr, Kristin/Frank, Sabine/Staemmler, Daniel (Hrsg.), Lernen in der digitalen Gesellschaft – offen, vernetzt, integrativ, Berlin, 2013.

Lutz, Lennart, Autonome Fahrzeuge als rechtliche Herausforderung, NJW 2015, S. 119–124.

Manyika, James/Chui, Michael/Bughin, Jacques/Dobbs, Richard/Bisson, Peter/Marrs, Alex, Disruptive technologies: Advances that will transform life, business, and the global economy, San Francisco, 2013.

Masing, Johannes, Datenschutz - ein unterentwickeltes oder überzogenes Grundrecht?, RDV 2014, S. 3–9.

Monopolkommission, Hauptgutachten XX 2012/2013 – Kap. 1: Google, Facebook & Co. – eine Herausforderung für die Wettbewerbspolitik, 2014.

Morozov, Evgeny, Achtung, Achtsamkeit!, FAZ vom 17.2.2014, S. 35.

Nordemann, Bernd/Rüberg, Michael/Schaefer, Martin, 3D-Druck als Herausforderung für die Immaterialgüterrechte, NJW 2015, S. 1265–1271.

Oppermann, Thomas, Deutschland in guter Verfassung?, 60 Jahre Grundgesetz, JZ 2009, S. 481–491.

Pentland, Alex, Society's Nervous System: Building Effective Government, Energy, and Public Health Systems, 2010.

Piketty, Thomas, Le capital au XXIe siècle, Paris, 2013.

Pötters, Stephan, Primärrechtliche Vorgaben für eine Reform des Datenschutzrechts, RDV 2015, S. 10–16.

Raabe, Oliver/Weis, Eva, Datenschutz im »Smarthome«, RDV 2014, S. 231–240.

Rammo, Katrin/Holzgräfe, Datenschutz bei vernetzten Autos – elektronische Fahrtenbücher, in: Taeger, Jürgen (Hrsg.), Big Data & Co, Neue Herausforderungen für das Informationsrecht, Edewecht, 2014, S. 351–365.

Rieß, Joachim/Agard, Andreas, Der Schutz von Kundendaten im Kontext des vernetzten Fahrzeugs, PinG 2015, S. 98–103.

Rifkin, Jeremy, Die Null-Grenzkosten-Gesellschaft, Das Internet der Dinge, kollaboratives Gemeingut und der Rückzug des Kapitalismus, 2014.

Ritzer, Christoph, Verhaltensregeln (Code of Conduct) im Datenschutz – Gestaltungsmöglichkeiten für Unternehmen in Verbänden, in: Taeger, Jürgen (Hrsg.), Big Data & Co, Neue Herausforderungen für das Informationsrecht, Edewecht, 2014, S. 501–512.

Roßnagel, Alexander: Grundrechtsausgleich beim vernetzten Automobil, Herausforderungen, Leistungsfähigkeit und Gestaltungsbedarf des Rechts, DuD 2015, S. 353–358.

Rubinyi, Kati, The Car in 2035, Mobility planning for the near future, New York, 2014.

Rüdiger, Benjamin, Smart Home - intelligentes Wohnen ohne Privatsphäre, RDV 2014, S. 253–258.

Schirrmacher, Frank, Der verwettete Mensch, in: Geiselberger, Heinrich (Hrsg.), Big Data, Das neue Versprechen der Allwissenheit, Berlin, 2013, S. 273–280.

Schirrmacher, Frank, Ego, Das Spiel des Lebens, Frankfurt, M., Zürich, Wien, 2013.

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

Schneider, Jochen/Härting, Niko, Warum wir ein neues BDSG brauchen, Kritischer Beitrag zum BDSG und zu dessen Defiziten, ZD 2011, S. 63–68.

Schneider, Jochen/Härting, Niko, Datenschutz in Europa – Plädoyer für einen Neubeginn, Zehn „Navigationsempfehlungen", damit das EU-Datenschutzrecht internettauglich und effektiv wird, CR 2014, S. 306–312.

Schultz, Stefan, EU-Strafe für Microsoft: Machtlos gegen die Web-Giganten, Spiegel online vom 6.3.2013, www.spiegel.de/forum/wirtschaft/eu-strafe-fuer-microsoft-machtlos-gegen-die-web-giganten-thread-84616-1.html.

Schulz, Martin, Technologischer Totalitarismus - Warum wir jetzt kämpfen müssen?, FAZ vom 6.2.2014, S. 25, http://www.faz.net/aktuell/feuilleton/debatten/die-digital-debatte/politik-in-der-digitalen-welt/technologischer-totalitarismus-warum-wir-jetzt-kaempfen-muessen-12786805.html (3.4.2015).

Schulz, Roland, Billige Witze, http://sz-magazin.sueddeutsche.de/texte/anzeigen/42640/Billige-Witze (3.4.2015).

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

Simitis, Spiros (Hrsg.), Bundesdatenschutzgesetz, 7. Aufl., Baden-Baden, 2011.

Singer, Natasha, White House Proposes Broad Consumer Data Privacy Bill, New York Times vom 27.2.2015, http://www.nytimes.com/2015/02/28/business/white-house-proposes-broad-consumer-data-privacy-bill.html?_r=0 (20.3.2015).

Solmecke, Christian, Rechtliche Aspekte des 3D-Drucks, in: Taeger, Jürgen (Hrsg.), Big Data & Co, Neue Herausforderungen für das Informationsrecht, Edewecht, 2014, S. 283–295.

Stiglitz, Joseph E., Der Preis der Ungleichheit, Wie die Spaltung der Gesellschaft unsere Zukunft bedroht, München, 2012.

Taeger, Jürgen (Hrsg.), Big Data & Co, Neue Herausforderungen für das Informationsrecht, Edewecht, 2014.

Tene, Omer/Polonetsky, Jules, Big Data for All: Privacy and User Control in the Age of Analytics, Northwestern Journal of Technology and Intellectual Property 11 (2013), S. 239–273.

Thaler, Richard, Toward a Positive Theory of Consumer Choice, Journal of Economic Behavior and Organization 1 (1980), S. 39.

The White House, Consumer Data Privacy in a Networked World, A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy, 2012.

Uerpmann-Wittzack, Robert, Principles of International Internet Law, German Law Journal 1 (2010), S. 1245–1263.

Ullrich, Hanns, Patente, Wettbewerb und technische Normen: Rechts- und ordnungspolitische Fragestellungen, GRUR 2007, S. 817–830.

VDE, VDE-Trendreport 2014 - Schwerpunkt: Smart Citys, Frankfurt am Main, 2014.

Voegeli, Julia, Die Regulierung des Domainnamensystems durch die Internet Corporation for Assigned Names and Numbers (ICANN), Köln, 2006.

Vomhof, Martina, Verhaltensregeln nach § 38a BDSG, Der Code of Conduct der Versicherungswirtschaft, PinG 2014, S. 209–219.

Weichert, Tilo, Big Data – eine Herausforderung für den Datenschutz, in: Geiselberger, Heinrich (Hrsg.), Big Data, Das neue Versprechen der Allwissenheit, Berlin, 2013, S. 131–148.

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

Weiß, Wolfgang, Selbstregulierung der Wirtschaft – noch sinnvoll nach der Finanzkrise?, Der Staat 53 (2014), S. 555–575.

Weitzman, Martin L., The share economy, Conquering stagflation, Cambridge, Mass, 1984.

Welzer, Harald, Vorsicht, Datensammler, Wenn man etwas merkt, ist es zu spät, FAZ vom 23.4.2014, S. 9.

Zech, Herbert, Daten als Wirtschaftsgut – Überlegungen zu einem „Recht des Datenerzeugers“, C&R 2015, S. 137–146.

Zeh, Juli, Schützt den Datenkörper!, FAZ vom 11.2.2014, S. 34.

Zinke, Michaela, Eine Erweiterung der Verbandsklagebefugnisse auf datenschutzrechtliche Verstöße stärkt den Datenschutz in Zeiten von Big Data, in: Taeger, Jürgen (Hrsg.), Big Data & Co, Neue Herausforderungen für das Informationsrecht, Edewecht, 2014, S. 161–170.

Zuboff, Shoshana, Die Google-Gefahr: Schürfrechte am Leben, FAZ vom 30.4.2014, S. 9.