Tutzinger Studien zur Politik

herausgegeben von der
Akademie für Politische Bildung, Tutzing

Band 8

Hans-Jürgen Papier | Ursula Münch
Gero Kellermann [Hrsg.]

Freiheit und Sicherheit

Verfassungspolitik, Grundrechtsschutz, Sicherheitsgesetze

Nomos

AKADEMIE FÜR POLITISCHE BILDUNG TUTZING

Matthias Rossi

Schutz der Privatsphäre – Aktuelle Gefährdungen

1. Einleitung

Das Thema »Schutz der Privatsphäre – Aktuelle Gefährdungen« lässt sich aus einer Vielzahl unterschiedlicher Perspektiven betrachten. Es impliziert rechtliche Überlegungen, ist aber keinesfalls und schon gar nicht in erster Linie auf diese beschränkt. Im Gegenteil: Sowohl der »Schutz der Privatsphäre« als vor allem auch deren »aktuelle Gefährdungen« verlangen primär nach einer tatsächlichen Darstellung. Freilich lassen sich beide Komponenten – die tatsächliche und die rechtliche – weder strikt voneinander trennen noch stehen sie in einem bestimmten Verhältnis zueinander. Denn ebenso, wie der rechtliche Schutz der Privatsphäre auf aktuelle Gefährdungen reagieren und sie also mindern kann, kann seine Ausgestaltung umgekehrt auch ihre Ursache sein. Zudem wird der Schutz der Privatsphäre auch in einem Rechtsstaat eben nicht nur mit den Mitteln des Rechts bewirkt. Von entscheidender Bedeutung sind daneben etwa auch technische Begebenheiten sowie vor allem soziale Standards – Aspekte, die ihrerseits zwar auch durch das Recht gesteuert werden können, sich aber letztlich einer vollständigen Regulierung entziehen bzw. ihr regelmäßig zeitlich vorausgehen.

Das Thema ist also in mehrfacher Hinsicht so komplex, dass die nachfolgende Darstellung von vorneherein nicht für sich in Anspruch nimmt, ihm in jeder Hinsicht gerecht zu werden. Dies gilt für die Ausführungen zu aktuellen (tatsächlichen) Gefährdungen ebenso wie für die Behandlung des (rechtlichen) Schutzes der Privatsphäre. Vielmehr soll das Thema in einem Dreischritt erschlossen werden: In einem ersten Schritt werden einige mehr oder weniger assoziativ ausgewählte Beispiele für aktuelle Gefährdungen benannt (2.), aus denen in einem zweiten Schritt strukturelle Gefährdungen destilliert werden (3.). In einem dritten Schritt sollen sodann die Herausforderungen skizziert werden, denen sich der (rechtliche) Schutz der Privatsphäre gegenübersieht (4.). Dabei ist bereits an dieser Stelle zu betonen, dass sich die nachfolgenden Ausführungen vor allem auf den Datenschutz und somit von vorneherein nur auf einen Teilaspekt der rechtlichen Ausge-

staltung des Schutzes der Privatsphäre beziehen. Zudem nehmen die Überlegungen eine öffentlich-rechtliche Perspektive des Schutzes der Privatsphäre ein und blenden die praktisch durchaus bedeutsamen zivilrechtlichen und die flankierenden strafrechtlichen Instrumente[1] zum Schutz des allgemeinen Persönlichkeitsrechts weitgehend aus. Auch der durch die Unverletzlichkeit der Wohnung grundrechtlich fundierte räumliche Schutz der Privatsphäre wird außen vor bleiben.

2. Beispiele für aktuelle Gefährdungen

Die moderne Welt ist voller Beispiele für Gefährdungen der Privatsphäre. Sie resultieren letztlich alle aus der ständigen und ubiquitären Verfügbarkeit und der Verknüpfbarkeit von Informationen, genauer gesagt von Daten, die zu Informationen und zu (vermeintlichem) Wissen werden können.[2] Die zeitlich und örtlich unbegrenzte Datenflut macht es dem Einzelnen im Zusammenspiel mit der kaum noch kontrollierbaren »Verlinkung« bzw. »Verlinkbarkeit« nahezu unmöglich, »selbst zu entscheiden, wer was wann und zu welcher Gelegenheit über einen weiß«.[3] Der noch 1983 als visionär erscheinende Befund des Bundesverfassungsgerichts, unter den Bedingungen der automatischen Datenverarbeitung gebe es kein belangloses Datum mehr[4], wirkt rund 30 Jahre später als Beschreibung des zentralen Problems, das aber ebenso wenig in das Bewusstsein der Bevölkerung vorgedrungen ist wie rechtlich zufriedenstellend gelöst wurde. Vielmehr hat sich das Problem im Zuge der technischen Möglichkeiten der digitalisiert vernetzten Welt potenziert: Sowohl die Datenmenge als auch ihre Verknüpfbarkeit haben Größenordnungen erreicht, gegen die sich die Möglichkeiten der automatischen Datenverarbeitung aus dem Jahr 1983 geradezu als bescheiden ausnehmen. Und sie wachsen ständig an: Jeder einzelne produziert täglich Unmengen an Daten, deren Speicherung jedenfalls nicht an technischen oder finanziellen Grenzen scheitert, sodass ihre Verfügbarkeit und Verknüpfbarkeit nicht nur theoretisch, sondern auch ganz praktisch gewährleistet ist.

---

1 Vgl. insb. die §§ 201 ff. StGB.

2 Zu den Begrifflichkeiten vgl. einführend Albers 2013: Rn. 10ff. m.w.N.

3 So die Umschreibung des Rechts auf informationelle Selbstbestimmung durch das grundlegende Volkszählungsurteil, BVerfGE 65, 1 (43).

4 BVerfGE 65, 1 (45).

Im Folgenden sollen Beispiele für aktuelle Gefährdungen der Privatsphäre aus verschiedenen (sich überschneidenden) Lebensbereichen genannt werden, die exemplarisch herausgegriffen werden, weil in ihnen besonders viele bzw. besonders sensible Daten generiert werden und weil die Verknüpfung der einzelnen Daten hier nicht nur möglich, sondern geradezu gewollt ist: der Kommunikationsbereich einschließlich der Nutzung des Internets (2.1), der Zahlungsbereich (2.2), die Mobilität (2.3), der Gesundheitsbereich (2.4), der Arbeitsbereich (2.5) sowie das sogenannte »Internet der Dinge« (2.6).

2.1 Kommunikationsbereich

Der wohl wichtigste Bereich für aktuelle Gefährdungen der Privatsphäre ist der Kommunikationsbereich einschließlich der Nutzung des Internet. Beides soll im Rahmen dieser nur typisierten Aufzählung von Gefährdungen nicht strikt voneinander getrennt werden. Denn zahlreiche der Kommunikationsformen wie etwa Mail, Twitter, Skype und sonstige Formen bedienen sich des Internet.

Die grundlegende Gefährdung der Privatsphäre liegt dabei zunächst darin, dass jeder Schritt im Internet eine Spur hinterlässt, die nachvollzogen werden kann. Jede besuchte Seite, jede Suchanfrage, jeder Klick, selbst die Dauer des Besuchs einer Seite wird registriert. Verglichen mit der realen Welt bedeutete dies, dass man ständig beobachtet wird – beim Zeitungslesen, beim Einkaufen, bei der Auswahl der Produkte, bei seinen Gesprächen in der Familie, mit Freunden, im beruflichen Alltag, beim Fernsehen wie beim Radiohören, kurzum: ständig. Schwerer als die ohnehin kaum schon vorstellbare ständige Beobachtung wiegt, dass die Beobachtung selbst ständig aufgezeichnet wird und permanent abrufbar bleibt – soweit die Daten nicht gelöscht werden, was aber regelmäßig außerhalb des Einflusses der betroffenen Person liegt. Vor diesem Hintergrund nimmt es nicht wunder, dass jegliche Nutzung des Internets als erhebliche Gefährdung der Privatsphäre zu qualifizieren ist, so sicher und unbeobachtet man sich auch fühlen mag.

Neben dieser allgemeinen Gefährdung durch die Nutzung des Internets lassen sich zahlreiche einzelne Aspekte präzisieren, die sich als konkrete Gefährdung der Privatsphäre darstellen können:

Zunächst sei der Einsatz sogenannter »Webhoster« oder »Webanalysetools« in den Blick genommen, welche das Besucheraufkommen auf einer Website zur Optimierung ebendieser messen und dabei auch die IP-Adres-

sen sammeln. Ebenfalls als ein Mittel der Webanalyse stellen sich Zählpixel auf Webseiten dar. Ein Zählpixel ist ein auf einer Website oder in einer E-Mail verstecktes kleines transparentes Bild, welches die Besucherzahlen misst bzw. anzeigt, ob eine versandte E-Mail bereits geöffnet wurde, indem es auf einen Analyse-Server heruntergeladen wird, sobald die Website bzw. die E-Mail geöffnet wird. Hierbei werden jedoch mit der IP-Adresse, den Bewegungen des Nutzers auf der Website und den Daten hinsichtlich des verwendeten Browsers etc. wieder personenbezogene Daten erhoben. IP-Adressen gelten aber als personenbezogene Daten, welche Rückschlüsse auf die benutzende Person zulassen. Ob die datenschutzrechtlichen Bedenken durch die Pseudonymisierung von IP-Adressen gänzlich ausgeräumt werden können, sei an dieser Stelle dahingestellt.[5] Problematisch ist jedenfalls, dass der konkrete Nutzer in der Regel weder von dem Einsatz solcher Instrumente weiß noch ihre Bedeutung hinreichend beurteilen kann. Mögen die gesammelten Daten auch noch so profan sein, beginnt mit ihnen doch bereits der Kontrollverlust, vor dem das Recht auf informationelle Selbstbestimmung doch gerade schützen will.

Aus dem Bereich der Mobilfunkkommunikation seien die sogenannten IMSI-Catcher angesprochen. Auf jeder Handychipkarte ist die IMSI (International Mobile Subscriber Identity), eine weltweit nur einmal vergebene Kennnummer, gespeichert. Mit Hilfe eines IMSI-Catchers[6] kann die Strafverfolgungsbehörde, wenn die Voraussetzungen des § 100i StPO vorliegen, die IMSI eines Mobilfunknutzers für spätere Maßnahmen der Telekommunikationsüberwachung gemäß §§ 100a ff. StPO ermitteln. Außerdem lassen sich der Standort der eingesetzten SIM-Karte bestimmen oder ausgehende Gespräche abhören. Bedenken gegen den IMSI-Catcher ergeben sich daraus, dass auch Daten unbeteiligter Personen erfasst werden. Gemäß § 100i Abs. 2 S. 2 StPO dürfen aber die personenbezogenen Daten Dritter ausschließlich zum Zwecke des Datenabgleichs zur Ermittlung der gesuchten Geräte- und Kartennummer verwendet werden und sind nach Beendigung dieser Maßnahme unverzüglich zu löschen.

Schließlich seien in aller Kürze auch noch die sogenannten Social Media erwähnt. Durch die Nutzung von Social Media bzw. entsprechenden Apps wie Facebook, Instagram, Twitter und vielen weiteren ist eine weitgehende »freiwillige« Aufgabe der Privatsphäre vonseiten der Nutzer erfolgt. Auf diese besonderen Probleme der »Freiwilligkeit« des Verzichts auf einen an-

5 So das LG Frankfurt, Urteil vom 18. Februar 2014 (Az. 3-10 O 86/12).

6 Vgl. hierzu Harnisch/Pohlmann 2009: 202ff.

gemessenen Schutz der Privatsphäre wird bei den strukturellen Betrachtungen zurückzukommen sein.

Ebenfalls nur angedeutet werden sollen die Gefährdungen, die vom Cloud Computing, vom Einsatz von Cookies, vom Framing sowie von zahlreichen anderen technischen Instrumenten für die Privatsphäre ausgehen. Sie alle wurzeln letztlich aber in der Verwendung des Internet.

Selbst die alte analoge Kommunikationsform des Briefverkehrs, um damit abzuschließen, ist vor der digitalen Erfassung nicht sicher. Die deutsche Post (wie auch sehr viele andere Versandunternehmen im In- und Ausland) fotografiert bzw. scannt jeden Brief, der versendet wird. Dies dient zum einen dem korrekten Briefversand, aber aus diesen Daten lässt sich auch schließen, wer wie viel Post woher und oft auch von wem bekommt. In einigen Fällen werden diese Daten auch an (nicht nur inländische) staatliche Behörden weitergegeben.

2.2 Zahlungsbereich

Neben den Internet- und Telekommunikationsunternehmen sind es vor allem die Banken und andere Zahlungsinstitute, die über so viele und so detaillierte Daten verfügen, dass von einer Gefährdung der Privatsphäre gesprochen werden muss.

Der gesamte bargeldlose Verkehr erlaubt nicht nur den an einer konkreten Transaktion Beteiligten, sondern auch den Banken – und unter bestimmten Voraussetzungen auch dem Staat mit seinen Steuer- und Strafverfolgungsbehörden – den Zugriff auf Daten, die in ihrer Summe ein sehr präzises Persönlichkeitsbild zeichnen. Ein Tages-, jedenfalls aber ein Monatsablauf stellt sich in den Bankauszügen fast schon wie ein Kalender, möglicherweise gar wie ein Tagebuch dar. Vor diesem Hintergrund ist die Aufweichung des Bankgeheimnisses nicht vorschnell dem legitimen Ziel nach einer gleichmäßigen Besteuerung und der Bekämpfung von Schwarzarbeit und Geldwäsche zu opfern, sondern nur dann hinzunehmen, wenn dafür Vorsorge getroffen ist, dass die Daten im Übrigen nicht verwendet werden.

Als problematisch erweist sich neben dem allgemeinen bargeldlosen Zahlungsverkehr vor allem das Kreditscoring. Unter Scoring versteht man systematische Verfahren, mit denen Wahrscheinlichkeiten für zukünftige Ereignisse berechnet und Entscheidungen objektiv unterstützt werden können. Beim Kreditscoring wird dieses Verfahren eingesetzt, um das Verhalten von Kunden und damit verbundene Chancen und Risiken bei Kreditgeschäften bereits im Vorfeld einschätzen zu können. Unbefriedigend an diesem Ver-

fahren ist, dass der Betroffene die für das Scoring verwendeten Daten nicht auf ihre Richtigkeit überprüfen kann. Aus datenschutzrechtlicher Perspektive ist daher insbesondere die Novelle des BDSG vom 1. April 2010 zu begrüßen. Seitdem richtet sich die Zulässigkeit des Scoringverfahrens nach § 28b BDSG, zudem sind den Betroffenen zahlreiche Auskunftsrechte eingeräumt worden. Sie mindern den Eingriff in die Privatsphäre freilich nur, wenn sie auch in Anspruch genommen werden.

Als weiteres Beispiel für eine aktuelle Gefährdung der Privatsphäre seien die zahlreichen Kunden- oder Treuekarten genannt, die nahezu jedes mittelständische oder größere Unternehmen mittlerweile anbietet. Primäres Ziel ist es, Kunden durch das Versprechen von Extrarabatten, Boni und Kaufvorteilen zum Kauf zu motivieren und an die jeweilige Handelskette zu binden. Gleichzeitig werden aber so viele kundenindividuelle Informationen wie möglich gesammelt, um mit gezielter Werbung für bestimmte Produkte den Umsatz zu steigern oder diese Informationen durch die Weitergabe an Dritte zu barem Geld zu machen. Hierzu werden Kunden mit entsprechenden Anreizen dazu bewegt, eine Einwilligungserklärung zu unterzeichnen. Kritisch zu betrachten ist, dass dem »gläsernen Konsumenten«[7] oftmals nicht bewusst ist, welche Folgen eine solche Einwilligungserklärung nach sich zieht. Im Vordergrund steht vielmehr »die Belohnung« für die Auskunftsfreudigkeit.

Schließlich sei auch die Gefährdung des sogenannten »Phishing« dem Bereich des Zahlungsverkehrs zugeordnet, weil es dabei in vielen Fällen darum geht, Zugriff auf die Online-Konten der Opfer zu erhalten. Beim Phishing wird der Betrogene durch angeblich von seiner Bank stammende Mails oder Anrufe darum gebeten, sich mit seinen privaten Daten auf einer separaten Seite einzuloggen. Mithilfe dieser gefälschten Seite werden sodann die Daten abgegriffen, die im Folgenden auf der richtigen Seite zum Zugriff auf das Geld verwendet werden.

2.3 Mobilität

Hinsichtlich der Mobilität seien verschiedene Möglichkeiten in Erinnerung gerufen, den Aufenthaltsort von Personen (genauer natürlich nur von technischen Geräten) im Nachhinein zu erfassen oder gar permanent zu kon-

7 Müller 2002: 75.

trollieren und auf diese Art und Weise Bewegungsprofile zu erstellen, die ihrerseits als erhebliche Eingriffe in die Privatsphäre zu qualifizieren sind.

Zunächst ist insofern ins Bewusstsein zu rufen, dass satellitengestützte Mautsysteme, wie sie etwa in Deutschland verwendet werden, nicht nur zur Berechnung der zurückgelegten (und zu zahlenden) Strecken verwendet werden können, sondern zugleich auch eine zeitgenaue Lokalisierung des Fahrzeugs möglich ist.

Auch die sogenannte Handyortung bedient sich des satellitengestützten »Global Positioning Systems« (GPS), präzisiert diese Lokalisierung zudem aber auch noch über das »Global System for Mobile Communication« (GMS) durch die Ermittlung der jeweiligen Sendemasten des Mobilfunkanbieters oder öffentlicher WLAN-Hotspots. Dabei kann die Position gebietsabhängig auf bis zu 100 Meter genau bestimmt werden. Die Vorteile der Handyortung zeigen sich vor allem in der Standortfeststellung nach Notrufen oder bei der Suche nach einem verlorenen oder gestohlenen Handy. Darüber hinaus gibt es vermehrt standortbezogene Dienste (zum Beispiel Twitter), die es dem Nutzer ermöglichen, die eigene Position der Netzgemeinde mitzuteilen oder ortsabhängige Informationen zur Verfügung stellen (zum Beispiel die nächstgelegene Apotheke). Allerdings birgt die Handyortung eine erhebliche Missbrauchsgefahr, wenn beispielsweise versucht wird, den Standort eines anderen ohne dessen Zustimmung zu ermitteln (Fremdortung), oder wenn das Handy einem anderen als dem in die Standortübermittlung eingewilligten Teilnehmer zur Nutzung überlassen wird und dieser nicht von der Ortung weiß. Mit der Novelle des TKG vom 3. März 2012 wurde dieser Missbrauchsgefahr Rechnung getragen. So setzt die Übermittlung von Standortdaten eines Mobilfunkendgerätes an einen anderen Teilnehmer oder Dritte, die nicht Anbieter des Dienstes mit Zusatznutzen sind, gemäß § 98 Abs. 1 Satz 4 TKG nun eine »ausdrücklich, gesondert und schriftlich« erteilte Einwilligung des Teilnehmers gegenüber dem Anbieter des Dienstes mit Zusatznutzen voraus. Zudem muss der Anbieter gemäß § 98 Abs. 1 Satz 2 TKG sowie § 98 Abs. 1 Satz 5 TKG den Nutzer bei jeder Standortfeststellung mit einer Textmitteilung an das Endgerät, dessen Standortdaten ermittelt wurden, informieren.

Unabhängig von der konkreten Handyortung lässt sich das sogenannte »Geotargeting« ganz allgemein als Gefährdung der Privatsphäre begreifen. Beim Geotargeting werden die IP-Adressen von Geräten ihrer geografischen Herkunft zugeordnet, worauf in einem nächsten Schritt das entsprechende Informationsangebot an den konkreten Standort angepasst wird. Unmittelbar bezieht sich das Geotargeting nur auf das jeweilige technische Gerät. Mittelbar berührt es die Privatsphäre allerdings in doppelter

Hinsicht: Zum einen ist in vielen, ja in den meisten Fällen jeder IP-Adresse auch eine bestimmte Person zuzuordnen, die mit nur wenig Zusatzwissen – etwa der Mail-Adresse oder einer Telefonnummer – auch individuell bestimmt werden kann. Zum anderen kann auch die standortbezogene Auswahl des Informationsangebots insofern als Beeinträchtigung der Privatsphäre verstanden werden, als eben dieser Standort erfasst und gespeichert wird.

Ungleich schwerer wiegen Eingriffe, die durch Geodaten- oder Panoramadienste wie Google Street View etc. vorgenommen werden. Neben Bildern von öffentlichen Straßen oder Plätzen sind regelmäßig auch Gebäude, Kraftfahrzeuge und Personen so detailliert zu sehen, dass das Fahrzeug ohne Weiteres einer bestimmten Person zugeordnet werden kann oder nachvollziehbar ist, wer die abgebildete Person ist und an welchem Ort sie sich zu welchem Zeitpunkt aufhielt. Auch die ebenso erstaunlich wie erschreckend präzisen Luftbildaufnahmen von Grundstücken und ihren Bebauungen sind geeignet, die Privatsphäre des Einzelnen zu beeinträchtigen. Zwar besteht die Möglichkeit, Widerspruch gegen die Veröffentlichung einzelner Bilder bei den Anbietern einzulegen, allerdings werden die betroffenen Personen vielfach nur durch Zufall und im Zweifel keine Kenntnis von den von ihnen aufgenommenen Bildern erlangen.

Als weiteres und keineswegs letztes Beispiel für aktuelle Bedrohungen der Privatsphäre aus dem Bereich der Mobilität seien sogenannte Dashcams genannt, also Kameras, die in Fahrzeugen befestigt sind, das Verkehrsgeschehen filmen und im Falle eines Unfalls Beweismaterial liefern sollen. Solche »Armaturenbrettkameras« sind in anderen Ländern längst üblich, in Deutschland sind sie im Vordringen. Datenschutzrechtlich werden sie überwiegend als anlasslose Videoüberwachung des Straßenverkehrs qualifiziert, welche die Privatsphäre anderer Verkehrsteilnehmer so erheblich beeinträchtigt, dass sie überwiegend für nicht zulässig erachtet wird.[8] Ihre Verbreitung und Nutzung hat dieses datenschutzrechtliche Verbot freilich nicht verhindert.

2.4 Gesundheitsbereich

Aus dem Gesundheitsbereich seien nur zwei Beispiele für aktuelle Gefährdungen der Privatsphäre genannt.

8 Vgl. ZD-Aktuell 2014, 03978 und ZD-Aktuell 2014, 03934.

Zum einen hat die elektronische Gesundheitskarte dazu geführt, dass bestimmte medizinische Daten auf der Gesundheitskarte selbst gespeichert sind. Der Regelung vorangegangen sind umfassende politische Diskussionen, die sich gerade auch auf den Datenschutz bezogen. Dementsprechend restriktiv sind die Regelungen über die zu speichernden medizinischen Daten ausgefallen und dementsprechend hoch sind die Anforderungen an die Datensicherheit. Gleichwohl hat die elektronische Gesundheitskarte ein Tor aufgestoßen, an dessen Ende erhebliche Eingriffe in die (gesundheitsbezogene) Privatsphäre des Einzelnen stehen können.

Schwerer als diese gesetzlich angeordnete Speicherung von bestimmten medizinischen Daten wiegt die Datenerfassung über sogenannte »Gesundheits-Apps«, die gerne auch euphemistisch als »Fitness-Apps« bezeichnet werden. Sie erfassen permanent bestimmte körperfunktionsbezogene Daten wie den Puls, den Blutdruck oder auch die Kalorienzufuhr bzw. den Kalorienverbrauch, zum Teil aber auch sehr viel mehr. Indem die erhobenen Daten zum Teil direkt in einer Cloud gespeichert werden, entziehen sie sich – jedenfalls theoretisch – der alleinigen Verfügung des Einzelnen. Dies wiegt umso schwerer, als die Daten in besonderer Weise der Privat-, ja gar der Intimsphäre des Einzelnen zuzurechnen sind. Die vermeintliche Freiwilligkeit der Datenerfassung steht diesem Befund nicht entgegen, zumal Versicherungen und andere Unternehmen verstärkt dazu übergehen, die regelmäßige Erfassung der Körperdaten zur Voraussetzung bestimmter Dienstleistungen zu machen oder doch jedenfalls als Anreiz mit besonders günstigen Konditionen zu entlohnen.

2.5 Arbeitsbereich

Aus dem Arbeitsbereich sei zunächst die Überwachung von Mitarbeitern am Arbeitsplatz als aktuelle Gefährdung der Privatsphäre benannt, die in einigen Wirtschaftsbereichen zur Praxis zählt. Dabei können unterschiedliche Ziele im Vordergrund stehen: die Arbeitssicherheit, die Sicherung von Rechten des geistigen Eigentums, die Verhinderung von Straftaten ebenso wie die schlichte Kontrolle der Arbeitstätigkeit. Die Möglichkeiten des Arbeitgebers reichen von der klassischen Videoüberwachung über die Überwachung des Mail- und Telefonverkehrs bis hin zur Aufzeichnung des gesamten Surfverhaltens der Mitarbeiter. Problematisch ist hierbei, dass nicht nur dienstliche Kommunikation vom Arbeitgeber »mitgelesen« wird, sondern unter Umständen auch private. Vor allem aber stellt die heimliche Videoüberwachung am Arbeitsplatz einen sehr starken Eingriff in das Allgemeine Persönlich-

keitsrecht dar,[9] der dementsprechend sehr hohen Anforderungen unterworfen ist.

2.6 Internet der Dinge

Eine Gefährdung der Privatsphäre stellt sicherlich auch das sogenannte »Internet der Dinge« dar. Der Begriff verdeutlich den Trend, dass der Zugang zum Internet nicht mehr allein dem PC vorbehalten ist, sondern auch zu anderen Funktionen bestimmte Geräte mit dem Internet vernetzt sind. Der intelligente Kühlschrank sei ebenso als ein solches Beispiel genannt wie der Rauchmelder, der nicht nur einen akustischen und optischen Alarm auslöst, sondern per Netz sogleich die Feuerwehr und den Krankenwagen alarmiert. Solche automatisierten »emergency calls«-Systeme finden sich mittlerweile auch in Autos, die in Abhängigkeit von genauen Bewegungs- bzw. Verzögerungsdaten einen Unfall melden und dabei Daten über den Standort abgeben, zudem aber auch die letzte Geschwindigkeit etc. speichern. Trotz der Konzeption als sogenanntes »schlafendes System« bestehen Bedenken hinsichtlich der Aufzeichnung des Fahrverhaltens der Fahrzeugnutzer. So könnte es in Zukunft noch schwerer werden, einen Unfall ohne Einbeziehung der Versicherung zu regeln, Gerichte könnten aus ganz anderen Gründen eine Auslesung der Geräte anordnen, um festzustellen, wann der Fahrzeughalter wo war, und darüber hinaus besteht auch, wie bei allen technischen Geräten, die Möglichkeit des unbefugten Zugriffs Dritter auf die Informationen, welche das Gerät sammelt.

Zurück vom Auto lockt das »smart house« oder heimeliger noch das »smart home« mit seiner intelligenten Energiebewirtschaftung, seiner intelligenten Beleuchtung und seinen intelligenten Sicherheits- und Überwachungssystemen. Als »intelligent« wird dabei schon bezeichnet, was miteinander vernetzt ist und über eine App gesteuert werden kann. Die Vernetzung ist dabei aber zugleich das Einfallstor für eine Gefährdung der Privatsphäre, denn mit dem Hacken des Zugangs etwa zu Überwachungskameras wird der Sinn und Zweck solcher Überwachungen in ihr Gegenteil verkehrt.

Auch der zunehmende Einsatz von RFID-Transpondern lässt sich zum Internet der Dinge rechnen. Als RFID (Radio Frequency Identification; Funkerkennung) bezeichnet man ein technisches System, mit dessen Hilfe

9 Vgl. hierzu etwa Brodtrück 2014.

Daten ohne Berührung oder Sichtkontakt gelesen und gespeichert werden können. Hierzu werden vor allem Textilien oder Ausweise (seit 2010 alle Personalausweise) mit einem RFID-Transponder ausgestattet, auf welchem wichtige Daten gespeichert sind. Die Datenübertragung zwischen Lesegerät und Transponder erfolgt per Funk. Aus datenschutzrechtlicher Sicht bergen die RFID-Transponder zahlreiche Risiken, weil der Verbraucher bzw. Nutzer häufig nicht weiß, dass in seinem Kleidungsstück ein Transponder verarbeitet ist. Trägt der Verbraucher dieses Kleidungsstück, so kann mithilfe des jeweils nächst gelegensten Lesegeräts der Standort und bei gezielter Platzierung mehrerer Lesegeräte gar ein Bewegungsprofil des Betroffenen erstellt werden. Außerdem könnten so Daten über das Kaufverhalten des Kunden gespeichert werden.

3. Strukturelle Gefährdungen

Jedes der genannten Beispiele birgt eine besondere Gefahr für die Privatsphäre, jede der skizzierten Gefahren bedarf insoweit einer besonderen Lösung. Die Rechtsordnung hat zum Teil durch Rückgriff auf geltende Rechtsgrundsätze, zum Teil durch Schaffung neuer Regeln auf konkrete Gefahren reagiert oder jedenfalls zu reagieren versucht. Ein wirkungsvoller Schutz der Privatsphäre gegenüber aktuellen und neuen Gefährdungen kann indes nur gelingen, wenn man sich jenseits der konkreten Gefahren der strukturellen Gefährdungen bewusst wird, die von der digital vernetzten Welt ausgehen. Insofern seien mit den Unsicherheiten hinsichtlich der Gefahrenquelle (3.1), den Besonderheiten der Gefährdungen (3.2) und der besonderen Intensität des drohenden Schadens (3.3) drei Aspekte näher beleuchtet.

3.1 Unsicherheit hinsichtlich der Gefahrenquelle

Zunächst einmal ist festzuhalten, dass zwar relativ rasch eine Einigung hinsichtlich (mancher) aktueller Gefährdungen der Privatsphäre erzielt werden mag, dass aber erhebliche Unsicherheit darüber besteht, wer diese Gefährdungen zu verantworten hat, wer deshalb umgekehrt auch zu ihrer Behebung heranzuziehen ist.

So ist nicht eindeutig auszumachen, ob die Gefährdungen primär von staatlichen Stellen oder in erster Linie von Privaten ausgehen. Zwar mag man bei einzelnen Beispielen eine konkrete Zuordnung vornehmen können. Eine Datenverarbeitung durch staatliche Stellen scheint jedenfalls auf den

ersten Blick selbstverständlich als eine dem Staat zuzurechnende Gefährdung der Privatsphäre zu qualifizieren sein, während etwa die Überwachung des Arbeitsplatzes (jedenfalls bei einem privaten Arbeitgeber) in den Verantwortungsbereich eines Privaten fallen wird. Doch bei genauerer Betrachtung knüpft diese Differenzierung nur an den letzten Schritt des Eingriffs in die Privatsphäre an und vernachlässigt den Gesamtkontext der Gefährdung. Eine Gesamtbetrachtung der aktuellen Gefährdung zeigt indes, dass eine Differenzierung zwischen staatlichen und privaten Akteuren, ja sogar eine Differenzierung zwischen Fremd- und Eigenverursachung der Gefährdung so einfach nicht ist.

3.1.1 Staatliche und private Akteure

Was insofern zunächst die Differenzierung zwischen vom Staat und von Privaten ausgehenden Gefährdungen betrifft, ist in Erinnerung zu rufen, dass sowohl im Kommunikationsbereich wie etwa auch im Zahlungsbereich, um zwei der oben genannten Beispiele herauszugreifen, die Daten zuvörderst von Privatpersonen erhoben und vorgehalten werden. Die meisten Informationen über jeden Internetnutzer haben nicht etwa die Staaten, sondern die Internet Service Provider oder Suchmaschinenbetreiber. Der Staat macht sich diese Daten zwar vielfältig zunutze, hält sie aber weder selbst vor noch generiert er sie gar. Es sind vielmehr die Nutzer selbst, die diese Daten erzeugen. Ähnlich – wenngleich auch mit zum Teil erheblichen Unterschieden – stellt sich dies im Zahlungsverkehr dar. Was Banken über einen wissen (können), sollte jedem Kunden an seinen Kontoauszügen unmittelbar deutlich werden. Sie enthalten mehr als bloße technische Zahlungsinformationen – sie lassen Rückschlüsse auf das Konsumverhalten, auf das Freizeitverhalten, auf das Sozialleben, auf Ernährungsgewohnheiten und auf die Gesundheit des Kunden ebenso wie etwaiger Familienmitglieder zu, um nur einige Beispiele zu benennen. Der Staat tritt erneut nur im Hintergrund auf, indem er sich alle oder bestimmte Informationen ständig oder anlassbezogen übermitteln lässt. Zugleich wirkt er im Vorfeld auf die Datenbasis ein, indem er die Banken und andere Zahlungsinstitute verpflichtet, auch jenseits ihrer eigenen Interessen bestimmte Daten zu erheben und zu speichern. Diese beiden Beispiele mögen verdeutlichen, dass die grundrechtlich begründete Differenzierung zwischen Gefährdungen durch staatliche Institutionen und solchen durch private Personen den tatsächlichen Begebenheiten nicht hinreichend Rechnung trägt.

Die größeren Gefahren für die Privatsphäre, so lässt sich auch ohne viel Fantasie erkennen, gehen in der digital vernetzten Welt von privaten Ak-

teuren aus. Dies hat mehrere Ursachen, von denen zwei genannt seien: Zum einen sind sowohl nach der Konzeption des Grundgesetzes als auch nach der Konzeption der Grundrechtecharta und letztlich wohl nach der Konzeption einer jeden freiheitlich verfassten Gemeinschaft nur die staatlichen Stellen unmittelbar grundrechtsgebunden, während Privatpersonen grundsätzlich von den grundrechtlich geschützten Freiheiten profitieren und insofern privatautonom agieren können. Zwar werden auch Privatpersonen durch den Grundsatz der mittelbaren Drittwirkung an die Grundrechte zurückgebunden, zudem erzeugen die Grundrechte auch staatliche Schutzpflichten, die den Staat verpflichten, der Privatautonomie Grenzen zu setzen. Insgesamt aber sehen sich die staatlichen Akteure in Bezug auf den Schutz der Privatsphäre im Ergebnis sehr viel strengeren Regeln ausgesetzt als private Akteure – zu Recht natürlich, wie nur kurz mit Blick auf das staatliche Gewaltmonopol hervorgehoben werden soll. Doch es gibt neben dieser grundrechtlich begründeten Differenzierung zwischen staatlichen und privaten Akteuren einen zweiten Grund für die besondere Gefährdung durch private Akteure: Das Misstrauen gegenüber Privaten scheint insgesamt geringer zu sein als gegenüber staatlichen Behörden. Anders ist es nicht erklärlich, dass jede obligatorische Informationsübermittlung an den Staat nicht nur rechtlich, sondern vor allem auch politisch bekämpft wird, während die freiwillige Informationsüberlassung an Private noch nicht einmal als Bedrohung wahrgenommen wird. Dieses fehlende Bewusstsein für das von Privaten ausgehende Gefahrpotenzial wiegt umso schlimmer, als zur Bekämpfung solcher Gefahren im Zweifel ein schlechterer Rechtsschutz zur Verfügung steht – nicht nur, aber vor allem, wenn die Gefahren gar nicht von in-, sondern von ausländischen Personen ausgehen.

3.1.2 Fremd- und Eigenverursachung der Gefahr

Nicht nur die Zuordnung der Gefahr zu staatlichen bzw. privaten Personen bereitet Schwierigkeiten. Auch die Frage, wer genau eine Gefahr zu verantworten hat, war und ist umstritten. Der gesellschaftliche Konsens und ihm nachfolgend das einfache Recht schwankt hier unsicher zwischen der Annahme einer Zustandsverantwortlichkeit und einer Verhaltensverantwortlichkeit, wie sich exemplarisch an der Frage der Providerhaftung darstellen ließe. Jenseits der Frage, wer für einen Schaden haftet, ist aber vorrangig zu klären, wer zur Vermeidung von Gefährdungen in die Pflicht genommen werden kann. Diesbezüglich wird sich auch der jeweils Betroffene nicht ganz ausnehmen können. Wer permanent selbst seine Privatsphäre perforiert, wird sich nicht wundern dürfen, wenn sie eines Tages vollstän-

dig löchrig ist. Juristisch betrachtet sind insofern Gedanken der Schadenminderungspflicht in die Gesamtbetrachtung einzubeziehen, ebenso wie etwa auch das Verbraucherschutzrecht, jüngst das Kapitalanlagerecht und im Übrigen auch das (Wirtschafts-)Strafrecht Grundsätze und konkrete Regeln zur Frage kennen, bis zu welchen Grenzen man für eigenes Verhalten haftet. Freilich soll es nicht erneut nur um die Haftung für einen eingetreten Schaden gehen, sondern primär die Frage aufgeworfen werden, wie prospektiv auf aktuelle Gefährdungen der Privatsphäre zu reagieren ist. Die Mitbeteiligung der Gefährdeten an der Setzung der Gefahr kann deshalb nur verdeutlichen, dass die Bekämpfung der Gefahr zugleich sehr viel früher (etwa durch umfassende Aufklärung) wie auch an anderen Instrumenten als der einseitigen Haftungszuweisung ansetzen muss (etwa an technischen Voraussetzungen eines effektiven Systemdatenschutzes). Insgesamt kann der Gefährdung der Privatsphäre in der digitalisiert vernetzten Welt nicht ohne ein gesundes Maß an Eigenverantwortung, an Datenvermeidung also, begegnet werden.

3.2 Besonderheiten der Gefährdungen

3.2.1 Fehlendes Bewusstsein

Eine erste Besonderheit der Gefährdung der Privatsphäre liegt in dem fehlenden Bewusstsein für eine Gefahr. Dies hat mehrere Ursachen:

In vielen Fällen ist dem Einzelnen weder die Datenerhebung noch eine Datenverarbeitung erkennbar. Zahlreiche der oben genannten Beispiele aus dem Kommunikationsbereich verdeutlichen, dass eine Datenerhebung und -verarbeitung »im Hintergrund«, letztlich also heimlich stattfindet. Dem Nutzer sind sie nicht erkennbar. Selbst wenn sie erkennbar sein sollten, wirkt jede einzelne Preisgabe eines Datums für sich genommen harmlos. Diese vermeintliche Harmlosigkeit jeder einzelnen Datenpreisgabe ist sicherlich der Hauptgrund für die besondere Gefährdung der Privatsphäre. Dass es, wie bereits zitiert, im Zeitalter der automatisierten Datenverarbeitung kein belangloses Datum mehr gibt, ist nicht derart in das Bewusstsein des durchschnittlichen Nutzers gelangt, dass er sein Verhalten danach ausrichten würde. In der Regel fehlt das Misstrauen. Dies verwundert insofern, als der allgemein bekannte Satz »Das Internet vergisst nicht!« doch einen deutlichen Appell-Charakter aufweist: Er versteht sich nicht nur als Befund, sondern jedenfalls auch als Warnung, insbesondere die sozialen Netzwerke und auch die Suchmaschinen nur mit Augenmaß zu nutzen. Er will das Be-

wusstsein dafür fördern, dass man sich im Internet ebenso wie in der realen Welt nicht unbeobachtet bewegt, sondern Spuren hinterlässt – Spuren, die im Unterschied zur realen Welt durch die Vielzahl der Nutzer und die Perpetuierung der Daten leichter auffindbar bzw. nachvollziehbar sind.[10] Deshalb schützt auch die Informationsflut, mit der sich mancher Nutzer trösten mag, allenfalls vor einer längerfristigen Aufmerksamkeit, nicht hingegen vor der grundsätzlichen Abruf- oder Rekonstruierbarkeit von Informationen.[11] Das in politischen Diskussionen über das Maß an Kontrolle so gern vorgebrachte Argument, der normale (will sagen: der rechtskonforme) Bürger habe doch nichts zu verbergen, soll zwar beruhigend wirken, verhallt aber letztlich doch in einem besonders bedrohlichen Echo: Zum Zeitpunkt der Datenverwendung können sich die politischen wie die rechtlichen Maßstäbe derart gewandelt haben, dass der Datenpreisgabe zu einem früheren Zeitpunkt niemals zugestimmt worden wäre.

3.2.2 Unvermeidbarkeit

Selbst bei vorhandenem Bewusstsein ist die Preisgabe von Daten, die in ihrer Summe zu einer Gefährdung der Privatsphäre führen können, häufig aber gar nicht vermeidbar – dies ist eine weitere Besonderheit der aktuellen Gefährdungen der Privatsphäre. Erneut zeigen die zahlreichen Beispiele aus dem Kommunikationsbereich, darüber hinaus aber auch aus dem Zahlungsbereich, dass der Einzelne kaum oder sogar überhaupt keine Ausweichmöglichkeiten hat. Diese Alternativlosigkeit zur Datenpreisgabe ergibt sich zum (sehr viel kleineren) Teil aus rechtlichen Vorgaben (etwa aus gesetzlichen Informationspflichten), zum (sehr viel größeren) Teil aus faktischen Begebenheiten (etwa der Nutzung von Social Media) und zum letzten Teil aus einer Kombination von beidem (etwa der Zustimmung zu Datenschutzgrundsätzen als Voraussetzung für die Nutzung von Social Media).

Namentlich die Nutzung von Social Media wie Facebook, Twitter, Instagram oder WhatsApp gehören jedenfalls für jüngere Generationen derart zur sozialen Realität, dass auf ihre Verwendung nicht verzichtet wird. Es besteht insoweit ein faktischer sozialer Druck zur Nutzung bestimmter Dienste und damit zugleich aber auch zur Bereitstellung zahlreicher Daten.

10 Einer jüngeren Studie zufolge vergisst das Internet entgegen der allgemeinen Überzeugung doch recht schnell, wie am Beispiel von Links in Tweets zu sechs Großereignissen der Jahre 2009 bis 2012 aufgezeigt wird: Mehr als ein Viertel der verlinkten Quellen war nicht mehr abrufbar. Vgl. hierzu Lischka 2012.

11 So schon Rossi 2013: 239ff.

Datensparsame Alternativen fehlen. Zwar gibt es einzelne Suchmaschinen, die damit werben, keine oder jedenfalls nur sehr viel weniger Daten über das Surfverhalten im Netz zu sammeln (zum Beispiel »ixquick«). Doch erstens sind sie schon mangels Masse nicht so erfolgreich wie der Marktführer Google und zweitens haben sich entsprechende Alternativen zu Social Media – soweit ersichtlich – nicht herausgebildet. Dies mag man, sollte man aber nicht als Marktversagen beurteilen. Vielmehr scheint es hier bislang keine Nachfrage nach einem daten- und persönlichkeitsschützenden Angebot in nennenswertem Umfang zu geben. Das kann sich ändern, muss es aber nicht. Derzeit befördert der preisorientierte Markt vielmehr eher noch die Nutzung des Internets als vermeintlich kostenlose Informations- und Kommunikationsplattform. Solange die Kosten der Datenpreisgabe nicht derart in den exakt bezifferten Geldpreis einbezogen werden, solange mit anderen Worten die entstehenden externen Datenkosten nicht in die Preisbestimmung internalisiert werden, solange werden sich keine Alternativen zu den genannten Nutzungsarten im Internet bilden. Im Gegenteil: Sowohl der Markt als auch der Staat befördern die Nutzung des Internets – der Markt letztlich über den Preis, der Staat durch den Ausbau der elektronischen Verwaltung bei gleichzeitigem Abbau der »analogen« Angebote. Dass noch vor zehn Jahren über den drohenden Digital Divide diskutiert wurde, scheint mit der Allgegenwärtigkeit und den Annehmlichkeiten des Internets längst vergessen.

3.2.3 Unwiderruflichkeit

Die dritte strukturelle Besonderheit der aktuellen Gefährdungen der Privatsphäre liegt in der Unwiderruflichkeit der einmal bereitgestellten Daten. Sobald Informationen die Sphäre des Privaten verlassen haben, verliert der Einzelne zwar nicht rechtlich seine Verfügungsbefugnis, doch regelmäßig aber faktisch seine Verfügungsmöglichkeit. Die diversen datenschutz-, zivil-, presse- und strafrechtlichen Instrumente zum Schutz der persönlichen Ehre mögen gerade in ihrem Zusammenspiel zwar nach Kräften versuchen, die Herrschaft des Einzelnen über seine Informationen zurückzugewinnen.[12] Vollständig garantieren können sie dies indes nicht.

Gleiches gilt auch für das sogenannte »Recht auf Vergessen«, das der EuGH jüngst im Vorgriff auf die Datenschutzgrundverordnung grundrechtlich untermauert, klugerweise aber nur in der Pressemitteilung als sol-

12 Vgl. Rossi 2013: 239ff.

ches und nicht im Urteil selbst benannt hat.[13] Denn ein Recht auf Vergessen kann es angesichts des technischen Phänomens Internet schon aus technischen Gründen nicht geben. Gelöscht werden die Informationen aus einem Speicher. Doch ob sie aus allen Speichern gelöscht werden, vermag niemand zu garantieren. Der besondere Charakter von Informationen, der darin liegt, dass sie nicht ausschließlich und ausschließend sind, sondern trotz Teilung vollständig beim Inhaber verbleiben, steht einer Kontrolle über alle Speicher entgegen. Insbesondere kann nicht ausgeschlossen werden, dass die Informationen auch bei ihrer physischen Vernichtung in den Köpfen vorhanden bleiben. Und eine Rekonstruierbarkeit von Informationen ist durch die zahlreichen Möglichkeiten einer Rekombination nicht vorhersehbar. Im Ergebnis muss man sich darüber bewusst sein, dass das Recht ein Löschen zwar bestimmen, das Vergessen aber nicht erzwingen kann.[14]

3.2.4 Bedeutungsänderung

Als vierte strukturelle Besonderheit der aktuellen Gefährdungen der Privatsphäre muss hervorgehoben werden, dass der Einzelne nicht nur der Selbstbestimmung seiner Daten verlustig zu gehen droht, sondern vor allem die Kontrolle über ihren semantischen Inhalt verliert. Die permanente Verknüpfbarkeit der Daten und ihre Anreicherung mit anderem, mit bereits vorhandenem ebenso wie mit später erworbenem Wissen, kann zu einem Bedeutungswandel der einmal – freiwillig oder unfreiwillig – preisgegebenen Daten führen. Im Zusammenhang mit der bereits erwähnten vermeintlichen Harmlosigkeit jeder einzelnen Dateipreisgabe wirkt diese Möglichkeit der Bedeutungsänderung deshalb als besonders gefährlich, weil sie nicht mehr zu beeinflussen ist. Eine auf Facebook zu einem bestimmten Zeitpunkt und in einem bestimmten, etwa privaten Kontext preisgegebene Information mag zu einem späteren Zeitpunkt in einem anderen, etwa geschäftlichen Kontext eine ganz andere Bedeutung erlangen als sie ursprünglich gehabt hat.

3.2.5 Unzureichender Rechtsschutz

Als letzte strukturelle Besonderheit der aktuellen Gefährdungen der Privatsphäre sei darauf hingewiesen, dass es in vielen Fällen nur einen unzurei-

13 EuGH, Urteil vom 13. Mai 2014, Rs. C-131/12 (Google Spain und Google) Slg. 2014, I-0000.
14 Vgl. Rossi 2013: 239ff.

chenden Rechtsschutz gegen Verletzungen der Privatsphäre gibt. Die besondere Gefährdung der Privatsphäre resultiert insofern daraus, dass weder eine Gefahr hinreichend effektiv abgewendet noch ein durch eine realisierte Gefahr hervorgerufener Schaden ausreichend ersetzt werden kann. Primärer Rechtsschutz kommt in der Regel zu spät, sekundärer Rechtsschutz beseitigt den Schaden in der Regel nicht. Der Satz: »Audacter calumniare, semper aliquid haeret« – »Wage es nur zu verleumden, irgendetwas bleibt immer hängen« bewahrheitet sich somit auch unter den Bedingungen des modernen Rechtsstaats. Unterlassungsansprüche mögen dem Betroffenen, wenn er sie denn gerichtlich durchsetzt, das Gefühl geben, im Recht gewesen zu sein. Doch darüber hinaus verhindern sie bestenfalls die Perpetuierung des Eingriffs in die Privatsphäre, heben diesen aber regelmäßig nicht auf. Und hinsichtlich etwaiger sekundärrechtlicher Ansprüche auf Schadenersatz lehrt die sehr nüchtern zu betrachtende Rechtsprechung der Oberlandesgerichte zum Presserecht, dass eine etwaige Schadenersatzpflicht für die Verlage weniger eine juristische Grenze als ein ökonomisches Kalkül ist.

3.3 Besondere Intensität des drohenden Schadens

Eine letzte Besonderheit betrifft den möglichen Schaden, der nämlich über die Beeinträchtigung und Verletzung der Privatsphäre deutlich hinausgehen kann. Er lässt sich in einem Satz dahingehend umschreiben, dass sich die Gefährdungen von der Rekonstruierbarkeit des Verhaltens bis zu einer Manipulierbarkeit der Gedanken erstrecken können und dem Menschen am Ende möglicherweise gar seine Subjektqualität nehmen.

3.3.1 Vollständigkeit der Datenerfassung

Ausgangspunkt dieser These ist die Erkenntnis, dass in der digitalisiert vernetzten Welt eine vollständige Datenerfassung jedes einzelnen Menschen möglich ist bzw. jedenfalls doch möglich sein kann. Insbesondere im Zusammenspiel der Kenntnisse über das Surf- und Suchverhalten im Internet, über das Kommunikationsverhalten oder gar die Kommunikation selbst, über den Zahlungsverkehrs sowie über das Bewegungsprofil einer Person lässt sich ohne Weiteres rekonstruieren, wer was wann gemacht hat. Zieht man zusätzlich noch die über eine Gesundheits-App freiwillig oder unfreiwillig generierten Daten hinzu, gewinnt man nicht nur ein nahezu vollständiges Bild vom Verhaltens des einzelnen Menschen, sondern auch von seinen grundlegenden physiologischen Funktionen. Das bloße Übereinanderlegen

der einzelnen durch den Betroffenen selbst generierten Informationsfolien – das Surf- und Suchverhalten im Internet, die Bewegungsdaten, die Gesundheitsdaten – gegebenenfalls kombiniert mit extern gewonnenen Informationen, Daten aus der privaten oder öffentlichen Überwachung des Raums etwa, Daten aus dem Zahlungsverkehr – lassen schon heute eine erschreckend genaue Rekonstruktion des menschlichen Verhaltens zu, die manche Science-Fiction in die Welt des Gestern verbannt. Freilich setzt diese Vollständigkeit eben auch einen Zugriff auf die unterschiedlichen Informationsfolien voraus. Doch erstens konzentriert sich das Wissen durch die permanente Ausweitung des Internets auf alle Lebensbereiche auf wenige große Unternehmen, die insoweit zu Recht im Verdacht stehen, als Datenkraken sämtliche Informationen aufzusaugen und zu speichern. Die Informationen, die etwa Google, Apple und Microsoft, Facebook und Amazon über ihre Nutzer haben, genügen für sich schon, um ein genaues Persönlichkeitsprofil zu erstellen. Noch schlimmer wird es, wenn auf alle diese Informationssammlungen zurückgegriffen werden kann – sei es durch private Vereinbarungen oder Unternehmensübernahmen, sei es durch hoheitlichen Zugriff auf diese Daten. Dann wird nicht nur der Kunde, dann wird auch der Bürger schnell gläsern.

3.3.2 Verhaltenskontrolle

Ob eine solche Rekonstruierbarkeit des Verhaltens auch schon in Echtzeit möglich ist mit der Folge, dass das menschliche Verhalten nicht nur nachvollzogen, sondern permanent beobachtet werden kann, ist schwer einzuschätzen. Vorstellbar ist dies freilich ohne Weiteres, in vielen Einzelbereichen wird dies sogar praktiziert, wissentlich und willentlich. Dass der Aufenthaltsort von Personen (genauer gesagt freilich von technischen Geräten) permanent und in Echtzeit ermittelbar ist, nutzen tatsächlich wohl weniger die Datenkraken oder der Staat, nutzen vielmehr besorgte Eltern in Bezug auf ihre Kinder, unsichere Eheleute in Bezug auf ihren Partner, Hundebesitzer in Bezug auf ihren Liebling, Autoverleiher und Speditionsunternehmen, zunehmend aber auch Private in Bezug auf ihre Wagen. Die Beispiele ließen sich endlos fortsetzen, täglich kämen neue hinzu. Manche erscheinen für sich genommen harmlos, sind zudem vermeintlich objekt- und weniger personenbezogen, einige erfolgen mit (erzwungenem) Einverständnis der Betroffenen, alle beschränken sich auf bestimmte Daten – in den Beispielen etwa den Aufenthaltsort.

Eine Verknüpfung der verschiedenen Daten hingegen, eine Kombination der Kenntnisse über den Aufenthaltsort, die Kommunikation, das Internet-

verhalten und den physiologischen Zustand des Betroffenen ließe nicht nur eine Rekonstruktion, sondern eine laufende Beobachtung eines einzelnen Menschen in Echtzeit zu. Dann ließe sich sein Verhalten nicht nur kontrollieren, sondern auch steuern.

3.3.3 Gedankenkontrolle

Noch schwerwiegender wird, dass die Datenerfassung längst nicht nur auf das äußere Verhalten bezogen ist, sondern auch eine Gedankenkontrolle ermöglicht. Namentlich das Surfverhalten im Internet erlaubt einen direkten Zugang zu den Gedanken des einzelnen Nutzers. Suchmaschinen finden nicht nur Antworten, sondern lesen primär erst einmal Fragen. Sie sind insofern als Lesegeräte der menschlichen Gedanken zu begreifen. Zwar mögen die Suchanfragen erstens nur einen Ausschnitt aus den hinter ihnen stehenden Gedanken bilden und zweitens von den Suchmaschinen nach wie vor primär syntaktisch und weniger semantisch verstanden werden, doch abgesehen davon, dass längst an einer semantischen Suchmaschinenoptimierung gearbeitet wird, ist doch schon mit dem rudimentären Wissen der Sucheinträge deutlich, dass nicht nur eine Verhaltens-, sondern auch eine Willenskontrolle möglich ist. Wer, um ein banales Beispiel aus dem Alltag zu wählen, zunächst nach Brückentagen, anschließend nach Urlaubszielen, sodann nach (einer bestimmten Art von) Unterkünften, nach Mietautos (womöglich mit Kindersitzen), zugleich nach touristischen Highlights in der Urlaubsregion sucht oder gar schon die Reservierung eines Museums oder eines Konzerts vornimmt, offenbart neben seinen konkreten Zielen auch seine Gedanken und die Art der Gedankenführung. Und dies ist nur ein vergleichsweises harmloses Beispiel, das aber genügen soll, um die Folgen dieser Gedankenkontrolle zu skizzieren, die Vorhersehbarkeit des menschlichen Verhaltens.

3.3.4 Verhaltenslenkung

Wie sehr sich die im Wege einer Verhaltensforschung gewonnenen Informationen zur Verhaltenslenkung nutzen lassen, hat Facebook mit seiner Nutzerforschung demonstriert. Nachdem einigen Nutzer primär positive, anderen primär negative Nachrichten angezeigt wurden, wurde deutlich, dass Facebook sich nicht nur als vermeintlich neutraler Verwalter der Informationen betätigt hat, sondern selbst steuernd in den Informationsfluss eingegriffen hat. Die Folgen mögen im konkreten Einzelfall banal gewesen sein – wer mehr positive Nachrichten erhalten hat, hat auch seinerseits pri-

mär positive Inhalte veröffentlicht, und umgekehrt. Doch auch diese banalen Folgen offenbaren das Potenzial zur Verhaltenslenkung.

3.3.5 Gedankenmanipulation

Einen noch stärkeren Eingriff in die Privatsphäre als diese – nicht ohne Weiteres erkennbare – Verhaltenslenkung bedeutet die Möglichkeit, neben dem Verhalten bereits die Gedanken zu manipulieren. Technisch ist es nur ein kleiner Schritt von der Beeinflussung des Tuns zur Beeinflussung des Denkens und des Wollens. Die personalisierte Werbung zeigt es längst, wenngleich sicherlich noch nicht mit dem angestrebten Erfolg. Doch die Algorithmen der Suchmaschinen bestimmen längst nicht nur die Suchergebnisse, sondern auch weitere Suchwünsche. Vor allem filtern sie aus, reduzieren die Möglichkeiten der Gedanken und beeinflussen so als wahrgenommene Außenwelt die wahrnehmende Innenwelt.

3.3.6 Der Mensch als Maschine

Ob diese Entwicklungen als aktuelle Gefährdungen der Privatsphäre wahrgenommen werden oder nicht, hängt sicherlich auch von der (rhetorischen) Frage ab, ob als Ziel solcher Manipulationen überhaupt noch der Mensch gesehen wird. Fast scheint es, als ob der Mensch nicht als selbstbestimmtes, sondern als programmierbares Wesen begriffen wird; als ob die umfassende Betrachtung und Erfassung des Menschen ihn weniger als Subjekt denn als Objekt begreift; als ob sich der Mensch weniger in Worten als vielmehr in Zahlen und Algorithmen beschreiben ließe. Wäre dem so, wäre nicht nur die Privatsphäre des Menschen, sondern wäre der Mensch als Mensch in Gefahr.

4. Herausforderungen an die rechtliche Bewältigung

Wie nun kann die Privatsphäre gegen solche Gefährdungen geschützt werden, wie vor allem kann sie in rechtlicher Hinsicht geschützt werden? Dazu seien einige grundsätzliche Überlegungen dargelegt, nicht ohne noch einmal in Erinnerung zu rufen, dass das deutsche Recht ein vielfältiges Instrumentarium zum Schutz der Privatsphäre enthält, das nicht vollständig infrage zu stellen ist.

4.1 Regulierungsbedarf und Novellierungsfähigkeit

Hervorzuheben ist zunächst, dass das Recht auf aktuelle – und das heißt letztlich sich ständig verändernde – Gefährdungen der Privatsphäre überhaupt reagieren können muss. Die Anpassungsfähigkeit des Rechts ist dabei weniger eine rechtstechnische Frage. Entscheidend ist vielmehr, dass, wie und auch wann ein Regulierungsbedarf überhaupt erkannt wird.

Diesbezüglich ist das Datenschutzrecht schon in der Vergangenheit ein gutes Beispiel für die innovative Kraft des Föderalismus. Entstanden aus einem – primär auf Datensicherheit, weniger auf den Schutz der hinter den Daten stehenden Personen zielenden – hessischen Landesgesetz, hat sich das Datenschutzrecht über andere Bundesländer bis hin auf Bundesebene ausgebreitet. Die beschworene innovative Kraft des Föderalismus liegt mithin in einer Vielzahl der Gesetzgeber und in der Möglichkeit einer pluralistischen politischen Meinungsbildung. Vor diesem Hintergrund ist die Tendenz zur Zentralisierung des Datenschutzes, wie sie in der geplanten europäischen Datenschutzgrundverordnung zum Ausdruck kommt, zu bedauern. (Freilich ist schon jetzt einzuräumen, dass auch faktisch ein einheitliches Datenschutzrecht mit möglichst hohem Schutzniveau erheblich zu einem effektiveren Schutz der Privatsphäre beitragen wird.)

Eine entscheidende Rolle beim Erkennen eines Regelungsbedarfs hat in der Vergangenheit auch das Bundesverfassungsgericht gespielt. Es hat in seinem Volkszählungsurteil nicht nur das Grundrecht auf informationelle Selbstbestimmung aus der Taufe gehoben, sondern es hat zugleich die wesentlichen Grundsätze des Datenschutzrechts postuliert, die nicht an Bedeutung verloren, sondern im Gegenteil an Bedeutung gewonnen haben. Auch die Schaffung eines Grundrechts auf Vertraulichkeit und Integrität informationstechnischer Systeme[15] ist Ausdruck eines erkannten Regulierungs- und Schutzbedarfs: Er schließt eine Schutzlücke in Bereichen, in denen weder das Kommunikationsgrundrecht noch das Recht auf informationelle Selbstbestimmung oder die Unverletzlichkeit der Wohnung einen ausreichenden Schutz gewähren.

15 BVerfGE 120, 274ff.

4.2 Adressaten

Eine zweite Überlegung betrifft die möglichen Adressaten eines Konzepts zum Schutz der Privatsphäre durch aktuelle Gefährdungen. Das überkommene, primär grundrechtlich abgeleitete Konfusionsargument, nach dem nur der Staat grundrechtlich gebändigt, Private hingegen grundrechtlich geschützt werden, lässt sich womöglich nicht durchgängig aufrechterhalten. In Bereichen, in denen die Datenmacht in erster Linie bei privaten Unternehmen liegt, genügen Schutzpflichten und mittelbare Drittwirkungen möglicherweise nicht mehr, um einen effektiven Schutz der Privatsphäre zu gewährleisten. Jedenfalls sollte die Durchsetzbarkeit von entsprechenden Betroffenenrechten gegenüber privaten Unternehmen (noch weiter) gestärkt werden.

4.3 Überwindung von Kompetenzgrenzen

Nicht nur die Differenzierung zwischen staatlichen und privaten Adressaten, auch Kompetenzgrenzen müssen überwunden werden. Das gilt weniger im Verhältnis zwischen der Europäischen Union und ihren Mitgliedstaaten, wo die intendierte Datenschutzgrundverordnung insoweit einen richtigen Weg einschlägt (wenngleich auch noch unklar ist, in welchen Bereichen den Mitgliedstaaten ein Regelungsspielraum verbleibt und inwieweit das vorgesehene »Kohärenzverfahren« zu einer einheitlichen Anwendung der Grundverordnung in den Mitgliedstaaten führen wird). Es gilt vielmehr mit Blick auf den Umstand, dass die großen datensammelnden, -verarbeitenden und auch -generierenden Unternehmen häufig im Ausland, meist außerhalb der Europäischen Union sitzen und deshalb jedenfalls nicht ohne Weiteres dem nationalen oder auch europäischen Datenschutzrecht unterfallen. Ob und unter welchen Voraussetzungen sie sich den nationalen bzw. europäischen Standards unterwerfen, wird letztlich in einem politischen Kompromiss zu beantworten sein, in den naturgemäß auch andere, bezogen auf den Schutz der Privatsphäre also sachfremde, Erwägungen hineinspielen.

Literaturverzeichnis

Albers, Marion (2013): Datenschutzrecht (§ 62), in: Dirk Ehlers / Michael Fehling / Hermann Pünder (Hg.), Besonderes Verwaltungsrecht, Bd. 2, Heidelberg, S. 1148– 1189.

Brodtrück, Lydia (2014): Entschädigung wegen Verletzung des allgemeinen Persönlichkeitsrechts bei Krankenkontrolle durch verdeckte Videoüberwachung, in: Arbeitsrecht Aktuell (ArbRAktuell) (4/2014), S. 114.

Harnisch, Stefanie / Pohlmann, Martin (2009): Strafprozessuale Maßnahmen bei Mobilfunkendgeräten. Die Befugnis zum Einsatz des sog. IMSI-Catchers, in: HRRS – Onlinezeitschrift für Höchstrichterliche Rechtsprechung zum Strafrecht 10 (5/2009), S. 202–217.

Lischka, Konrad (2012): Studie zur Web-Haltbarkeit: Das Netz vergisst schnell, in: Spiegel Online vom 22. September 2012 (online unter: www.spiegel.de/netzwelt/web/web-archiv-studie-zur-haltbarkeit-von-online-quellen-a-856936.html – letzter Zugriff: 19.02.2016).

Müller, Frank (2002): Kundenkarten und Bonussysteme als Instrumente der Kundenbindung und Informationsgewinnung, Hamburg.

Rossi, Matthias (2013): Informationsfluss zwischen Lethe und Mnemosyne. Zum Recht auf Vergessen, Recht auf Erinnern, in: Arnd Koch / Matthias Rossi (Hg.), Gerechtigkeitsfragen in Gesellschaft und Wirtschaft. 40 Jahre Juristische Fakultät Augsburg, Baden-Baden, S. 239–257.