verbraucherzentrale

Beiträge zur Verbraucherforschung
Band 1

Christian Bala und Klaus Müller (Hrsg.)

Der gläserne Verbraucher

Wird Datenschutz zum Verbraucherschutz?

Beiträge zur Verbraucherforschung

herausgeben von
Dr. Christian Bala
für das Kompetenzzentrum Verbraucherforschung NRW (KVF NRW) und
Klaus Müller
für die Verbraucherzentrale Nordrhein-Westfalen e. V.

ISSN 2197-943X

Band 1

Das KVF NRW ist ein Kooperationsprojekt der Verbraucherzentrale NRW e. V. mit dem Ministerium für Klimaschutz, Umwelt, Landwirtschaft, Natur- und Verbraucherschutz (MKULNV) und dem Ministerium für Innovation, Wissenschaft und Forschung (MIWF) des Landes Nordrhein-Westfalen.

Das 2011 gegründete KVF NRW hat die Aufgabe, die Verbraucherforschung zu unterstützen, um so eine Wissensbasis als Grundlage für effizientes verbraucher- und wirtschaftspolitisches Handeln zu schaffen. Mit den „Beiträgen zur Verbraucherforschung" dokumentiert das KVF NRW seine Workshops, die Wissenschaftlerinnen und Wissenschaftlern verschiedener Fachrichtungen die Gelegenheit bieten, sich interdisziplinär über verbraucherrelevante Fragen auszutauschen. Diese halbjährlichen Tagungen sollen die Diskussion zwischen Wissenschaft, Politik und Verbraucherorganisationen anregen.

Die in diesem Band versammelten Beiträge geben die Meinung und die wissenschaftlichen Erkenntnisse der Autorinnen und Autoren wieder und müssen nicht mit den Meinungen und Positionen des KVF NRW, der Verbraucherzentrale NRW e. V., des MKULNV und des MIWF übereinstimmen.

Ministerium für Innovation, Wissenschaft und Forschung des Landes Nordrhein-Westfalen
Ministerium für Klimaschutz, Umwelt, Landwirtschaft, Natur- und Verbraucherschutz des Landes Nordrhein-Westfalen
verbraucherzentrale Nordrhein-Westfalen

Christian Bala und Klaus Müller (Hrsg.)

Der gläserne Verbraucher

Wird Datenschutz zum Verbraucherschutz?

Bibliografische Information der Deutschen Nationalbibliothek

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.dnb.de abrufbar.

1. Auflage, 2014

ISSN 2197-943X
ISBN Print 978-3-86336-901-9
ISBN E-Book (PDF) 978-3-86336-903-3

Printed in Germany

Inhalt

7 **Geleitwort**
Johannes Remmel

9 **Geleitwort**
Svenja Schulze

11 **Der gläserne Verbraucher: Konsum und Überwachung**
Christian Bala und Klaus Müller

41 **Die Privatsphäre des Verbrauchers – ein Luxusgut?**
Rainer Böhme und Sebastian Luhn

57 **Datenschutz und Cloud Computing aus Verbrauchersicht**
Georg Borges und Sascha Adler

83 **Smart Meter: Strom sparen – Daten verschwenden?**
Ulrich Greveler

93 **Der gläserne Patient – Chance oder Risiko?**
Britta Böckmann

105 **Bitcoin – Anonym Einkaufen im Internet?**
Artus Krohn-Grimberghe und Christoph Sorge

115 **Zusammenfassende Thesen**
Kompetenzzentrum Verbraucherforschung NRW

124 **Autorenverzeichnis**
126 **Impressum**

Geleitwort

Foto: MKULNV

Johannes Remmel

Minister für Klimaschutz, Umwelt, Landwirtschaft, Natur- und Verbraucherschutz des Landes Nordrhein-Westfalen

Wir wissen, dass Verbraucherinnen und Verbraucher jeden Tag neue Datenspuren im Netz hinterlassen. Besonders die sozialen Netzwerke sind zu einer wahren Fundgrube über persönliche Informationen geworden, die auch von Geheimdiensten abgeschöpft werden können, wie der PRISM-Skandal gezeigt hat.

Zugleich entstehen technologische Entwicklungen, die sinnvolle Neuerungen für Verbraucherinnen und Verbraucher bringen, wie etwa Smart Meter, welche den Energieverbrauch transparent machen und Einsparmöglichkeiten in intelligenten Stromnetzen eröffnen. Damit verbunden sind aber auch Herausforderungen für den Daten- und Verbraucherdatenschutz.

Diese Technologien sind für die überwiegende Mehrheit der Verbraucherinnen und Verbraucher tatsächlich „Neuland“, das wissenschaftlich und nicht skandalgetrieben erkundet werden sollte. Das ist die Aufgabe der Verbraucherforschung, die die Landesregierung und die Verbraucherzentrale Nordrhein-Westfalen durch die Gründung des Kompetenzzentrums Verbraucherforschung NRW (KVF NRW) stärken möchte.

Der vorliegende erste Band der vom KVF NRW herausgegebenen „Beiträge zur Verbraucherforschung“, die auf den halbjährlichen Workshops zur Verbraucherforschung basieren, beschäftigt sich mit dem „gläsernen Verbraucher“, ohne dabei in Alarmismus zu verfallen. Wissenschaftlerinnen und Wissenschaftler verschiedener Fachrichtungen stellen die Chancen und Risiken dar, die von Smart Metern, der Telemedizin, dem Cloud Computing oder der vir-

tuellen Währung Bitcoin ausgehen. Damit wurden Zukunftsthemen mit einer hohen Relevanz für Verbraucherinnen und Verbraucher aufgegriffen.

Zielgruppe der Veröffentlichung sind nicht nur die verbraucherpolitischen Akteurinnen und Akteure, denen Handlungsempfehlungen geboten werden, und die wissenschaftliche Gemeinschaft, sondern sie ist auch für die Verbraucherinnen und Verbraucher von Nutzen. Das wichtige Ziel des Wissenstransfers, das die Projektpartnerinnen und -partner mit der Gründung des KVF NRW verbanden, wird so auf vorbildliche Weise verwirklicht.

Den „Beiträgen zur Verbraucherforschung“ wünsche ich daher zahlreiche Leserinnen und Leser.

Geleitwort

Foto: MIWF / Dietmar Wadewitz

Svenja Schulze

Ministerin für Innovation, Wissenschaft und Forschung des Landes Nordrhein-Westfalen

Das Recht, über seine persönlichen Daten selbst zu bestimmen, gehört zur freien Entfaltung der Persönlichkeit. Das stellte das Bundesverfassungsgericht in seinem Volkszählungsurteil von 1983 fest. Damals fand EDV noch auf teuren Großrechnern statt. Eine weltweite Vernetzung erschien erst als vage Möglichkeit.

Seither ist viel geschehen. Dazu haben Wissenschaften und technische Innovationen wesentlich beigetragen: Riesige Datenmengen können gespeichert und verarbeitet werden, moderne IT findet intelligente und effiziente Lösungen für Probleme in der Energieversorgung oder der Medizin. Überall kann man online sein.

Dieser Fortschritt hat einen Preis: Jede Bewegung im Internet hinterlässt Spuren, die ausgewertet werden können. Soziale Netzwerke haben die Kommunikationsgewohnheiten der Menschen verändert. Und Effizienzinteressen können mit der Privatsphäre des Einzelnen in Konflikt geraten.

Der vorliegende Sammelband enthält Beiträge aus der Rechtswissenschaft, der Wirtschaftswissenschaft und der Informatik. Differenziert wird aufgezeigt, wie das Recht auf informationelle Selbstbestimmung der Verbraucherinnen und Verbraucher durch technologische Innovationen herausgefordert wird, wie es verteidigt werden kann und wie eine verantwortungsbewusste Wissenschaft mit diesem Problem umgeht.

Der erste Band der „Beiträge zur Verbraucherforschung“, die durch das Kompetenzzentrum Verbraucherforschung NRW (KVF NRW) herausgegeben werden, stellt bemerkenswerte Fragen zu den Zukunftstechnologien. Diese Fragen spielen in der allgemeinen Debatte um Facebook, Google & Co. bisher eine untergeordnete Rolle, sind aber von hoher gesellschaftlicher Relevanz, da diese Technologien unser Alltagsleben prägen – auch in Zukunft.

Mit dieser Veröffentlichung vermittelt das KVF NRW eine interdisziplinäre Perspektive: Forscherinnen und Forscher werden unter dem Dach der Verbraucherforschung zusammengebracht. Deshalb hoffe ich, dass diesem gelungenen ersten Band weitere folgen. Ich wünsche der Schriftenreihe eine positive Resonanz in der Fachwelt und bei Verbraucherinnen und Verbrauchern.

Der gläserne Verbraucher: Konsum und Überwachung

Sozialwissenschaftliche Vorbemerkungen

Christian Bala und Klaus Müller

Abstract

Technischer und gesellschaftlicher Wandel haben den Charakter der Überwachung verändert. Tagtäglich werden Daten von Verbraucherinnen und Verbrauchern im Internet erhoben oder von ihnen selbst preisgegeben. Dabei sind sowohl die weitere Verwendung der Daten als auch die möglichen Konsequenzen von umfassenden Profilen für die Betroffenen unklar. Der Beitrag beschreibt den veränderten Charakter der Überwachung, die Bedeutung des „Internets der Dinge" und die möglichen Auswirkungen im Bereich des Konsums. Berücksichtigt werden dabei auch Folgen des NSA-Skandals.

1 Datenkraken – gestern und heute

Auch wenn es die „Datenkrake“ noch nicht in die einschlägigen zoologischen Bestimmungsbücher geschafft hat, über ein Hauptmerkmal der Spezies *Octopus speculari* ist schnell Einigkeit erzielt: Sie muss ihren unersättlichen Hunger durch Überwachung stillen. Ob Geheimdienste oder zivile Behörden, ob Suchmaschinengiganten, Auskunfteien oder der Einzelhandel, sie alle brauchen Daten, um aus ihnen Informationen zu gewinnen, die helfen ihre Arbeit zu optimieren, damit sie effizienter und zielgenauer handeln können.

Im Englischen meint *surveillance* nicht nur „Überwachung“, sondern steht auch für „Kontrolle“ und „Beobachtung“, und umschreibt das Verhalten der „Datenkraken“ somit recht genau: „Nicht die Information bringt die Überwachung hervor, sondern die Überwachung die Information.“ (Knocke 2013, 9) Aus der Masse der verfügbaren Daten, die für sich genommen harmlos erscheinen und die aus verschiedenen Überwachungsquellen stammen, können wahlweise ökonomisch wertvolle oder sicherheitsrelevante Informationen gewonnen werden.

Seit dem Ende des Zweiten Weltkriegs galt „Big Brother“ als Inbegriff der Überwachung. Orwell beschrieb in seiner Dystopie „1984“ einen totalitären Staat, in dem es keine Privatsphäre mehr gibt: „Man konnte natürlich nie wissen, ob man im Augenblick gerade beobachtet wurde oder nicht.“ (Orwell 2011, 9) Der fiktive Staat Ozeanien ist eine gesamtgesellschaftliche Verwirklichung von Benthams Panopticon (siehe Semple 1993), einem Gefängnis, in dem die Gefangenen nie wissen, ob sie gerade überwacht werden, und sich deshalb diszipliniert verhalten. Regelkonformität wird in Ozeanien erzwungen, der Präventionsstaat sanktioniert abweichendes Verhalten schon im Vorfeld. Dieses Szenario inspirierte zahlreiche literarische und wissenschaftliche Werke[1] und ist als Metapher präsent.

1 Panoptische Dystopien finden sich u. a. in der „Traveler“-Trilogie (Twelve Hawks 2012), in der Graphic Novel „V“ (Moore und Lloyd 2003) oder in dem Jugendroman „Little Brother“ (Doctorov 2011). Ein Präventionsstaat wird auch in Philip K. Dicks Kurzgeschichte „Minority Report“ (in Dick 2002) beschrieben. Michel Foucault (1994) hat mit „Überwachen und Strafen“ eine Gesellschaftstheorie des Panopticons vorgelegt.

Tatsächlich zeigen die totalitären Erfahrungen des 20. Jahrhunderts nicht allein die Gefahren eines Überwachungsstaates, sondern auch, dass einmal erhobene Daten, werden sie aus ihrem ursprünglichen Kontext genommen, beliebig für andere Zwecke missbraucht werden können: Mithilfe der Melderegister wurde im Deutschen Reich die Ausgrenzung und Vernichtung der deutschen Jüdinnen und Juden organisiert (Aly und Roth 2005). In den Niederlanden konnten die Nazis auf der Grundlage von Volkszählungen und Bevölkerungsregistern, die vor dem Überfall erstellt worden waren, die Jüdinnen und Juden recht einfach identifizieren und deportieren, im benachbarten Belgien konnte die Besatzungsmacht nicht auf solche Daten zurückgreifen, da dort die Religionszugehörigkeit nicht amtlich erhoben wurde (siehe die Beiträge in Hürter und Zarusky 2008).

Insofern war es konsequent, den Datenschutz als eine Barriere zwischen den Bürgerinnen und Bürgern und dem „Datenhunger" des Staates zu verstehen, auch wenn die ersten deutschen Schutzgesetze, so in Hessen (1970) oder später das Bundesdatenschutzgesetz (1977), Regelungen für den Datenschutz in Unternehmen enthielten. Im Bewusstsein der Öffentlichkeit blieben jedoch die staatlichen Datensammlungen, etwa durch die Rasterfahndung der 1970er-Jahre oder die geplante Volkszählung von 1983, die durch das Bundesverfassungsgericht gestoppt wurde. Das Volkszählungsurteil (BVerfG 1983) war wegweisend, denn damit erhielt das „Recht auf informationelle Selbstbestimmung", obwohl nicht im Grundgesetz verankert, den Charakter eines Grundrechts (siehe Witt 2012, 50–53; siehe auch Lewinski 2012). Eine vier Jahre später durchgeführte Volkszählung stieß auf breiten Widerstand bei Parteien, Gewerkschaften und sogar in einzelnen Kommunen (Bergmann 2009).

Wie anders stellte sich die Situation im Jahr 2012 dar, als das Kompetenzzentrum Verbraucherforschung NRW (KVF NRW) am 19. November den Workshop „Der gläserne Verbraucher" im Düsseldorfer Heinrich-Heine-Institut veranstaltete. Als Datenkraken galten nun Google, Facebook & Co (siehe exemplarisch Adamek 2011 oder Dworschak 2011). Während der Zensus 2011 (Auer-Reinsdorff, Jakobs und Lepperhoff 2011, 37–38) geräuschlos vonstatten ging, empörte sich Deutschland 2008 über Google Street View (Forgó, Krügel und Müllenbach 2010). Der Fokus verschob sich vom Staat auf soziale Netzwerke und Tracking-Technologien im Internet. Das Vertrauen der Bundesbürgerinnen und -bürger in den Staat und die Behörden hinsichtlich des verantwortungs-

vollen Umgangs mit Daten, ist laut einer Umfrage des Branchenverbandes BITKOM (2011a, 26), hoch, obwohl kritische Autorinnen und Autoren stets auf den Zusammenhang von privatwirtschaftlichen und staatlichen Datensammlungen hinwiesen (bspw. Auer-Reinsdorff, Jakobs und Lepperhoff 2011 oder Kurz und Rieger 2011).

Zugleich offenbaren Teile der Öffentlichkeit bisweilen einen recht sorglosen Umgang mit personenbezogenen Daten gegenüber der Privatwirtschaft. Dies gilt aber nicht für alle Altersgruppen gleichermaßen. So nutzt „die Mehrheit der zwölf- bis 24-jährigen" in sozialen Netzwerken, das belegt eine Studie der Landesanstalt für Medien NRW, „restriktive Datenschutzeinstellungen (48 Prozent ‚Wenigoffenbarer' und 39 Prozent ‚Privatsphäre-Manager')" (Landesanstalt für Medien NRW 2012). Aber „jeder siebte (14 Prozent ‚Vieloffenbarer') verwendet recht offene Einstellungen, hat einen hohen Anteil an unbekannten Kontakten und zeigt zugleich ein aktives Kommunikationsverhalten im Netz." (Landesanstalt für Medien NRW 2012; siehe ausführlich Schenk, Niemann, Reinmann und Roßnagel 2012) Jüngere Nutzerinnen und Nutzer scheinen sich also stärker mit den Privatsphäreeinstellungen, in ihrem sozialen Netzwerk zu beschäftigen und sie auch aktiv anzupassen. Ältere User (ab fünfzig Jahren) gehen hingegen „leichtfertiger mit diesen Einstellungen um. Gut jeder fünfte (22 Prozent) unter ihnen hat sich noch nie mit den Privatsphäreeinstellungen des genutzten Netzwerks auseinandergesetzt" (BITKOM 2011b, 24).

Gerade der berühmte „Otto Normalverbraucher" legt nicht immer eine gesunde Skepsis an den Tag und erweist sich somit als verletzlich: Im Januar 2011 tarnte sich ein Team der Computer-Sendung „c't TV" als Vertreterinnen und Vertreter eines Gesundheitsinstituts. Mit dem Versprechen, Rückzahlungen von ihrer Krankenkasse zu erhalten, gaben die Passantinnen und Passanten nicht nur Informationen über ihre gesundheitliche Vorgeschichte und Lebensweise preis, sondern lieferten freiwillig Namen und Adressen, Bankdaten, inklusive EC-Kartennummer mit PIN sowie Haar- und Blutproben (siehe c't TV 2011). Nichtsdestotrotz findet die überwiegende Mehrheit der Deutschen Datenschutz wichtig, wünscht sich aber, dass andere aktiv werden. 81 Prozent finden, dass Unternehmen mehr für den Datenschutz tun sollten, 55 Prozent wünschen, dass der Staat ein entsprechendes Qualitätssiegel herausgibt oder strengere Regeln erlässt (72 Prozent) (BITKOM 2011a, 23–25).

Im Sommer 2013 wandelte sich die Sicht auf die „Datenkraken“ erneut, als die Informationen des Whistleblowers Edward Snowden die weitreichenden Programme der National Security Agency (NSA) und des britischen Government Communications Headquarters (GCHQ) enthüllten. Regierungen, die massenhafte und verdachtsunabhängige Bespitzelung von Bürgerinnen und Bürger mit dem Schutz vor der Gefahr des Terrorismus rechtfertigten, ließen die Dystopien eines Überwachungsstaates neu aufleben, „1984“ wurde wieder zu einen Bestseller (sha 2013).

In Deutschland versuchten Regierungspolitiker den Skandal zu relativieren; so wurde im Einklang mit Barack Obama betont, dass diese Maßnahmen zum Schutz vor Terrorismus notwendig seien. Die wahre Bedrohung, so Innenminister Hans-Peter Friedrich (CSU), gehe von den Internetgiganten aus: „Die Freiheit von Menschen wird durch unkontrollierte Machtkonzentration bedroht. Wer etwa wie Internetkonzerne aufgrund der im Netz gesammelten Daten ein exaktes Persönlichkeitsbild von mir zeichnen kann, ohne ausreichend an Gesetze gebunden zu sein, hat ein viel größeres Machtpotential als jeder demokratisch kontrollierte Geheimdienst.“ Und weiter: Was „will die NSA denn mit Ihren Daten? Es ist völlig irrelevant für den Auftrag des Nachrichtendienstes, was irgendjemand zu einem anderen am Telefon sagt, es sei denn, er will Bomben bauen und damit den Hamburger Hauptbahnhof in die Luft jagen. Denjenigen zu finden ist der Auftrag der Nachrichtendienste und sonst nichts. Wenn aber ein Privatunternehmen mehr über mich weiß als ich selbst, macht mich das nervös.“ (Hans-Peter Friedrich im Gespräch mit Schindler, Doerry und Gude 2013, 34)[2] Diese Argumentation spielt das Recht auf informationelle Selbstbestimmung gegen das vermeintliche „Supergrundrecht“[3] Sicherheit aus (siehe Solove 2011) und sie zieht eine Grenze zwischen „guten“ und „bösen“ Datensammlern, der staatlichen Überwachung einerseits und der Datenerhebung durch Unternehmen mit dem Ziel des Gewinnstrebens andererseits.

2 Ähnlich äußerte sich Bundesinnenminister Hans-Peter Friedrich (im Gespräch mit Jansen und Trebar 2013) im September im „Tagesspiegel“: „Denn die wirkliche Bedrohung unserer Freiheit geht nicht vom amerikanischen, britischen oder französischen Geheimdienst aus. Es sind vielmehr die großen weltweit operierenden Internetkonzerne, die unsere Daten massenhaft auswerten, analysieren und verkaufen. Das ist die Gefahr für unsere Freiheit und unsere Bürgerrechte.“

3 Siehe dazu auch die Stellungnahme der Gesellschaft für Informatik (2013, 18–19).

Es gibt gute Gründe, an diesem einfachen, schwarz-weiß-zeichnenden Weltbild zu zweifeln: So hat sich der Charakter der Überwachung in der „flüchtigen Moderne“ (Bauman 2003; 2008) verändert (Abschnitt 2). Dieser soziale Wandel wird durch die „Informatisierung des Alltags“ (Mattern 2007b) beschleunigt (Abschnitt 3), dieser Trend hat den Workshop, der diesem Sammelband zugrunde liegt, maßgeblich motiviert. Diese technischen und gesellschaftlichen Veränderungen machen es möglich, den Konsum umfassend zu kontrollieren (Abschnitt 4) und führen so zur sozialen Klassifikation von Verbrauchergruppen (Abschnitt 5). Schließlich, das ist eine Erkenntnis aus dem NSA-Skandal, fließen privatwirtschaftliche und staatliche Überwachung ineinander und ergänzen sich (Abschnitt 6).

2 „Flüchtige Überwachung“

Im Januar 1999, also 14 Jahre vor PRISM, sagte der ehemaligen CEO von Sun Microsystems Scott McNealy (zit. nach Sprenger 1999): „You have zero privacy anyway. Get over it.“ Google war zu diesem Zeitpunkt ein junges Unternehmen, das noch nicht damit begonnen hatte, Werbung mit Suchanfragen zu koppeln, und Mark Zuckerberg war gerade einmal 14 Jahre alt, doch schon bezeichnete McNealy Diskussionen um den Verbraucherdatenschutz als „red herring“ (zit. nach Sprenger 1999), auf gut Deutsch als Ablenkungsmanöver, als Nebelkerze. Ob die Bemerkung zynisch oder einfach nur ehrlich gemeint war, sei dahingestellt, sie zeigte aber, dass die Privatsphäre der Nutzerinnen und Nutzer von Software und Onlinediensten von nun an zur Debatte stand.

Es war auch der Zeitpunkt, als sich erstmals Stimmen meldeten, die prognostizierten, dass die Technologie der Vernetzung zu einer „transparenten Gesellschaft“ führen werde. Der Science-Fiction-Autor David Brin (1998) verfasste den Entwurf einer offenen und freien Gesellschaft, die auf reziproker Transparenz fußt. Legen die Menschen ihre Geheimnisse offen, so würde dies langfristig gesellschaftliche Toleranz fördern. Umgekehrt verhindere eine Transpa-

renz Machtkonzentration und -missbrauch, so Brin (1998). Diese Sicht wird heute von der Post-Privacy-Bewegung (u. a. Heller 2011) vertreten.

Doch während es mittlerweile zur Gewohnheit von Millionen von Menschen gehört, Googles Dienste zu nutzen und dafür mit einem Einblick in ihre Privatsphäre zu zahlen oder ihre Erlebnisse auf Facebook zu teilen, wissen diese Nutzerinnen und Nutzer wenig darüber, welche Daten gespeichert sind und wozu sie genutzt werden. Jeder Mensch kann „in allen Bereichen des Alltagslebens pausenlos überprüft, beobachtet, getestet, bewertet, beurteilt und in Kategorien eingeordnet werden [...]. Und zwar völlig einseitig." (Bauman und Lyon 2013, 24) Die Transparenz ist nicht reziprok, es existiert ein Machtgefälle, und dies prägt den Charakter der Überwachung.

Der Soziologe Zygmunt Bauman spricht im Rahmen seiner Theorie von der „flüchtigen" oder „liquiden Moderne" (2003; 2008) von einer post-panoptischen, flüchtigen Überwachung (siehe Bauman 2003, 17-18). Anders als im Panopticon ziele die Überwachung nicht auf Disziplinierung des Einzelnen (vgl. Foucault 1994), sondern auf Sicherheit und Klassifizierung (siehe Bauman und Lyon 2013, vgl. auch die Theoriediskussion in Lyon 2006).

Gerade im Bereich des Konsums „wird Überwachung zunehmend ‚weicher'. Sie löst sich aus ihren alten Verankerungen, da sich für einen bestimmten Zweck erhobene Daten immer leichter anderen Zwecken zuführen lassen. Dadurch breitet sich Überwachung in unvorstellbarer Weise aus, wobei sie an der Verflüchtigung alles Festen teilnimmt und zugleich zu ihr beiträgt. Sie schwappt geradezu über, wenn die sie bislang einfassenden Rahmenrichtlinien unter dem Druck der Forderungen nach mehr ‚Sicherheit' und den Marketingbemühungen von Technologiefirmen nachgeben." (Bauman und Lyon 2013, 13) Indem Datenspuren jederzeit nachzuverfolgen sind, „operiert die Überwachung sowohl über räumliche als auch zeitliche Distanzen und strömt über nationalstaatliche Grenzen hinweg" (Baumann und Lyon 2013, 16). Flüchtige Überwachung ist an keinen spezifischen Zweck gebunden, einmal erhobene Daten können ihrem Kontext entnommen werden, neue Informationen entstehen, Big-Data-Analysen (Mayer-Schönberger und Cuiker 2013) bieten der Wirtschaft und dem Staat vielfältige Möglichkeiten, die Datenbestände zu nutzen.

An dieser flüchtigen Überwachung haben die Nutzerinnen und Nutzer ihren Anteil, Bauman spricht von einer „Do-it-your-self-Sklaverei“ (Bauman und Lyon 2013, 36), indem sie sich in sozialen Netzwerken selbst enthüllen und im Sinne der Aufmerksamkeitsökonomie (Franck 2010) ihren sozialen Status an der Anzahl ihrer Facebook-Freunde messen (siehe Wiedemann 2011). Einer Studie zufolge soll ein positives Feedback auf Facebook das Belohnungssystem im Hirn aktivieren (siehe anw 2013b). Der Wunsch nach sozialer Anerkennung ist sicher keine neue Erscheinung, doch hier geht er mit dem sozialen Druck sich preiszugeben einher (siehe Bauman 2009, 9).

Durch ihren Content machen die User die Plattformen, auf denen sie sich um die Aufmerksamkeit ihrer Peers bemühen, attraktiv, sie generieren Inhalte und liefern zugleich wertvolle Informationen, welche die Plattformbetreiber monetarisieren können (siehe Frank, Softwareentwickler aus Hamburg 2011; Sandoval 2012, 150). Die Daten und auch die Nutzerinnen und Nutzer selbst werden zu einer Ware, indem sie sich als nützlich erweisen, „als Produkte, die ‚aufmerksamkeitsstark‘ sind, die *Nachfrage* wecken und Kunden anziehen“ (Bauman und Lyon 2013, 47, Hervorhebungen im Original; siehe auch Baumann 2009, 12-14; Baumann und Lyon 2013, 42-50).

Doch soziale Netzwerke oder andere Online-Dienstleister bilden nur einen Teil der umfassenden, flüchtigen Überwachung der Verbraucherinnen und Verbraucher.

3 Informatisierung des Alltags

Die Aufmerksamkeit der Öffentlichkeit wurde lange durch die Privatsphäre in sozialen Netzwerken und das Tracking der Online-Werbewirtschaft gebunden, weil dies die sichtbare Seite des Verbraucherdatenschutzes ist. Das KVF NRW wollte mit dem Workshop „Der gläserne Verbraucher“ einen weniger beachteten, jedoch tiefgreifenden und zukunftsweisenden Trend ins Blickfeld der interdisziplinären Verbraucherforschung und der verbraucherpolitischen Ak-

teure rücken, die Informatisierung des Alltags (siehe dazu Becker 2011; Mattern 2007b; Stampfl 2013). Zudem war es das Ziel, Raum für alternative theoretische Ansätze zur Privatsphäre der Verbraucherinnen und Verbraucher zu geben. Der vorliegende erste Band der „Beiträge zur Verbraucherforschung" versammelt die Vorträge des 3. NRW-Workshops Verbraucherforschung[4], die um Handlungsempfehlungen an die Adresse der verbraucherpolitischen Akteure ergänzt wurden:

- Welchen Wert hat die Privatsphäre für den Einzelnen und welchen Wert hat Privacy für die Gesellschaft? Mit dieser Frage beschäftigen sich *Rainer Böhme* und *Sebastian Luhn* in ihrem Beitrag und plädieren für eine ökonomische Ergänzung der vornehmlich juristischen oder technischen Datenschutzperspektiven.
- Ein besonders sensibles Beispiel ist das Cloud Computing, dessen Herausforderungen für die Verbraucherinnen und Verbraucher von *Georg Borges* und *Sascha Adler* analysiert wird. Dabei wird deutlich, dass Nutzerinnen und Nutzer nicht nur selbst Betroffene sind, sondern dass Verbraucherinnen und Verbraucher auch personenbezogene Daten Dritter verarbeiten und deshalb in diesem Bereich dem Datenschutz verpflichtet sind.
- Smarte Netze (Smart Grid) gelten als unerlässlich, um zukünftig einen effizienten und nachhaltigen Stromverbrauch zu gewährleisten. Dazu bedarf es der Installation von intelligenten Stromzählern (Smart Metern) in den Haushalten, die jedoch nicht nur Abrechnungsdaten enthalten, wie *Ulrich Greveler* analysiert, sondern „erhebliche Einblicke in die private Lebensgestaltung der Stromkunden bis hinein in die Intimsphäre" gestatten.
- Einen effizienteren Umgang mit den knappen Ressourcen des Gesundheitswesens verspricht auch die Telemedizin. Doch gerade in diesem Bereich fallen hochsensible Daten an, die eines besonderen Schutzes bedürfen. *Britta Böckmann* schlägt dazu stärkere Regulierungen und die Umsetzung konkreter datenschutzrechtlicher Maßnahmen vor.

4 Die ersten beiden Workshops („Ist das Leitbild des mündigen Verbrauchers noch zeitgemäß?", 4. Oktober 2011 und „Patentrezept Information?", 26. Juni 2012) werden 2014 in einem von Christian Bala und Klaus Müller herausgegebenen Sammelband dokumentiert, der im Klartext Verlag erscheint und über die Landeszentrale für politische Bildung Nordrhein-Westfalen beziehbar sein wird.
Die Präsentationen des 3. Workshops sind auf der Webseite des KVF NRW dokumentiert: http://www.vz-nrw.de/3-workshop-verbraucherforschung.

- Eine Kaufentscheidung zieht unweigerlich die Frage der Bezahlung nach sich. Doch die Möglichkeiten einer sicheren Zahlung sind begrenzt und vor allem die vom Telemediengesetz (§ 13 Abs. 6) vorgesehene anonyme oder pseudonyme Nutzung von Telemedien und ihrer Bezahlung stellt ein Problem dar. *Artus Krohn-Grimberghe* und *Christoph Sorge* stellen den Bitcoin als mögliche Alternative vor und weisen auf die Implikationen für den Verbraucherschutz hin.

Die Beiträge und die Diskussion im Rahmen des Workshops, die durch ein zusammenfassendes Thesenpapier dokumentiert werden, zeigen, dass es zahlreiche Herausforderungen für Verbraucherinnen und Verbraucher gibt: Einerseits stiften webbasierte Dienste wie das Cloud Computing oder die Telemedizin oder smarte Netze einen hohen Nutzen, andererseits generieren sie eine Vielzahl von Daten, von denen die Verbraucherinnen und Verbraucher nicht wissen, wozu sie verwendet werden. Es gibt Möglichkeiten, seine Anonymität im Netz zu wahren, doch sind sie mit einem erhöhten Aufwand und somit Kosten verbunden, die Konsumenten und Konsumenten nicht tragen wollen oder können (siehe Langheinrich 2007, 245). Zudem fehlt es an technischem Know-How und an einem Bewusstsein, wie weitreichend der Verlust der Privatsphäre ist und welche Folgen das für den einzelnen Verbraucher haben kann.

4 Konsum und Kontrolle

Bereits heute wird das Kaufverhalten der Verbraucherinnen und Verbraucher umfassend protokolliert; so führen viele Kundenkarten mit sich, sie sind ein direktes Instrument zur Überwachung (siehe Zurawski 2011). Kameras und RFID-Funkettiketten (Radio-Frequency Identification) dienen in Geschäften schon längst nicht mehr allein der Sicherheit oder Vorbeugung von Ladendiebstählen, sondern werden genutzt, um die Präferenzen und das Verhalten der Kunden zu vermessen (siehe Kösch 2013; Martin-Jung 2012; Mayer-Schönberger und Cuiker 2013, 138; Urban und Halm 2009). Auf dem Flughafen Johannesburg setzt der niederländische Kaffeeproduzent *Douwe Egberts* an

seinen Automaten Gesichtserkennung ein, gähnenden Passagieren wird ein Gratis-Kaffee serviert (siehe Nudd 2013).

Längst ist nicht mehr der Personal Computer (PC) das einzige Gerät, das mit dem Internet verbunden ist, Smartphones, GPS-Empfänger, Fernseher, Radios und RFID-Chips sammeln, speichern, verarbeiten und kommunizieren tagtäglich Daten, sie sind zu lokalisieren und können mit konkreten Personen in Verbindung gebracht werden (siehe Mattern 2007a, 13–14). Dieser Trend wird sich mit durch die Möglichkeiten des Ubiquitious oder Pervasive Computing fortsetzen, der Computer wird hinter dem „Internet der Dinge" zurücktreten (siehe Doctorov 2012; Mattern 2003; Mattern und Floerkemeier 2010, Weiser 1991), Alltagsgegenstände – Kühlschränke, Herde, die Beleuchtung, Autoreifen, etc. – werden ihre Funktionsweise und die Nutzung überwachen und auch miteinander kommunizieren, neue Gadgets, beispielsweise Google Glass oder Smart Watches, werden Einzug in das soziale Leben halten und nicht nur die Daten ihrer Besitzerinnen und Besitzer, sondern auch die ihrer Umgebung sammeln. Durch Wearable Computing (siehe Schumacher 2013) werden die Körperfunktionen überwacht, ein Trend, der bereits im durch die Quantified-Self-Bewegung in der Gesellschaft angekommen ist. Messbar ist alles, Puls- und Herzfrequenz, Atmung, die allgemeine Fitness, auch für die Überwachung des Schlafes finden sich technische Lösungen (siehe bsc 2013).

Im Kern sind dies alles Überwachungstechnologien, die das Leben leichter gestalten können: Werden meine Backups automatisch in der Cloud durchgeführt, schützt mich dies vor Datenverlust. Durch die Überwachung meines Stromverbrauchs kann ich Einsparpotenziale erkennen und mich auch umweltfreundlicher verhalten. Wenn mein Kühlschrank seinen Inhalt überwacht, dann schützt mich das vor einer Lebensmittelvergiftung. Werde ich durch Kameras in der Küche beobachtet und von einem Rechner auf Fehler und Abweichungen vom Rezept hingewiesen, dann kann ich ein schmackhaftes Abendessen kochen (siehe Morozov 2013b, 34). Überwacht der Autoreifen den Luftdruck, erhöht das meine Sicherheit im Straßenverkehr. Überwache ich meinen Schlaf, lebe ich gesünder und erkenne vielleicht frühzeitig eine Apnoe. Evgeny Morozov (2013b, 34) nennt das „wohlwollende Überwachung", deren Ziel es sei, zu optimieren und die Effizienz zu steigern.

Diese Form der Überwachung leistet einem „Technologiepaternalismus“ Vorschub, der konformes Verhalten hervorrufen soll (siehe Spiekermann und Pallas 2007). Noch ist diese Selbstüberwachung freiwillig, doch schon bieten amerikanische Autoversicherer ihren Kundinnen und Kunden „günstigere Tarife, wenn diese sich der Überwachung durch einen Bordcomputer unterwerfen“ (Häntzschel 2013). Auch deutsche Autoversicherer prüfen die Akzeptanz sogenannter Telematik-Tarife (siehe cst und afp 2013), bereits zum Januar 2014 kommt das erste Angebot dieser Art in Deutschland auf den Markt (siehe axk 2013). Smarte Technologien lassen sich auch mit sozialer Kontrolle und nichtmateriellen Anreizen verbinden. So werden im Projekt „BinCam“ Fotos vom Hausmüll geschossen, die Bilder werden ausgewertet und mit den Informationen auf die Facebook-Seite des Nutzers hochgeladen. Die Daten werden wöchentlich zusammengefasst, „und wenn die Mengen an Nahrungsmitteln und recyclebaren Materialien abnehmen, bekommen die Besitzer (symbolische) Blätter und Barren“ (Morozov 2013b, 20; siehe im Original Thieme et al. 2012).

Durch diese wohlwollende Überwachung im Internet der Dinge fallen „potenziell eine große Menge teilweise sensibler und intimer Daten an. [...] Und wenn in Zukunft vernetzte und ‚schlaue‘ Alltagsdinge Information von sich geben, physische Dinge also quasi selbst zu Medien werden, dann stellt sich auch die Frage, wer eigentlich über den Inhalt bestimmen darf und wer die Objektivität und Richtigkeit von ‚Aussagen‘ smarter Objekte garantiert.“ (Mattern 2007a, 16, siehe auch Roßnagel 2007) Schon die Frage, wem die Daten gehören, ist nicht leicht zu beantworten. Das Recht auf informationelle Selbstbestimmung begründet keine Eigentumsrecht an persönlichen Daten[5] (siehe Buchner 2006: 221-230; Papier 2012: 69). Wohl aber stellen die von den Nutzern erhobenen Daten immaterielle Güter dar, welche von den Firmen als ihr Eigentum betrachtet werden. Ob in Zukunft „digital gebildete“ Verbraucherinnen und Verbraucher den Wert ihrer Daten erkennen und sie monetarisieren oder

5 „Dieses Recht auf ‚informationelle Selbstbestimmung‘ ist nicht schrankenlos gewährleistet. Der Einzelne hat nicht ein Recht im Sinne einer absoluten, uneinschränkbaren Herrschaft über ‚seine‘ Daten; er ist vielmehr eine sich innerhalb der sozialen Gemeinschaft entfaltende, auf Kommunikation angewiesene Persönlichkeit. Information, auch soweit sie personenbezogen ist, stellt ein Abbild sozialer Realität dar, das nicht ausschließlich dem Betroffenen allein zugeordnet werden kann.“ (BVerfG 1983)

bewusst gegen Dienstleistungen eintauschen, also ihre „Machtfülle“ nutzen (Mayer-Schönberger und Cuiker 2013, 185), ist noch nicht abzusehen.

Ein weiteres Problem ist die Deutungshoheit über die aus den erhobenen Daten gewonnen Informationen.

5 Kafkaeske Erlebnisse

Privatwirtschaftliche und staatliche Überwachung verfolgt das Ziel, Daten zu sammeln, die dann informatisiert werden. Diese Informationen „werden gemacht und zwar mit bestimmten Absichten, die ihren Form und ihren Inhalt prägen“ (Becker 2007, 14). Daten, die in einem bestimmten Kontext entstanden sind, können, werden sie von Dritten ausgewertet und interpretiert, Auswirkungen auf reale Personen haben. „Surveillance generates information, which is often stored in record systems and used for new purposes. Being watched and inhibited in one’s behavior is only one part of the problem; the other dimension is that the data is warehoused for unknown future uses.“ (Solove 2004, 42)

Für Daniel J. Solove (2004; 2011) wird die Orwellsche Metapher vom „Big Brother“ überstrapaziert. Überwachung in der Konsumgesellschaft hat nicht Disziplinierung zum Ziel, obwohl dies auch eine Folge sein kann, sondern die Sammlung von Daten zu Marketingzwecken (Solove 2004, 34; siehe Bloching, Luck und Ramge 2012; Turow 2012). Mit diesen Informationen kann das Kaufverhalten von Verbraucherinnen und Verbrauchern eingeschätzt und gesteuert werden. „Consumer surveillance can be understood as a form of surveillance that aims at predicting and, in combination with (personalized) advertising, controlling the behavior of consumers.“ (Sandoval 2012, 148) Verbraucherinnen und Verbraucher erhalten aufgrund ihrer bisherigen Interessen gefilterte angepasste Werbung, die den Charakter einer Empfehlung hat.[6]

6 Die einschränkenden, paternalistischen Implikationen dieser Praxis hat Pariser (2012) beschrieben.

Die gesammelten Daten eines Individuums können zu Dossiers oder Profilen gebündelt werden (siehe Auer-Reinsdorff, Jakobs und Lepperhoff 2011; Solove 2004, 13-26), die problembehaftet sind: „Our digital biography is thus an unauthorized one, only partially true and very reductive. We must all live with these unauthorized biographies about us, the complete contents of which we often do not get to see. Although a more extensive dossier might be less reductive in capturing our personalities, it would have greater controlling effects on an individual's life." (Solove 2004, 46) Die Gefahr ist, dass letztlich nur noch das Dossier zählt oder die aufgrund von Big-Data-Analysen gefundenen Vorhersagen (siehe Mayer-Schönberger und Cuiker 2013, 242); dann wird nicht mehr das tatsächliche Verhalten des Individuums Grundlage einer Bewertung, sondern die Eigenschaften seines digitalen Doubles.

Die Effekte solcher Dossiers ähneln den Erfahrungen der Hauptfigur, Joseph K., in Franz Kafkas unvollendeten Roman „Der Prozess" (2005). K. sieht sich einer Anklage gegenüber, deren Inhalt er nicht kennt und gegen die er sich nicht wehren kann, da das Gericht nicht greifbar ist. „*The Trial* captures the sense of helplessness, frustration, and vulnerability one experiences when a large bureaucratic organization has control over a vast dossier of details about one's life. At any time, something could happen to Joseph K.; decisions are made based on his data, and Joseph K. has no say, no knowledge, and no ability to fight back. He is completely at the mercy of the bureaucratic process." (Solove 2004, 38)

Diese Erfahrung haben bereits Menschen gemacht, denen ihre Daten, die sie in sozialen Netzwerken offenbarten, zum Verhängnis wurden. Nur selten sind die Zusammenhänge so erkennbar wie in dem Fall, den der Jurist Victor Mayer-Schönberger (2011, 10-12) dargestellt hat: Die US-amerikanische Lehramtsanwärterin Stacy Snyder erhielt von ihrer Universität nach bestandenen Prüfungen keine Lehrbefugnis, weil sie Jahre zuvor bei MySpace ein Foto von sich hochgeladen hatte, das sie mit einem Piraten-Hütchen und einem Plastikbecher zeigte. Sie selbst gab dem Bild den Titel „Drunken Pirate". Darin wurde eine Standeswidrigkeit gesehen: „Das Foto ermutige Schüler zum ungesetzlichen Trinken von Alkohol," so die Begründung der Universität (Mayer-Schönberger 2011, 10). Einen Prozess gegen die Entscheidung verlor Stacy Snyder.

Wie Millionen andere auch, hat Stacy Snyder ihre Daten freiwillig preisgegeben, weil sie ein Partybild, das sie nicht als Geheimnis empfand, mit Freunden teilen wollte. Aus ihrem Kontext herausgerissen wurden diese Daten zu einer anderen Information gemacht, nämlich dass sie moralisch nicht für den Schuldienst geeignet sei.

Ähnliche Exklusionsmechanismen können auch in der Welt des Konsums beobachtet werden: So werten Kreditagenturen die Facebook-Profile von Antragstellern aus, falsche „Freunde" oder die mangelnde Popularität der Netzwerkpräsenz haben negative Auswirkungen auf die Kreditwürdigkeit. Noch verwenden nur kleinere Unternehmen dieses Mittel, doch britische Verbraucherschützer sehen es nur noch als eine Zeitfrage an, wann große Banken diese Datenbestände nutzen. (Siehe Eichelberger 2013a; 2013b; O.A. 2013) In Deutschland ist ein Forschungsauftrag der Schufa, mit dem die mögliche Nutzung von Daten aus sozialen Netzwerken untersucht werden sollte, im Sommer 2012 nach Protesten vorerst gescheitert (siehe anw 2012a; 2012b).

Bereits im Jahr 2006 berichtete die britische Tageszeitung „The Guardian", dass Kunden an Telefonhotlines aufgrund ihres Wertes für die Firma bewertet werden: Die Anrufe von Kunden erster Klasse werden schnell bearbeitet, gilt man als armer Kunde, landet man in der dritten Klasse und wird an das preiswerteste Call Center weitergeleitet. Auch erhalten diese Kunden keine Informationen über neue Rabatte oder Werbekampagnen (siehe Bauman 2009, 10–11; Booth 2006). Unternehmen betreiben, so analysiert Zygmunt Bauman (2009, 11) diese Praktik, „eine Art ‚negative Überwachung' [...]. Sie brauchen eine Möglichkeit die Datenbank mit jenen Informationen zu füttern, die geeignet sind, ‚fehlerhafte Konsumenten' herauszufiltern – das Unkraut des konsumistischen Gartens, Menschen, denen es an Geld, Kreditkarten, und/oder Kauflust mangelt, und die immun sind gegen die Verlockungen der Werbung. Als Ergebnis der negativen Auslese wird nur zahlungskräftigen und kaufwilligen Mitspielern erlaubt, weiterhin am Konsumspiel teilzunehmen."

Die Konsumüberwachung führt zu sozialen Klassifizierungen (siehe Gandy Jr 1993), aufgrund von hinterlassenen Datenspuren gelten Individuen als potenzielle oder wertlose Kunden (siehe Turow 2012). Diese Einteilung wirkt normativ, sie bevorzugt oder benachteiligt Individuen und Gruppen, wie Achim Tiffe (2013, 162) in einem Editorial der Zeitschrift „Verbraucher und Recht" betont:

„Wenn in Zukunft das Eigentum an Sachen durch deren Nutzung zunehmend verdrängt wird [...] wird das Scoring immer wichtiger. Ein schlechter Score-Wert führt dann nicht nur zur Ablehnung eines Kredit- oder Mobilfunkvertrages, sondern auch zur Verweigerung des Zugangs zu Dienstleistungen wie z. B. der Mobilität in der Stadt." In dem sie klassifiziert werden, müssen sie sich als „gute" oder „wertvolle" Verbraucherinnen und Verbraucher erweisen. Es genügt dann nicht mehr, Bedürfnisse befriedigen zu wollen, sondern sie müssen ihre „Tauglichkeit als Konsument" nachweisen. (Siehe Bauman und Lyon 2013, 48)

Die Mechanismen, die hinter der Ermittlung eines Terror-Scores oder der Beurteilung der Kreditwürdigkeit eines Kunden liegen, sind ähnlich (siehe Auer-Reinsdorff, Jakobs und Lepperhoff 2011, 34–45; Baumann und Lyon 2013, 88–89; Bowker und Star 2000; Meister 2013). „Die Logik ist im Bereich staatlicher Terrorabwehr die gleiche wie im Bereich des Customer Relationship Management. Es ist die Logik der Sicherheit, und das heißt heute eben: der Risikovorsorge. Staatliche Einrichtungen wollen Anschläge verhindern, Unternehmen wollen Kostenfaktoren vermeiden, Banken wollen Kreditrisiken minimieren – und alle wollen mittels Prognosen die Verfügung über die Zukunft erreichen. Im Kern werden hier jeweils automatische Entscheidungen über einzelne Menschen gefällt auf der Basis von Annahmen über Personengruppen – Terroristen oder ordentliche Bürger, ungewollte oder begehrte Kunden." (Bendrath 2007, 7)

Wie in Kafkas „Prozess" bleiben die Vorgänge, die zur Klassifikation führen, verborgen. Die Mechanismen aufgrund welcher Daten, welcher Algorithmen man einen Coupon für ein Café auf Smartphone bekommt, im Call Center aussortiert wird oder auf der No-Fly-Liste[7] landet, sind nicht durchschaubar und scheinbar willkürlich.

7 Auf die No-Fly-Liste des Terrorist Screening Centers (TSC), die verhindern soll, dass Terroristen an Bord von Flugzeugen gelangen, geraten immer wieder unbescholtene Bürger, so beispielsweise der 2009 verstorbene demokratische US-Senator Edward „Ted" Kennedey (siehe Swarns 2004) oder die ehemalige Mitarbeiterin des Justizministeriums und Whistleblowerin Jesselyn Radack (siehe Osang 2004; Slansky 2013), die auch zum Objekt polizeilicher und geheimdienstlicher Überwachungsmaßnahmen wurde.

6 „Public-Private-Partnership“?

Die großen privatwirtschaftlichen Datensammlungen wecken nicht nur die Begehrlichkeiten der Werbewirtschaft oder von Auskunfteien, mittels „Data Mining“ können Sicherheitsbehörden diese Informationen für ihre Ermittlungen nutzen (siehe Auer-Reinsdorff, Jakobs und Lepperhoff 2011, 46–49; Bendrath 2007, 6; Langheinrich 2007, 247). Nur zwei Tage vor der ersten Veröffentlichung von Glenn Greenwald (2013) über die Bespitzelung von Verizon-Kunden im „Guardian“ warnte der UN-Sonderbeauftragte für den Schutz der Meinungs- und Informationsfreiheit, Frank La Rue (zit. nach Ermert und axk 2013): „Staaten haben heute eine größere Fähigkeit zur gleichzeitigen, tiefgreifenden, gezielten und massiven Überwachung als jemals zuvor.“ In seinem Bericht betonte er unter anderem die Bedeutung von Social Media für die Überwachungsmaßnahmen: „Another tool used regularly by States today is social media monitoring. States have the capacity physically to monitor activities on social networking sites, blogs and media outlets to map connections and relationships, opinions and associations, and even locations. States can also apply highly sophisticated data mining technologies to publicly available information or to communications data provided by third party service providers. At a more basic level, States have also acquired technical means to obtain usernames and passwords from social networking sites such as Facebook.“ (United Nations 2013, 11).

Polizei und Geheimdienste sind also die Nutznießer der Datenbestände jener Internetkonzerne, die Innenminister Friedrich als Bedrohung der Privatsphäre identifiziert. Big Data ist auch für die Vertreterinnen und Vertreter der inneren Sicherheit ein Zauberwort, je leichter sie sich konkreten Personen zuordnen lassen, umso besser: Nur zwei Jahre vor den NSA-Enthüllungen, forderte Innenminister Friedrich noch einen Klarnamenzwang für Blogs und soziale Netzwerke (siehe Blum 2011; ck 2011). Facebook verpflichtet seine Nutzerinnen und Nutzer seit jeher, sich unter ihrem korrekten Namen zu registrieren, unlängst scheiterte das Unabhängige Landeszentrum für Datenschutz (ULD) Anonymität auf Facebook per Gerichtsurteil durchzusetzen (siehe Schleswig-Holsteinisches OVG 2013; vbr 2013). Constanze Kurz und Frank Rieger (2011, 104) stellen in ihrem Buch „Die Datenfresser“ fest: „Anonymität, die im Internet letztlich den einzig wirksamen Schutz vor Ausforschung und Informationsaus-

nutzung bietet, ist dem Konzern [gemeint ist hier Google, CBA/KM] ein Dorn im Auge. Die Interessen der Strafverfolger und die der kommerziellen Datensammler decken sich hier. [...] Entsprechend ist das Interesse der politischen Entscheider auch aus diesem Grund oft ausgesprochen gedämpft, wenn es um den Schutz der Privatsphäre der Bürger geht." Schon der Versuch, sich durch Verschlüsselungstechniken zu schützen, ruft die Aufmerksamkeit der transatlantischen Überwacher hervor (siehe Beuth 2013; Kurz 2013), laut dem Wassenaar-Abkommen gilt Kryptographie als Waffentechnologie (siehe Assange et al. 2013, 54; Schulzki-Haddouti 1998).

Die Enthüllung der Programme PRISM, Tempora, XKeyscore, etc. (siehe den Überblick bei Heise online 2013) hat gezeigt, dass Firmen nicht in der Lage sind, die Daten ihrer Kundinnen und Kunden vor staatlichen Zugriffen zu schützen, entweder kooperieren sie oder werden zur Kooperation gezwungen. Evgeny Morozov bezeichnet dies in der „Frankfurter Allgemeinen Zeitung" als eine „Public-Private-Partnership": „Silicon Valley betreibt, aktualisiert und monetarisiert die Infrastruktur, während die NSA nach Belieben zugreifen kann. Jede Seite spezialisiert sich, und beide Seiten profitieren." (Morozov 2013a).

Auch wenn die Unternehmen aufgrund rechtlicher „Maulkörbe" daran gehindert werden, ihre Zusammenarbeit mit den Sicherheitsbehörden transparent zu machen (siehe dpa und pek 2013; Bager 2013)[8], zeichnet sich ab,

8 Für die Einsichtnahme in die Datenbestände der Unternehmen in den USA benötigen die Sicherheitsbehörden nicht einmal einen richterlichen Beschluss, es genügt eine einfache Verfügung oder die eines geheim tagenden Sondergerichts. Die sogenannten National Security Letters (NSL) sind strafbewehrte Verfügungen, durch die Diensteanbieter gezwungen werden können, die über einen bestimmten Nutzer gespeicherten Daten den Behörden zu übergeben. Der betroffene Nutzer wird über den NSL nicht in Kenntnis gesetzt und die Empfänger eines NSL dürfen den Erhalt und den Inhalt eines NSL nicht veröffentlichen oder den Nutzer informieren. Umgekehrt können die Dienstleister gegen die Verfügung keinen Widerspruch einlegen, das kann nur die betroffene Person, die von den Behörden nicht informiert wurde und vom Empfänger nicht informiert werden darf (siehe dazu Angwin 2011; Assange et al. 2013, 24–26 u. 188–190). Google hat im Frühjahr 2013 erfolgreich gegen die Praxis der NSL geklagt, das Verfahren ist zur Zeit in der Berufung (siehe Zetter 2013). Auch durch den Foreign Intelligence Surveillance Act (FISA) können US-Behörden beim geheim tagenden United States Foreign Intelligence Surveillance Court (FISC) Personen und Unternehmen verpflichten gespeicherte Daten herauszugeben (siehe Lichtblau 2013).

dass wahrscheinlich ein direkter Zugriff auf die Daten von Google, Facebook, Yahoo, Microsoft (Hotmail und Skype) oder AOL besteht, rund fünfzig Firmen sollen in den USA mit der NSA kooperieren (siehe Ambinder 2013; anw 2013; mho 2013). So soll Microsoft der NSA technisch ermöglicht haben, Zugriff auf E-Mails zu nehmen, bevor diese verschlüsselt werden, oder Skype-Telefonate abzuhören (siehe jk 2013b).

Auch die Rückgrate des Internets, die Hauptleitungen und ihre Abzweigungen (Backbones), werden angezapft: Das britische GCHQ hat Zugriff auf die Leitungen „TAT-14 und AC-1 zur Kommunikation mit Nordamerika, das Kabel SeaMeWe-3 als Verbindung nach Afrika, Asien und Australien sowie das Kabel Pan-European-Crossing PEC, das viele Metropolregionen Westeuropas miteinander verbindet“ (Goetz, Ruprecht und Strozyk 2013). Dabei kooperieren – freiwillig oder unfreiwillig – sechs Firmen, die auch für die Internet-Infrastruktur in Deutschland verantwortlich sind, mit dem britischen Geheimdienst: British Telecommunications (BT), Level-3, Viatel, Interoute, Verizon und Vodafone (siehe Goetz, Ruprecht und Strozyk 2013). Einige sogenannte „Intercept Partner“ stellen eigens angepasste Hard- und Software zur Verfügung (siehe Bleich und Mondial 2013). Sind die Telekommunikationsunternehmen in den USA geschäftlich aktiv, so werden sie dort von den Behörden gezwungen, den Datenverkehr durch verplombte Abhörschnittstellen zu leiten (siehe Bleich und Mondial 2013, 24). Ob die NSA auch Zugriff auf deutsche Knotenpunkte hat, ist umstritten (siehe cis und Reuters 2013).

Auch wurde bekannt, dass Programme der NSA („Bullrun“) und des GCHQ („Edgehill“) existieren, die die Überwindung von Verschlüsselungstechniken wie Secure Sockets Layer (SSL) oder Virtual Private Networks (VPN) ermöglichen, indem sie Schlüssel entweder entwenden oder in Kooperation mit den Herstellern, die in den Artikeln des „Guardian“ (Ball, Borger und Greenwald 2013) und der „New York Times“ (Perlroth, Larsson und Shane 2013) auf Intervention der Geheimdienste nicht genannt werden (siehe jk 2013a), absichtlich Hintertüren einbauen (siehe ju 2013). Auch wenn sich die Meldung des „Spiegels“ (Poitras, Rosenbach und Stark 2013), dass es absichtliche Hintertüren in Smartphones gäbe, nicht aufrecht erhalten ließ (siehe Schmidt 2013), offenbart die dokumentierte NSA-Präsentation die Denkweise des Geheimdienstes hinsichtlich der Verbraucherinnen und Verbraucher und der privatwirtschaftlichen Datensammlungen: „Who knew in 1984 that this [man sieht ein Bild von

Steve Jobs mit dem iPhone] would be big brother and the zombies would be [man sieht Bilder von begeisterten iPhone-Nutzern] paying customers?“ (Zit. nach Poitras, Rosenbach und Stark 2013, 144–145)

Damit Verbraucherinnen und Verbraucher nicht zu „Zombies“ degradiert werden, muss Datenschutz zu einem gesellschaftlichen Thema werden. Im Zentrum steht die Frage, ob und wie die Datensouveränität der Verbraucherinnen und Verbraucher unter den Bedingungen des Konsums im Internet, der Nutzung digitaler Dienste und in einer vernetzten Welt erhalten, wiederhergestellt oder gestärkt werden kann. Dieser Band möchte dazu einen Beitrag leisten.

Literatur

Adamek, Sascha. 2011. *Die facebook-Falle: Wie das soziale Netzwerk unser Leben verkauft*. München: Heyne.

Aly, Götz und Karl Heinz Roth. 2005. *Die restlose Erfassung. Volkszählen, Identifizieren, Aussondern im Nationalsozialismus*. 2. Auflage. Frankfurt am Main: Fischer.

Ambinder, Marc. 2013. Sources: NSA sucks in data from 50 companies. *The Week*. 6. Juni. http://theweek.com/article/index/245311/sources-nsa-sucks-in-data-from-50-companies (Zugriff: 30. August 2013).

Angwin, Julia. 2011. Secret Orders Target Email. *Wall Street Journal*, 9. Oktober. http://online.wsj.com/article/SB10001424052970203476804576613284007315072.html# (Zugriff: 28. August 2013).

anw. 2012a. Bericht: Schufa will Daten in sozialen Netzwerken nutzen. *heise online*. 7. Juni. http://www.heise.de/newsticker/meldung/Bericht-Schufa-will-Daten-in-sozialen-Netzwerken-nutzen-1612450.html (Zugriff: 4. September 2013).

—. 2012b. Hasso-Plattner-Institut kündigt Schufa-Forschungsprojekt. *heise online*. 8. Juni. http://www.heise.de/newsticker/meldung/Hasso-Plattner-Institut-kuendigt-Schufa-Forschungsprojekt-1614109.html (Zugriff: 4. September 2013).

—. 2013a. Bericht: US-Regierung zapft Kundendaten von Internet-Firmen an. *heise online*. 7. Juni. http://www.heise.de/newsticker/meldung/Bericht-

US-Regierung-zapft-Kundendaten-von-Internet-Firmen-an-1884264.html (Zugriff: 30. August 2013).

—. 2013b. Facebook kann Belohnungssystem im Hirn aktivieren. *heise online*. 30. August. http://heise.de/-1945742 (Zugriff: 30. August 2013).

Assange, Julian, Jacob Appelbaum, Andy Müller-Maghun und Jérémie Zimmermann. 2013. *Cypherpunks: Unsere Freiheit und die Zukunft des Internets*. Frankfurt am Main: Campus.

Auer-Reinsdorff, Astrid, Joachim Jakobs und Niels Lepperhoff. 2011. *Vom Datum zum Dossier: Wie der Mensch mit seinen schutzlosen Daten in der Informationsgesellschaft ferngesteuert werden kann*. Hannover: Heise.

axk. 2013. Verwanzt versichert: Vom Fahrverhalten abhängiger Versicherungstarif bei S-Direkt. *heise online*. 12. November. http://www.heise.de/newsticker/meldung/Verwanzt-versichert-Vom-Fahrverhalten-abhaengiger-Versicherungstarif-bei-S-Direkt-2044361.html (Zugriff: 14. November 2013).

Bager, Jo. 2013. NSA-Affäre: Was wir wissen und was wir nicht wissen. *c't*. 22. August. http://www.heise.de/ct/artikel/NSA-Affaere-Was-wir-wissen-und-was-wir-nicht-wissen-1939810.html (Zugriff: 30. August 2013).

Ball, James, Julian Borger und Glenn Greenwald. 2013. Revealed: How US and UK spy agencies defeat internet privacy and security. *The Guardian*, 5. September. http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security (Zugriff: 9. September 2013).

Bauman, Zygmunt. 2003. *Flüchtige Moderne*. Frankfurt am Main: Suhrkamp.

—. 2008. *Flüchtige Zeiten: Leben in der Ungewissheit*. Hamburg: Hamburger Edition.

—. 2009. *Leben als Konsum*. Hamburg: Hamburger Edition.

Bauman, Zygmunt und David Lyon. 2013. *Daten, Drohnen, Disziplin: Ein Gespräch über flüchtige Überwachung*. Berlin: Suhrkamp.

Becker, Matthias. 2010. *Datenschatten: Auf dem Weg in die Überwachungsgesellschaft?* Hannover: Heise.

Bendrath, Ralf. 2007. Der gläserne Bürger und der vorsorgliche Staat: Zum Verhältnis von Überwachung und Sicherheit in der Informationsgesellschaft. *kommunikation@gesellschaft* 8 (Beitrag 7). http://www.soz.uni-frankfurt.de/K.G/B7_2007_Bendrath.pdf.

Bergmann, Nicole. 2009. *Volkszählung und Datenschutz: Proteste zur Volkszählung 1983 und 1987 in der Bundesrepublik Deutschland*. Hamburg: Diplomica-Verlag.

Beuth, Patrick. 2013. Prism: Verschlüsselte Mails machen die NSA neugierig. *Die Zeit*, 21. Juni. http://www.zeit.de/digital/datenschutz/2013-06/nsa-speichert-verschluesselte-mails (Zugriff: 2. September 2013).

BITKOM. 2011a. *Datenschutz im Internet: Eine repräsentative Untersuchung zum Thema Daten im Internet aus Nutzersicht*. 2. Auflage. Berlin: BITKOM. http://www.bitkom.org/files/documents/BITKOM_Publikation_Datenschutz_im_Internet.pdf.

—. 2011b. *Soziale Netzwerke. Eine repräsentative Untersuchung zur Nutzung sozialer Netzwerke im Internet*. 2. Auflage. Berlin: BITKOM. http://www.bitkom.org/files/documents/SozialeNetzwerke.pdf.

Bleich, Holger und Sebastian Mondial. 2013. Willfährige Helfer. Provider unterstützen die Geheimdienste beim Datenschnüffeln. *c't*, Nr. 18 (12. August): 24–25.

Bloching, Björn, Lars Luck und Thomas Ramge. 2012. *Data Unser: Wie Kundendaten die Wirtschaft revolutionieren*. München: Redline.

Blum, Daniel. 2011. Erkennbar politisch – Die Debatte um den Klarnamenzwang im Internet. *Deutschlandfunk*. 2. Oktober. http://www.dradio.de/dlf/sendungen/hintergrundpolitik/1568669/ (Zugriff: 30. August 2013).

Booth, Nick. 2006. „Press 1 if you're poor, 2 if you're loaded...". *The Guardian*, 2. März. http://www.theguardian.com/technology/2006/mar/02/newmedia.consumernews (Zugriff: 9. Oktober 2013).

Bowker, Geoffrey C. und Susan Leigh Star. 2000. *Sorting things out: Classification and its consequences*. Cambridge, MA: MIT Press.

Brin, David. 1998. *The transparent society: Will technology force us to choose between privacy and freedom?* Reading, MA: Perseus Books.

bsc. 2013. Quantified Self: Sleep Tracker mit Matratzenmontage. *heise online*. 25. September. http://heise.de/-1952834 (Zugriff: 14. Oktober 2013).

Buchner, Benedikt. 2006. *Informationelle Selbstbestimmung im Privatrecht*. Tübingen: Mohr Siebeck.

BVerfG, Urteil vom 15. Dezember 1983, Az. 1 BvR 209/83, 1 BvR 362/83, 1 BvR 484/83, 1 BvR 440/83, 1 BvR 420/83, 1 BvR 269/83 (Volkszählungsurteil). http://openjur.de/u/268440.html (= openJur 2012, 616).

c't TV. 2011. Aufgepasst! – Die Datensammler kommen! *heise Video*. 15. Januar. http://www.heise.de/video/artikel/Aufgepasst-Die-Datensammler-kommen-1510916.html.

cis und Reuters. 2013. Innenminister Friedrich bestreitet NSA-Zugriff auf De-Cix. *Spiegel Online*, 2. Juli. http://www.spiegel.de/netzwelt/netzpolitik/

innenminister-friedrich-bestreitet-nsa-zugriff-auf-de-cix-a-909086.html (Zugriff: 29. August 2013).
ck. 2011. Innenminister stellt Anonymität im Netz zur Disposition [2. Update]. *heise online*. 8. August. http://heise.de/-1319242 (Zugriff: 30. August 2013).
cst und afp. 2013. Kfz-Versicherung mit Kontrollgerät. *Spiegel Online*, 26. September. http://www.spiegel.de/auto/aktuell/kfz-versicherung-mit-kontrollgeraet-a-924716.html (Zugriff: 15. Oktober 2013).
Dick, Philip K. 2002. *Der unmögliche Planet: Stories*. München: Heyne.
Doctorow, Cory. 2011. *Little Brother: Roman*. Reinbek: Rowohlt.
—. 2012. Lockdown: The coming war on general-purpose computing. *Boing Boing*. 10. Januar. http://boingboing.net/2012/01/10/lockdown.html (Zugriff: 28. August 2013).
dpa und axk. 2013. Obama: „Niemand hört Ihre Anrufe ab". *heise online*. 7. Juni. http://www.heise.de/newsticker/meldung/Obama-Niemand-hoert-Ihre-Anrufe-ab-1885104.html (Zugriff: 28. August 2013).
Dworschak, Manfred. 2011. Im Netz der Späher. *Der Spiegel*, Nr. 2 (10. Januar): 114–124. http://www.spiegel.de/spiegel/print/d-76229521.html (Zugriff: 30. August 2013).
Eichelberger, Erika. 2013a. Your Facebook Friends Could Soon Prevent You From Getting a Loan. *Mother Jones*, 27. August. http://www.motherjones.com/mojo/2013/08/facebook-friends-credit-lenddo-kreditech-cnn (Zugriff: 20. September 2013).
—. 2013b. Can you be denied a loan because you're unpopular on Facebook? *Mother Jones*, 18. September. http://www.motherjones.com/politics/2013/09/lenders-vet-borrowers-social-media-facebook (Zugriff: 20. September 2013).
Ermert, Monika und axk. 2013. UN-Bericht warnt vor zuviel staatlicher Überwachung. *heise online*. 4. Juni. http://www.heise.de/newsticker/meldung/UN-Bericht-warnt-vor-zuviel-staatlicher-Ueberwachung-1876260.html (Zugriff: 27. August 2013).
Forgó, Nikolaus, Tina Krügel und Kathrin Müllenbach. 2010. Zur datenschutz- und persönlichkeitsrechtlichen Zulässigkeit von Google Street View. *Computer und Recht* 26, Nr. 9: 616–624. doi:10.9785/ovs-cr-2010-616.
Foucault, Michel. 1994. *Überwachen und Strafen: die Geburt des Gefängnisses*. Frankfurt am Main: Suhrkamp.

Franck, Georg. 2010. *Ökonomie der Aufmerksamkeit: Ein Entwurf*. 10. Auflage. München: Hanser.

Frank, Softwareentwickler aus Hamburg. 2011. Bericht aus der IT-Welt: Wie wir „user Content" zur Ware machen. In: *Generation Facebook: Über das Leben im Social Net*, hg. von Oliver Leistert und Theo Röhle, 75–77. Bielefeld: transcript.

Gandy Jr, Oscar H. 1993. *The panoptic sort: A political economy of personal information*. Boulder, CO: Westview.

Gesellschaft für Informatik. 2013. FAQ-Liste zu Sicherheit und Unsicherheit im Internet (Version 1.0). Bonn, 2. September. http://www.gi.de/fileadmin/redaktion/Download/GI-FAQ-Ausspaehung2013-V1.0.pdf.

Goetz, John, Anne Ruprecht und Jan Lukas Strozyk. 2013. Britische Spionage in Deutschland. Neue Dokumente belasten GCHQ. *tagesschau.de*. 28. August. http://www.tagesschau.de/inland/gchqtelekom100.html (Zugriff: 29. August 2013).

Greenwald, Glenn. 2013. NSA collecting phone records of millions of Verizon customers daily. *The Guardian*. 6. Juni. http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order (Zugriff: 27. August 2013).

Häntzschel, Jörg. 2013. Du kannst nicht mehr untertauchen. *Süddeutsche Zeitung* (7. Oktober): 11.

Heise online. 2013. PRISM – der Geheimdienst hört mit. *heise online*. http://www.heise.de/thema/?thema=PRISM (Zugriff: 27. August 2013).

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

Hürter, Johannes und Jürgen Zarusky, Hrsg. 2008. *Besatzung, Kollaboration, Holocaust: Neue Studien zur Verfolgung und Ermordung der europäischen Juden*. München: Oldenbourg.

Jansen, Frank und Christian Tretbar. 2013. „Internationale Internetkonzerne gefährden unsere Freiheit" [Gespräch mit Hans-Peter Friedrich]. *Der Tagesspiegel Online*, 7. September. http://www.tagesspiegel.de/politik/bundesinnenminister-hans-peter-friedrich-internationale-internetkonzerne-gefaehrden-unsere-freiheit/8755118.html (Zugriff: 9. September 2013).

jk. 2013a. PRISM-Überwachungskandal: Microsoft ermöglicht NSA Zugriff auf Skype, Outlook.com, Skydrive. *heise online*. 12. Juli. http://www.heise.de/newsticker/meldung/PRISM-Ueberwachungskandal-Microsoft-

ermoeglicht-NSA-Zugriff-auf-Skype-Outlook-com-Skydrive-1916340.html (Zugriff: 5. September 2013).

—. 2013b. Geheimdienste wollten Veröffentlichung über NSA-Verschlüsselungsattacke verhindern. *heise online*. 6. September. http://www.heise.de/newsticker/meldung/Geheimdienste-wollten-Veroeffentlichung-ueber-NSA-Verschluesselungsattacke-verhindern-1951133.html (Zugriff: 9. September 2013).

ju. 2013. NSA und GCHQ: Großangriff auf Verschlüsselung im Internet. *heise online*. 6. September. http://www.heise.de/newsticker/meldung/NSA-und-GCHQ-Grossangriff-auf-Verschluesselung-im-Internet-1950935.html (Zugriff: 9. September 2013).

Kafka, Franz. 2005. *Der Prozess: Roman*. Frankfurt am Main: Suhrkamp.

Knoke, Felix. 2013. Watching you: Der Ärger mit den Daten. *DE:BUG Magazin*, Nr. 175 (September): 9–11.

Kösch, Sascha. 2013. Big Brother in der Umkleide: Überwachung und Alltag. *DE:BUG Magazin*, Nr. 175 (September): 15.

Kurz, Constanze und Frank Rieger. 2011. *Die Datenfresser: Und wie wir die Kontrolle darüber zurückerlangen*. Frankfurt am Main: Fischer.

Kurz, Constanze. 2013. Verschlüsselung: Angriff auf die Anonymität im Netz. *FAZ.NET*, 9. August. http://www.faz.net/aktuell/feuilleton/aus-dem-maschinenraum/verschluesselung-angriff-auf-die-anonymitaet-im-netz-12452293.html (Zugriff: 2. September 2013).

Landesanstalt für Medien NRW. 2012. Zwischen Selbstoffenbarung und Privatheit: Wie schützen junge Menschen ihre Daten? Landesanstalt für Medien NRW präsentiert neue Studie zum Datenschutzverhalten junger Menschen in sozialen Netzwerken. 29. Oktober. http://www.lfm-nrw.de/aktuell/pressemitteilungen/pressemitteilungen-detail/article/zwischen-selbstoffenbarung-und-privatheit-wie-schuetzen-junge-menschen-ihre-daten.html (Zugriff: 14. Oktober 2013).

Langheinrich, Marc. 2007. Gibt es in einer total informatisierten Welt noch eine Privatsphäre? In: *Die Informatisierung des Alltags: Leben in smarten Umgebungen*, hg. von Friedemann Mattern, 233–264. Berlin: Springer.

Lewinski, Kai von. 2012. Zur Geschichte von Privatsphäre und Datenschutz – eine rechtshistorische Perspektive. In: *Datenschutz. Grundlagen, Entwicklungen und Kontroversen*, hg von. Jan-Hinrik Schmidt und Thilo Weichert, 23–33. Bonn: Bundeszentrale für politische Bildung.

Lichtblau, Eric. 2013. In Secret, Court Vastly Broadens Powers of N.S.A. *The New York Times*, 6. Juli. http://www.nytimes.com/2013/07/07/us/in-secret-court-vastly-broadens-powers-of-nsa.html (Zugriff: 3. September 2013).

Lyon, David, Hrsg. 2006. *Theorizing surveillance: The panopticon and beyond*. Cullompton, Devon: Willan Pub.

Martin-Jung, Helmut. 2012. Auswertung des Einkaufsverhaltens: Wie der Ladenkunde gläsern wird. *sueddeutsche.de*, 29. Januar. http://www.sueddeutsche.de/digital/auswertung-des-einkaufsverhaltens-wie-der-ladenkunde-glaesern-wird-1.1269137 (Zugriff: 2. September 2013).

Mattern, Friedemann. 2003. Vom Verschwinden des Computers – Die Vision des Ubiquitous Computing. In: *Total vernetzt*, hg. von Friedemann Mattern, 1–41. Berlin: Springer.

—. 2007a. Acht Thesen zur Informatisierung des Alltags. In: *Die Informatisierung des Alltags: Leben in smarten Umgebungen*, hg. von Friedemann Mattern, 11–16. Berlin: Springer.

—, Hrsg. 2007b. *Die Informatisierung des Alltags: Leben in smarten Umgebungen*. Berlin: Springer.

Mattern, Friedemann und Christian Floerkemeier. 2010. Vom Internet der Computer zum Internet der Dinge. *Informatik-Spektrum* 33, Nr. 2 (April): 107–121. http://www.vs.inf.ethz.ch/publ/papers/Internet-der-Dinge.pdf (Zugriff: 26. September 2013).

Mayer-Schönberger, Viktor und Kenneth Cukier. 2013. *Big Data: Die Revolution, die unser Leben verändern wird*. München: Redline.

Mayer-Schönberger, Viktor. 2011. *Delete: Die Tugend des Vergessens in digitalen Zeiten*. 2. Auflage. Berlin: Berlin University Press.

Meister, Andre. 2013. Willst du einen Kredit? Aber nur, wenn uns deine Facebook-Freunde passen und du uns in deinen PayPal Account lässt. *Netzpolitik.org*. 29. August. https://netzpolitik.org/2013/willst-du-einen-kredit-aber-nur-wenn-uns-deine-facebook-freunde-passen-und-du-uns-in-deinen-paypal-account-laesst/ (Zugriff: 2. September 2013).

mho. 2013. PRISM: NSA zahlte US-Unternehmen angeblich Millionen. *heise online*. 23. August. http://www.heise.de/newsticker/meldung/PRISM-NSA-zahlte-US-Unternehmen-angeblich-Millionen-1942031.html (Zugriff: 30. August 2013).

Moore, Alan und David Lloyd. 2003. *V wie Vendetta*. Bad Tölz: Tilsner.

Morozov, Evgeny. 2013a. Ideologie des Datenkonsums: Der Preis der Heuchelei – Überwachung. *Frankfurter Allgemeine Zeitung*, 24. Juli. http://www.faz.net/aktuell/feuilleton/debatten/ueberwachung/ideologie-des-datenkonsums-der-preis-der-heuchelei-12292822.html (Zugriff: 24. Juli 2013).

—. 2013b. *Smarte neue Welt: Digitale Technik und die Freiheit des Menschen*. München: Blessing.

Nudd, Tim. 2013. Coffee Brand Pours You a Free Cup When You Yawn at Its Vending Machine. *AdWeek*. 24. Juli. http://www.adweek.com/adfreak/coffee-brand-pours-you-free-cup-when-you-yawn-its-vending-machine-151401 (Zugriff: 5. September 2013).

O. A. 2013. Stat oil: Lenders are turning to social media to assess borrowers. *The Economist*. 9. Februar. http://www.economist.com/news/finance-and-economics/21571468-lenders-are-turning-social-media-assess-borrowers-stat-oil (Zugriff: 20. September 2013).

Orwell, George. 2011. *1984: Roman*. Berlin: Ullstein.

Osang, Alexander. 2004. Ein patriotischer Akt. *Der Spiegel*, Nr. 11 (8. März). http://www.spiegel.de/spiegel/print/d-30158036.html (Zugriff: 3. September 2013).

Papier, Hans-Jürgen. 2012. Verfassungsrechtliche Grundlegung des Datenschutzes. In: *Datenschutz. Grundlagen, Entwicklungen und Kontroversen*, hg von. Jan-Hinrik Schmidt und Thilo Weichert, 67–77. Bonn: Bundeszentrale für politische Bildung.

Pariser, Eli. 2012. *Filter Bubble: Wie wir im Internet entmündigt werden*. München: Hanser.

Perlroth, Nicole, Jeff Larson und Scott Shane. 2013. N.S.A. Able to Foil Basic Safeguards of Privacy on Web. *The New York Times*, 5. September. http://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html (Zugriff: 9. September 2013).

Poitras, Laura, Marcel Rosenbach und Holger Stark. 2013. iSpy. *Der Spiegel*, Nr. 27 (9. September): 144–147.

Roßnagel, Alexander. 2007. *Datenschutz in einem informatisierten Alltag: Gutachten*. Berlin: Stabsabt. der Friedrich-Ebert-Stiftung. http://library.fes.de/pdf-files/stabsabteilung/04548.pdf.

Sandoval, Marisol. 2012. A critical empirical case study if consumer surveillance on Web 2.0. In: *Internet and surveillance: The challenges of Web 2.0 and social media*, hg. von Christian Fuchs, Kees Boersma, Anders Albrechtslund und Marisol Sandoval, 147–169. New York: Routledge.

Schenk, Michael, Julia Niemann, Gabi Reinmann und Alexander Roßnagel, Hrsg. 2012. *Digitale Privatsphäre: Heranwachsende und Datenschutz auf sozialen Netzwerkplattformen*. Bd. 71. Schriftenreihe Medienforschung der LfM. Berlin: Vistas.

Schindler, Jörg, Martin Doerry und Hubert Gude. 2013. Spiegel-Gespräch [mit Bundesinnenminister Hans-Peter Friedrich]: „Es passieren auch Fehler". *Der Spiegel*, Nr. 35 (26. August): 32–34.

Schleswig-Holsteinisches OVG. 2013. Beschluss vom 22. April, Az. 4 MB 10/13 und 4 MB 11/13.

Schmidt, Jürgen. 2013. Die Grenzen der NSA. *c't*, Nr. 21 (23. September): 30.

Schulzki-Haddouti, Christiane. 1998. Umrüstung: Kryptographie gilt weiterhin als Waffe. *c't*, Nr. 26. http://www.heise.de/ct/artikel/Umruestung-286746.html (Zugriff: 17. Oktober 2013).

Schumacher, Florian. 2013. Angewachsen: Wie Wearables unseren Alltag verändern werden. *c't*, Nr. 25 (18. November): 86–90.

Semple, Janet. 1993. *Bentham's prison: A study of the panopticon penitentiary*. Oxford: Clarendon Press, Oxford University Press.

sha. 2013. Prism: George Orwells „1984" in USA und Großbritannien Bestseller. *Spiegel Online*, 13. Juni. http://www.spiegel.de/kultur/literatur/prism-george-orwells-1984-in-usa-und-grossbritannien-bestseller-a-905492.html (Zugriff: 28. August 2013).

Slansky, Heike. 2013. Anwältin wird Opfer von US-Geheimdienst. *ZDF heute journal*. Studio Washington: ZDF, 19. Juni. http://www.zdf.de/ZDFmediathek/beitrag/video/1926448/Anwaeltin-wird-Opfer-von-US-Geheimdienst (Zugriff: 28. August 2013).

Solove, Daniel J. 2004. *The digital person: Technology and privacy in the information age*. New York: New York University Press. http://docs.law.gwu.edu/facweb/dsolove/Digital-Person/text.htm.

—. 2011. *Nothing to hide: The false tradeoff between privacy and security*. New Haven: Yale University Press.

Spiekermann, Sarah und Frank Pallas. 2007. Technologiepaternalismus – Soziale Auswirkungen des Ubiquitous Computing jenseits von Privatsphäre. In: *Die Informatisierung des Alltags*, hg. von Friedemann Mattern, 311–325. Berlin: Springer. doi: 10.1007/978-3-540-71455-2_16.

Sprenger, Polly. 1999. Sun on Privacy: „Get Over It". *WIRED*. 26. Januar. http://www.wired.com/politics/law/news/1999/01/17538 (Zugriff: 16. Oktober 2013).

Stampfl, Nora S. 2013. *Die berechnete Welt: Leben unter dem Einfluss von Algorithmen*. Hannover: Heise.

Swarns, Rachel L. 2004. Senator? Terrorist? A Watch List Stops Kennedy at Airport. *The New York Times*, 20. August. http://www.nytimes.com/2004/08/20/national/20flight.html (Zugriff: 5. September 2013).

Thieme, Anja, Rob Comber, Julia Miebach, Jack Weeden, Nicole Kraemer, Shaun Lawson und Patrick Olivier. 2012. „We've bin watching you": Designing for reflection and social persuasion to promote sustainable lifestyles. In: *CHI ,12 Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, hg. von Joseph A. Konstan, 2337–2346. New York: ACM Press. doi:10.1145/2207676.2208394.

Tiffe, Achim. 2013. Social Media, Musik-Downloads, Cloud-Computing und „Beratungsklau" – wo werden die Herausforderungen im Verbraucherschutz der Zukunft liegen? *Verbraucher und Recht* 28, Nr. 5: 161–162.

Turow, Joseph. 2012. *The Daily You: How the advertising industry is defining your identity and your worth*. New Haven: Yale University Press.

Twelve Hawks, John. 2012. *Traveler: Im Auge des Bösen. Die Traveler-Trilogie in einem Band*. München: Goldmann.

United Nations. 2013. *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue*. A/HRC/23/40. New York: Human Rights Council. http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf (Zugriff: 27. August 2013).

Urban, Arnd I. und Gerhard Halm, Hrsg. 2009. *Mit RFID zur innovativen Kreislaufwirtschaft*. Kassel: Kassel University Press.

vbr. 2013. Schlappe für Datenschützer im Streit über Klarnamen bei Facebook. *heise online*. 23. April. http://www.heise.de/newsticker/meldung/Schlappe-fuer-Datenschuetzer-im-Streit-ueber-Klarnamen-bei-Facebook-1847955.html (Zugriff: 30. August 2013).

Weiser, Mark. 1991. The Computer for the 21st Century. *Scientific American* 265, Nr. 3 (September): 94–104. doi:10.1038/scientificamerican0991-94.

Wiedemann, Carolin. 2011. Facebook: Das Assessment-Center der alltäglichen Lebensführung. In: *Generation Facebook: Über das Leben im Social Net*, hg. von Oliver Leistert und Theo Röhle, 161–181. Bielefeld: transcript.

Witt, Bernhard C. 2012. *Datenschutz kompakt und verständlich: Eine praxisorientierte Einführung*. 3. Auflage. Wiesbaden: Vieweg + Teubner.

Zetter, Kim. 2013. Google Takes on Rare Fight Against National Security Letters. *Wired.com*. 4. April. http://www.wired.com/threatlevel/2013/04/google-fights-nsl/ (Zugriff: 3. September 2013).

Zurawski, Nils. 2011. „Budni, ist doch Ehrensache“ – Kundenkarten als Kontrollinstrument und die Alltäglichkeit des Einkaufens. In: *Überwachungspraxen – Praktiken der Überwachung: Analysen zum Verhältnis von Alltag, Technik und Kontrolle*, hg. von Nils Zurawski, 65–85. Opladen: Budrich UniPress.

Die Privatsphäre des Verbrauchers – ein Luxusgut?

Rainer Böhme und Sebastian Luhn

Abstract

Dieser Artikel plädiert für einen ökonomischen Zugang zu Fragen der Datenschutzregulierung. Dabei ist es wichtig, neben Kennzahlen der sozialen Wohlfahrt, die am Beispiel einer „Laffer-Kurve" für den Datenschutz diskutiert wird, auch Auswirkungen auf die Verteilungsgerechtigkeit zu betrachten. Mikroökonomische Argumente legen nahe, dass Umverteilungseffekte von Datenschutzregulierung insbesondere davon abhängen, ob Datenschutz allgemein verbindlich vorgeschrieben ist oder ob jeder einzelne Verbraucher sein gewünschtes Datenschutzniveau wählen darf.

1 Einleitung

Datenschutz und die Privatsphäre der Verbraucher werden üblicherweise aus juristischer oder technischer Perspektive betrachtet. Dabei geht es meist um Abwehrrechte des Verbrauchers gegenüber Unternehmen oder dem Staat oder um die Implikationen neuer Technik für den Datenschutz. Eine ökonomische Perspektive, sei sie mikroökonomisch oder makroökonomisch, also auf den Einzelnen oder die Gesellschaft bezogen, wird seltener eingenommen. Auch aktuelle Debatten über Datenschutz und die Privatsphäre in Medien, Politik und Gesellschaft werden meist über den Datenschutz per se geführt; Beispiele finden sich bei Krempl und Holland (2012), Wilkens (2012) sowie Steiner und Kuri (2013). Dem Datenschutz wird aus sich selbst heraus ein Wert beigemessen und er wird mit anderen, zu ihm in Konflikt stehenden Konzepten verglichen und bewertet, jedoch fehlt notgedrungen ein Vergleichsmaßstab.

In diesem Beitrag soll eine ökonomische Herangehensweise an das Thema Datenschutz und Privatsphäre aufgezeigt und diskutiert werden. Diese verspricht eine Quantifizierung des Wertes des Datenschutzes, sowohl für den Einzelnen als auch für die Gesellschaft als Ganzes. Zudem können ökonomische Argumente auf mögliche Veränderungen der politisch gegebenen Rahmenbedingungen angewendet werden, um die Folgen dieser Veränderungen abschätzen zu können.

Eine ökonomische Betrachtung bringt mit sich, dass Datenschutz und Privatsphäre ein Wert und damit ein Preis zugeordnet werden. Es bleibt zu analysieren, wie hoch dieser Preis ist und welche Verbraucher sich Datenschutz und Privatsphäre leisten können.

Die Frage, ob die weit gefasste *Privatsphäre* des Verbrauchers ein Luxusgut ist, lässt sich relativ einfach positiv beantworten: Die Größe des privaten Raumes, etwa in Form einer Wohnung oder eines Hauses, hängt direkt davon ab, wie viel der Einzelne zu zahlen in der Lage ist. Im Fokus dieses Beitrags steht daher der engere Begriff des *Datenschutzes*, einem Teilbereich der Privatsphäre, der nicht einfach durch größere Immobilien käuflich ist. Außerdem beschränkt sich die Darstellung auf den durchschnittlichen Verbraucher als Gegenstand

der Betrachtung. Für extreme Formen des sozialen Status' gelten spezielle Regeln, die hier jedoch nicht näher erörtert werden.

Dieser Beitrag ist folgendermaßen gegliedert: Zunächst wird der Wert der Privatsphäre unter gesamtgesellschaftlichen Aspekten betrachtet. Danach folgt die Diskussion unter mikroökonomischen Aspekten. Anschließend wird ein kurzes Fazit gezogen und es werden Handlungsempfehlungen für verbraucherpolitische Akteure gegeben.

2 Der Wert des Datenschutzes für die Gesellschaft

Um den Wert des Datenschutzes gesamtgesellschaftlich zu bemessen, ist es hilfreich, einige Annahmen zu treffen. Aspekte des Datenschutzes sowie deren gesetzlich festgelegte Ausprägungen können sehr komplex werden und jeder Teilaspekt für sich kann unterschiedlich starke Auswirkungen haben. Für eine Betrachtung der Auswirkungen ist es daher hilfreich, von einer eindimensionalen Skala auszugehen, die an ihren Enden durch die Größen „gar kein Datenschutz" beziehungsweise „alle personenbezogenen Daten sind geheim" (d. h. maximal denkbarer Datenschutz) begrenzt wird. Wenn kein Datenschutz existiert, kann man davon ausgehen, dass alle personenbezogenen Daten bekannt und öffentlich zugänglich sind. Zudem kann der Aspekt des Wertes des Datenschutzes vereinfacht als Auswirkung auf die soziale Wohlfahrt der Gesellschaft dargestellt werden. Diese wiederum wird in einem dafür geeigneten Maß gemessen, wie zum Beispiel dem Bruttoinlandsprodukt (BIP) als erste Näherung.

Durch diese Annahmen ist es möglich, die soziale Wohlfahrt als Funktion des Umfangs des Datenschutzes in einem Diagramm darzustellen. Der daraus folgende Zusammenhang kann zwar, wie der Beitrag weiter zeigt, theoretisch begründet, aber nicht empirisch belegt werden. Das hängt zum einen damit zusammen, dass es sehr aufwändig ist, sowohl das Datenschutzniveau als

auch die soziale Wohlfahrt zu messen, zum anderen mit der Tatsache, dass es noch viele weitere Einflussfaktoren der sozialen Wohlfahrt gibt, sodass der Einfluss eines einzelnen Faktors schwierig zu isolieren ist. Der Einfluss des Datenschutzniveaus verschiedener Staaten etwa auf die soziale Wohlfahrt dieser Staaten ist kaum in konkrete Zahlen zu fassen. Jentzsch (2007) beispielsweise untersuchte empirisch, inwieweit sich das Datenschutzniveau sowie dessen Regulierung auf Wirtschaftsauskunfteien und die Kreditvergabe in verschiedenen Ländern auswirken. Dabei stellte sich heraus, dass bei einem stärkeren Datenschutz zumindest kein negativer Effekt zu beobachten war. Für eine konkretere Aussage waren die Daten jedoch von zu vielen anderen Einflussfaktoren abhängig.

Aus theoretischen Überlegungen heraus kann eine Laffer-Kurve des Datenschutzes hergeleitet werden, die im Folgenden diskutiert wird.

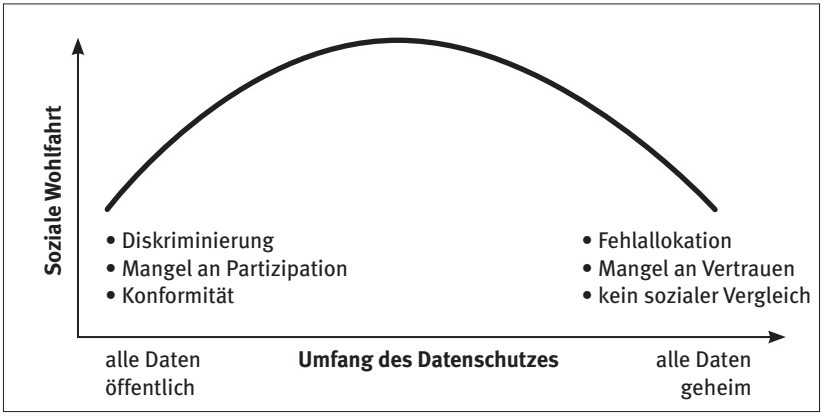

Abbildung 1: Laffer-Kurve des Datenschutzes (eigene Darstellung)

Die sogenannte Laffer-Kurve wurde ursprünglich von Arthur B. Laffer vorgeschlagen, um den Zusammenhang zwischen Steuersatz und Steuereinnahmen zu veranschaulichen (Schumann 1999). Die Steuereinnahmen sind demnach bei einem mittleren Steuersatz am höchsten. Abbildung 1 zeigt eine Adaption der Laffer-Kurve für den Datenschutz: Die soziale Wohlfahrt hängt hier vom Niveau des Datenschutzes ab, für den, wie bei der ursprünglichen Laffer-Kurve, ein mittlerer Wert die soziale Wohlfahrt maximiert.

Der Verlauf der Kurve wird mit theoretischen Überlegungen zur Situation an den Endpunkten begründet. Ein niedriges Datenschutzniveau kann zur Folge haben, dass Menschen in der Gesellschaft diskriminiert werden, da alle Informationen zu privaten oder sogar intimen Details öffentlich sind. Die Gefahr, dass jeder in der Gesellschaft über vermeintliche oder tatsächliche Fehltritte des Einzelnen informiert ist, führt zu einer Veränderung des Verhaltens hin zu mehr Konformität. Um Fehler zu vermeiden, nimmt zudem die Partizipation des Einzelnen an der Gesellschaft ab. Diese Effekte eines sehr niedrigen Datenschutzniveaus lassen sich zwar nur schwierig in ein ökonomisches Modell überführen, ein allgemeiner negativer Einfluss auf die soziale Wohlfahrt kann jedoch aus den oben genannten Argumenten abgeleitet werden.

Durch ein zu hohes Datenschutzniveau kann die soziale Wohlfahrt einer Gesellschaft ebenfalls sinken: Da im Falle einer Geheimhaltung aller Daten auch die Qualifikationen, Bedürfnisse und Wünsche der Wirtschaftssubjekte unbekannt sind, kann es zu Fehlallokationen durch Fehlbesetzungen am Arbeitsmarkt oder falsche oder zu wenige oder zu viel hergestellte Produkte kommen (Calzolari und Pavan 2006). Für manche Produkte ist zudem ein gewisses Vertrauen nötig, etwa bei Verträgen zwischen einem Kreditgeber und einem Kreditnehmer. Sind alle Daten geheim, kann dieses Vertrauen nicht durch Informationen über den Kreditnehmer, etwa seine Bonität, hergestellt werden. Das hat zur Folge, dass diese Produkte nicht oder nur zu unattraktiven Konditionen angeboten werden können (Stigler 1980). Verhaltensforscher argumentieren außerdem, dass die Leistungsbereitschaft von Wirtschaftssubjekten durch die Möglichkeit des sozialen Vergleichs steigt, der im Falle der vollständigen Geheimhaltung aller Daten ebenfalls nicht möglich ist.

Ziel der verbraucherpolitischen Akteure sollte es also sein, möglichst das mittlere Niveau des Datenschutzes zu realisieren, das die soziale Wohlfahrt maximiert. Die Wahl der richtigen Maßnahmen ist von Annahmen über den Status quo des Datenschutzes abhängig sowie von den Möglichkeiten, diesen Status zu verändern. Zentrale Fragen sind also, wo sich der Status quo des Datenschutzes im Laffer-Kurven-Modell befindet und ob die Optimierung dieses Niveaus durch Marktmechanismen erfolgen kann oder ob eine Regulierung erforderlich ist – und wenn ja, welcher Art diese sein kann.

3 Zu viel oder zu wenig Datenschutz?

Die Frage, ob das Datenschutzniveau in einer Gesellschaft zu niedrig oder zu hoch ist, hängt hauptsächlich davon ab, welches Niveau als ideal angesehen wird. Das Laffer-Kurven-Modell für den Datenschutz gibt schon deshalb keine Information darüber, weil schwierig zu definieren ist, was genau ein mittleres Datenschutzniveau ist. Dieser Aspekt wird in der Forschungsliteratur kontrovers diskutiert.

Autoren der Chicagoer Schule etwa argumentierten Anfang der 1980er-Jahre, dass die perfekte Information die Effizienz einer Ökonomie (und damit die soziale Wohlfahrt) erhöhe und somit erstrebenswert sei. Das Datenschutzniveau solle dementsprechend so niedrig wie möglich liegen (Posner 1981). Diese Argumentation stimmt nicht mit dem Laffer-Kurven-Modell überein. Dies könnte darin begründet sein, dass die Entwicklung der IT-Industrie und insbesondere des Internets erst einige Zeit später stattfand. Eine Konsequenz aus dieser Entwicklung ist die einfache Weiterleitung von Daten. Der Verbraucher hat unter Umständen keine Kontrolle und Übersicht über Daten, die er einer Firma anvertraut hat. Existieren keine Datenschutzrichtlinien, ist eine Sekundärnutzung der Verbraucherdaten, also etwa ein Weiterverkauf, problemlos möglich (Acquisti 2010). Neuere Arbeiten argumentieren daher differenzierter: Auf der einen Seite müssten gewisse Daten über Verbraucher verbreitet werden, um den Nutzen für den Einzelnen sowie als Folge davon die soziale Wohlfahrt zu maximieren, andererseits könnten Daten eines Verbrauchers auch in einer Weise missbraucht werden, die der sozialen Wohlfahrt schadet – etwa zur Versendung unerwünschter Werbung (Varian 1996).

Ein eher pragmatisches Argument für ein generell hohes Datenschutzniveau ist, dass die Beschaffung und Auswertung der Daten über Verbraucher mit Kosten verbunden ist. Diese Kosten können die Vorteile, die durch die gewonnenen Informationen entstehen, die jedoch im Voraus nicht bekannt sind, überwiegen. In einer Gesellschaft mit hohem Datenschutzniveau gäbe es eventuell keine Möglichkeit, die gewünschten Informationen zu beschaffen. Aus diesem Grund fielen auch keine Kosten für die Datenbeschaffung an, was der sozialen Wohlfahrt insgesamt zuträglich wäre (Hermalin und Katz 2006).

Langfristig ist jedoch davon auszugehen, dass solche Fehleinschätzungen auch bei geringem Datenschutzniveau nicht wiederholt werden, was dieses Argument entkräftet.

4 Regulierung oder Marktmechanismen?

Eine weitere kontrovers diskutierte Frage ist, ob das Datenschutzniveau durch den Markt oder durch Regulierung, also durch staatliche Stellen, festgesetzt werden sollte (Acquisti 2010). Für beide möglichen Szenarien gibt es Fallbeispiele: Während die Datenschutzpolitik in den USA vor allem auf eine Selbstregulierung des Marktes vertraut, wird der Datenschutz in der EU nach deutschen Vorbildern wie dem Bundesdatenschutzgesetz durch allgemeine Regelungen festgeschrieben.

In letzterem Fall misst man der Privatsphäre unabhängig von ökonomischen Überlegungen einen Wert zu, den es für sich genommen zu schützen gilt: Das Grundrecht auf Informationelle Selbstbestimmung legt fest, dass alle Bürgerinnen und Bürger ein Anrecht darauf haben, über ihre personenbezogenen Daten zu verfügen, und zu bestimmen, wer Zugang zu ihnen erhält (Steinmüller 2007). Wenn der Schutz personenbezogener Daten ein vorrangiges Ziel ist, hat sich gezeigt, dass ein regulativer Weg beschritten werden sollte, da Selbstregulierung oft nicht funktioniert. In den USA werden Daten von Verbrauchern regelmäßig ohne deren Zustimmung oder gar ohne deren Wissen gehandelt und analysiert.[1] Möglichkeiten, dies zu verhindern, existieren nicht oder werden von Verbrauchern nicht wahrgenommen (Acquisti 2010).

Falls das oberste Ziel jedoch die Optimierung der sozialen Wohlfahrt ist, ist die richtige Politik bezüglich des Datenschutzes nicht eindeutig. Einige Autoren argumentieren, dass Regulierung nur stattfinden sollte, wenn sich Marktme-

1 Dieses Manuskript ist vor Bekanntwerden des PRISM-Überwachungsprogramms entstanden.

chanismen in bestimmten Bereichen der Datenschutzregulierung als ineffizient erwiesen haben und die Regulierungsmaßnahme nicht so teuer ist, dass sie mehr kostet als die bestehende Ineffizienz des Marktes (Cate 2002, Cate et al. 2003, Rubin und Lenard 2001, Lenard und Rubin 2010). Striktere Datenschutzregeln können für Verbraucher allerdings auch ökonomische Vorteile haben (Acquisti 2010).

Die optimale Strategie bezüglich der Regulierung des Datenschutzes ist über rein ökonomische Argumente schwierig zu bestimmen, da es sowohl valide Hinweise gibt, dass ein erhöhter Datenschutz die Effizienz einer Ökonomie senkt, als auch, dass sie gesteigert wird. Zudem lassen sich die unterschiedlichen Aspekte des Datenschutzes sowie die unrechtmäßige Nutzung personenbezogener Daten schwer quantifizieren und zusammenfassen. Wie sehr ein Verbraucher vom Handel mit seinen personenbezogenen Daten betroffen ist, hängt auch davon ab, wie viel diese ihm wert sind. Diese Wertbemessung hat sich als schwierig erwiesen und bislang nicht zu eindeutigen Ergebnissen geführt (Acquisti 2010). Eine eindeutige Aussage darüber, wie viel Datenschutz aus gesamtgesellschaftlicher Perspektive genau richtig ist und wie dieses Niveau gewährleistet werden kann, kann momentan nicht getroffen werden.

Dieser Abschnitt wurde durch eine makroökonomische Perspektive motiviert. Dabei stand die Gesellschaft als Ganzes im Mittelpunkt. Im folgenden Abschnitt soll nun der einzelne Verbraucher in den Fokus gerückt werden. Dadurch kann mit Blick auf die Unterschiede jedes Einzelnen die Frage beantwortet werden, ob Datenschutz ein Luxusgut ist, das sich nicht alle Verbraucherinnen und Verbraucher leisten können. Schließlich können damit Umverteilungseffekte und Verteilungsgerechtigkeit diskutiert werden sowie die Auswirkungen, die der Datenschutz darauf hat.

5 Datenschutz als Luxusgut

Der Begriff Luxusgut impliziert, dass die Inanspruchnahme des Datenschutzes vom finanziellen und, damit oft verbunden, sozialen Status des Verbrauchers abhängig ist. In den folgenden Abschnitten wird der Frage nachgegangen, inwieweit die zuvor diskutierte Ausgestaltung der Datenschutzregulierung sowie das Niveau des Datenschutzes sich auf die Ausprägung und die Dynamik von sozialen Unterschieden in der Bevölkerung auswirken können. Dazu wird der Datenschutz zunächst theoretisch unter mikroökonomischen Gesichtspunkten betrachtet. Es folgt ein Fallbeispiel, das die Auswirkungen des Datenschutzes zeigt.

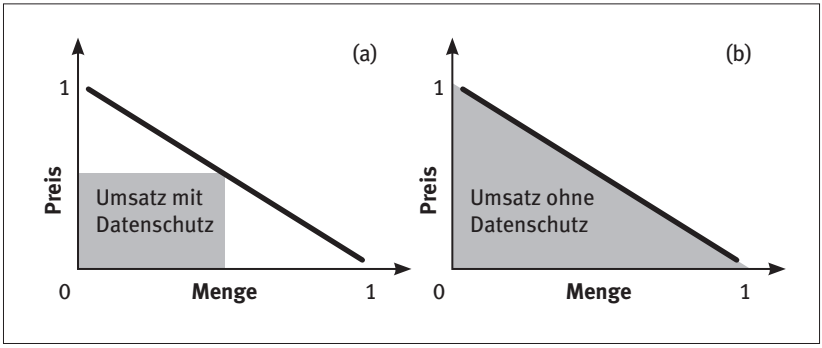

Abbildung 2: Datenschutz unter mikroökonomischer Betrachtung
(a) Nachfragefunktion sowie gewählter Preis bei verpflichtendem Datenschutz;
(b) Nachfragefunktion ohne Datenschutz, bei vollständiger Information
(eigene Darstellung).

Zur Darstellung der Rolle des Datenschutzes in einem mikroökonomischen Beispiel wird eine übliche lineare Nachfragekurve wie in Abbildung 2(a) verwendet. (Vgl. zu diesen und den folgenden Ausführungen Böhme und Koble (2007).) Zur Vereinfachung des Beispiels wird davon ausgegangen, dass der Anbieter über eine monopolistische Marktposition verfügt und unternehmerisch handelt, also seinen Gewinn und bei angenommenen vernachlässigbaren Grenzkosten seinen Umsatz zu maximieren versucht. In der Abbildung entspricht der Umsatz den Flächen unter der Kurve.

Ist Datenschutz verbindlich vorgeschrieben, so hat der Anbieter nur die allgemeine Information über die Nachfragekurve, kennt jedoch nicht die Zahlungsbereitschaft jedes einzelnen Kunden. Er muss also alle Kundinnen und Kunden gleich behandeln und kann nur einen Preis verlangen. Dieser Preis wird durch den Cournot-Punkt bestimmt, der den damit zu erzielenden Umsatz maximiert. Bei einer linearen Nachfragekurve wie in Abbildung 2(a) wird der Preis bei der Hälfte des Maximalpreises der Nachfragekurve liegen.

Gibt es keinen Datenschutz, ist also die Zahlungsbereitschaft jedes einzelnen Kunden bekannt oder aus personenbezogenen Daten erschließbar, so kann der Anbieter von jedem Kunden genau den Preis verlangen, den er zu zahlen bereit ist. Auf diese Weise ist eine perfekte Preisdiskriminierung möglich. Dies ist in Abbildung 2(b) zu sehen. Damit erzielt der Anbieter den maximal möglichen Umsatz dieser Nachfragefunktion. Aus diesen beiden Extrembeispielen lässt sich ein Maß für die Kosten beziehungsweise den Wert des Datenschutzes aus mikroökonomischer Perspektive ableiten: Es besteht aus der Differenz der beiden Umsätze.

In realistischen Fällen ist es jedoch so, dass Datenschutz weder verpflichtend ist noch vollständige Information über die Zahlungsbereitschaft jedes Kunden herrscht. Vielmehr gibt es Verbraucher, für die Datenschutz wichtig ist, und solche, für die er nebensächlich ist, über deren Zahlungsbereitschaft also vollständige Informationen vorliegen. In Deutschland etwa ist laut einer regelmäßig vom IT-Sicherheitsdienstleister Unisys durchgeführten Studie der Großteil der Bevölkerung an einem starken Datenschutz interessiert. Dies drückt sich zum Beispiel in der großen Sorge über den möglichen Missbrauch von personenbezogenen Daten (bei 68 Prozent der Befragten) aus oder in der Zustimmung zu gesetzlichen Regelungen sowie externer Begutachtung der Handhabung von Verbraucherdaten (81 beziehungsweise 69 Prozent). Die Studie geht ebenfalls auf die Abhängigkeit der Sorge über Datenschutz vom sozialen Status ein: Man kann erkennen, dass einkommensstärkere Verbrauchergruppen sowie solche mit höherem Bildungsgrad sich mehr über die Handhabung des Datenschutzes sorgen als sozial Schwächere (Unisys 2012).

Bezogen auf das mikroökonomische Modell bedeutet das Bedürfnis eines (großen) Teils der Bevölkerung nach Schutz der persönlichen Daten, dass der

Datenschutz für diejenigen Kunden optional ist, die ihn nachfragen. In diesem Fall ändert sich die Nachfragekurve, wie Abbildung 3 veranschaulicht:

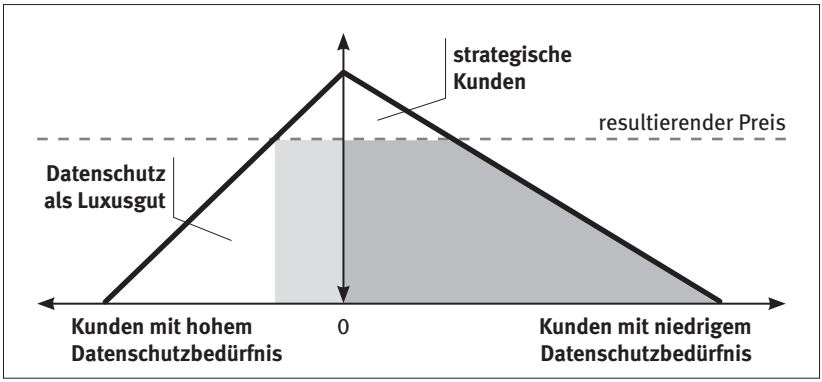

Abbildung 3: Nachfragekurve bei optionalem Datenschutz (eigene Darstellung).

Die Abbildung zeigt auf der linken Seite die Kunden, die ein hohes Datenschutzbedürfnis haben und rechts die Kunden mit niedrigem Datenschutzbedürfnis. Der Anbieter kann nun jedem Kunden entweder einen Festpreis anbieten oder – unter Aufweichung des Datenschutzes – genau die Zahlungsbereitschaft jedes einzelnen Kunden bedienen. Der Preis des Produkts wird also bei Beachtung des Datenschutzes über dem des Produkts im Falle eines verbindlichen Preises liegen. Das ist so, weil es strategische Kunden gibt: Kunden mit niedrigem Datenschutzbedürfnis können den Datenschutz für sich nutzen, um ihre höhere Zahlungsbereitschaft zu verschleiern. Der Anbieter kann also nicht den vollen Umsatz ausschöpfen, was Auswirkungen auf den Preis für Kunden mit hohem Datenschutzbedürfnis hat. Dies bedeutet zudem, dass Kunden mit hohem Datenschutzbedürfnis stets den maximalen Preis der Kunden zahlen müssen, denen Datenschutz unwichtig ist. Kunden mit geringerer Zahlungsbereitschaft und einem hohen Bedürfnis nach Datenschutz werden am Markt nicht bedient.

Aus diesem Modell ergibt sich Datenschutz notwendigerweise als Luxusgut. Nur Kunden mit hoher Zahlungsbereitschaft werden bedient, andere müssten den Datenschutz aufgeben, um das Gut ebenfalls konsumieren zu können.

6 Ein Fallbeispiel

Nach den bisherigen theoretischen Überlegungen lautet die Frage, ob sich auch in der Praxis ein Beispiel dafür finden lässt, dass Datenschutz ein Luxusgut ist, beziehungsweise wie sich optionaler Datenschutz in der Realität auswirkt. Da es weder möglich ist, die theoretischen mikroökonomischen Transaktionen in der realen Welt zu messen, noch die Laffer-Kurve des Datenschutzes mit empirischen Daten nachzuvollziehen, wird ein Fallbeispiel herangezogen: Peer-to-Peer-Kredite.

Dabei handelt es sich um internetbasierte Marktplattformen, auf der private Kreditgeber und Kreditnehmer gegenübergestellt werden. In Deutschland sind in diesem Bereich vor allem die smava GmbH und auxmoney GmbH aktiv. Kreditnehmer geben Gesuche ab, indem sie ein zu finanzierendes Projekt sowie unter Umständen den Kreditnehmer selbst beschreiben und einen gewünschten Zinssatz anbieten. Außerdem können noch weitere freiwillige Angaben gemacht werden, um potenzielle Kreditgeber zu gewinnen. Der Plattformbetreiber reichert diese Informationen an, indem er Bonitätsauskünfte der Kreditnehmer hinzufügt. Alle diese Daten können von jedem potenziellen Kreditgeber eingesehen werden, sie sind also öffentlich. Kreditgeber können dann entscheiden, welchem Kreditnehmer sie wie viel Kredit gewähren. Üblicherweise wird jedes Gesuch von mehreren Kreditgebern gedeckt und jeder Kreditgeber verteilt sein Budget auf mehrere Kreditnehmer. Diese Aufteilung sorgt für eine Verteilung der Risiken und ist der Grund für die Bezeichnung Peer-to-Peer-Kredit.

Diese Plattformen werden gezielt als Finanzierungsart vermarktet, bei der Personen mit schlechter Bonität einen Kredit bekommen, etwa indem damit geworben wird, dass auch Personen ohne Sicherheiten Kredite erhalten können (auxmoney GmbH 2013). Ein potenzieller Kreditnehmer muss dafür zumindest einige personenbezogene Daten offenlegen. Datenschutz ist hier insofern ein Luxusgut, als dass Personen mit guter Bonität von einer Bank einen Kredit bekommen, die ihre personenbezogenen Daten nicht veröffentlicht. Eine statistische Analyse der freiwilligen Angaben ergab zudem, dass es einen negativen Zusammenhang zwischen Bonität und der Ausführlichkeit dieser An-

gaben gibt. Kreditnehmer mit schlechterer Bonität veröffentlichen demnach mehr personenbezogene Daten. Dies führt jedoch nicht dazu, dass sich die Kreditkonditionen bemerkbar verbessern (Böhme und Pötzsch 2010).

7 Fazit und Ausblick

Die mikroökonomischen Überlegungen sowie das Fallbeispiel haben gezeigt, dass Datenschutz oftmals ein Luxusgut ist. Der Verzicht auf Datenschutz kann zu günstigeren Konditionen führen oder den Konsum eines Produkts überhaupt erst ermöglichen. Daraus lässt sich in Hinblick auf weitere Forschung die Arbeitsthese aufstellen, dass Datenschutz, sofern er optional ist, soziale Unterschiede verstärkt. Um Datenschutz nachfragen zu können, muss eine bestimmte Zahlungsbereitschaft oder eine Mindestbonität vorliegen. Als weitere These ließe sich untersuchen, ob verbindlicher Datenschutz diese sozialen Unterschiede nivellieren kann.

Die gesamtgesellschaftlichen Überlegungen haben gezeigt, dass beim Datenschutz aus ökonomischer Perspektive ein erheblicher Forschungsbedarf besteht. Auf makroökonomischer Ebene ist nicht geklärt, welche Auswirkungen Datenschutzregulierung und die Höhe des Datenschutzes haben. Neben den Auswirkungen auf die soziale Wohlfahrt sollten auch andere Aspekte, wie etwa die Verteilungsgerechtigkeit, untersucht werden.

8 Handlungsempfehlungen

Die wichtigste Handlungsempfehlung dieses Beitrags lautet, das Thema Datenschutz verstärkt aus ökonomischer Perspektive zu betrachten. Wie bereits

in der Einleitung angemerkt, wird Datenschutz bisher hauptsächlich aus juristischer oder technischer Sicht diskutiert. Eine ökonomische Perspektive kann dabei in vielerlei Hinsicht hilfreich sein. Zunächst ließe sich der ansonsten meist abstrakt betrachtete Wert des Datenschutzes quantifizieren. Zudem wäre eine Untersuchung der Auswirkungen des Datenschutzniveaus sowie dessen Regulierung auf die Wohlfahrt beziehungsweise die Ausprägung der sozialen Unterschiede innerhalb der Gesellschaft möglich. Hier besteht dringender Nachholbedarf in Forschung, Ausbildung und Praxis.

Zur Abschätzung der Auswirkungen des Datenschutzes auf die soziale Wohlfahrt beziehungsweise die Verteilungsgerechtigkeit sollten Studien durchgeführt werden. Dies kann im Rahmen von Rechtsfolgenabschätzungen neuer Datenschutzgesetze geschehen – nicht zuletzt auch aus aktuellem Anlass der geplanten EU-Datenschutzgrundverordnung.

Die Datenschutzregulierung in Deutschland sollte im Detail überprüft werden. Insbesondere sollte einzelnen Aspekten der konkreten Ausgestaltung von Datenschutzregulierung auf mögliche Umverteilungseffekte nachgegangen werden. Hier kann, je nach Ergebnis der Überprüfung, Änderungsbedarf entstehen.

Bei der Überprüfung der konkreten Ausgestaltung der Datenschutzregulierung kann zudem die Frage erörtert werden, ob Bereiche hohen Datenschutzniveaus diesen generell obligatorisch ausgestalten sollten. Die mikroökonomische Betrachtung des Datenschutzes lässt darauf schließen, dass durch eine solche Maßnahme potenziell unerwünschte Verteilungseffekte der Datenschutzregulierung gelindert werden können.

Literatur

Acquisti, Alessandro. 2010. The Economics of Personal Data and the Economics of Privacy. In: *The Economics of Personal Data and Privacy: 30 Years after the OECD Privacy Guidelines,* Paris, 1. Dezember 2010. http://www.oecd.org/sti/ieconomy/46968784.pdf.

auxmoney GmbH. 2013. *Kredite von Privat an Privat – auxmoney.* http://www.auxmoney.de (Zugriff: 30. Januar 2013).

Böhme, Rainer und Sven Kolbe. 2007. On the Viability of Privacy-Enhancing Technologies in a Self-regulated Business-to-consumer Market: Will Privacy Remain a Luxury Good? In: *Workshop on the Economics of Information Security (WEIS)*. Pittsburgh, PA: Carnegie Mellon University, 7. Juni 2007. http://weis2007.econinfosec.org/papers/30.pdf.

Böhme, Rainer und Stefanie Pötzsch. 2010. Social Lending aus der Sicht des Datenschutzes. In: *Sicherheit 2010: Sicherheit – Schutz und Zuverlässigkeit ; Konferenzband der 5. Jahrestagung des Fachbereichs Sicherheit der Gesellschaft für Informatik e.V. (GI), 5.-7. Oktober 2010 in Berlin*, hg. von Felix Freiling, 317–328. Bonn: Ges. für Informatik.

Calzolari, Giacomo und Alessandro Pavan. 2006. On the optimality of privacy in sequential contracting. *Journal of Economic Theory* 130, Nr. 1: 168–204. doi:10.1016/j.jet.2005.04.007.

Cate, Fred H. 2002. Principles of protecting privacy. *Cato Journal* 22, Nr. 1: 33–57.

Cate, Fred. H., Robert E. Litan, Michael Staten und Peter Wallison. 2003. *Financial privacy, consumer prosperity, and the public good: Maintaining the balance*. Washington, DC: Brookings Institution Press.

Hermalin, Benjamin E. und Michael L. Katz. 2006. Privacy, property rights and efficiency: The economics of privacy as secrecy. *Quantitative Marketing and Economics* 4, Nr. 3: 209–239. doi:10.1007/s11129-005-9004-7.

Jentzsch, Nicola. 2007. *Financial privacy. An international comparison of credit reporting systems*. Berlin; New York: Springer.

Krempl, Stefan und Martin Holland. 2012. Eklat um die Stiftung Datenschutz im Bundestag. *heise online*. 14. Dezember 2012. http://heise.de/-1769077 (Zugriff: 22. Januar 2013).

Lenard, Thomas M. and Paul H. Rubin. 2010. In defense of data: Information and the costs of privacy. *Policy & Internet* 2, Nr. 1: 149–183

Steiner, Falk und Jürgen Kuri. 2013. EU-Datenschutzreform: Die Schlacht um den Schutz der Privatsphäre. *heise online*. 15. Januar 2013. http://heise.de/-1783758 (Zugriff: 22. Januar 2013).

Posner, Richard A. 1981. The Economics of Privacy. *The American Economic Review* 71, Nr. 2: 405–409.

Rubin, Paul H. and Thomas M. Lenard. 2001. *Privacy and the Commercial Use of Personal Information*. Dordrecht: Kluwer Academic Publishers.

Schumann, Jochen. 1999. *Grundzüge der mikroökonomischen Theorie*. Berlin: Springer.

Steinmüller, Wilhelm. 2007. Das informationelle Selbstbestimmungsrecht – Wie es entstand und was man daraus lernen kann. *Recht der Datenverarbeitung* 13, Nr. 4: 158–161.

Stigler, Georg J. 1980. An Introduction to Privacy in Economics and Politics. *The Journal of Legal Studies* 9, Nr. 4: 623-644.

Unisys, 2012. *Unisys Security Index: Germany.* Online: http://www.unisys-securityindex.com/usi/germany (Zugriff: 30. Januar 2013).

Varian, Hal. 1996. *Economic Aspects of Personal Privacy*. Berkeley, CA. http://citeseerx.ist.psu.edu/viewdoc/download;jsessionid=5AD01379 15A3A930228A41B340E9F385?doi=10.1.1.39.1701&rep=rep1&type=pdf (Zugriff: 16. Juli 2013).

Wilkens, Andreas. 2012. Klarnamenzwang: Datenschützer droht Facebook mit Zwangsgeld. *heise online*. http://heise.de/-1770733 (Zugriff: 22. Januar 2013).

Datenschutz und Cloud Computing aus Verbrauchersicht

Georg Borges und Sascha Adler

Abstract

Die Nutzung von Diensten, die auf Cloud Computing beruhen, hat sich mittlerweile für viele Verbraucherinnen und Verbraucher zu einer Alltäglichkeit entwickelt. Oft ist ihnen aber nicht klar, dass sich hinter den betreffenden Diensten, denen sie ihre Daten anvertrauen, Cloud-Dienste verbergen und die Daten in Rechenzentren auf der ganzen Welt verarbeitet werden. Dies ist jedoch für die Einhaltung der datenschutzrechtlichen Anforderungen relevant, die in bestimmten Konstellationen auch für den Verbraucher maßgeblich sind, wenn er nämlich personenbezogene Daten mit Hilfe von Cloud-Diensten verarbeitet.

1 Einleitung – Die Bedeutung von Cloud-Diensten für den Verbraucher

Laufend werden unter der Bezeichnung Cloud Computing neue Dienste präsentiert, die sich sowohl an Privatleute als auch an Unternehmen richten. Weltweit nutzen Milliarden Menschen schon heute derartige Angebote und speichern eigene und fremde Daten bei Diensten wie iCloud, T-Cloud oder Dropbox. Viele Verbraucher sind sich zugleich aber nicht dessen bewusst, dass sie Daten „in die Cloud" übertragen. Für sie spielt es oft keine Rolle, wie der Dienst technisch ausgestaltet wird.

Zugleich nimmt die Sensibilität gegenüber unerwünschtem Zugriff auf Daten zu, die Angaben über persönliche Verhältnisse enthalten. Datenschutz, Datensicherheit und Identitätsschutz gewinnen daher immer mehr an Bedeutung und entwickeln sich zu gewichtigen Faktoren, wenn es um die Auswahl des „richtigen" Dienstes oder Anbieters geht. Für den Verbraucher stellt sich einerseits die Frage, welchem Anbieter er seine Daten bedenkenlos anvertrauen kann. Dabei ist eine Datenverarbeitung durch den Cloud-Anbieter im Einklang mit den gesetzlichen Vorgaben Grundvoraussetzung eines vertrauenswürdigen Dienstes. Andererseits ist der Verbraucher, wenn er seinerseits die Daten anderer Personen unter Nutzung von Cloud-Diensten verarbeiten will, selbst für die Einhaltung der datenschutzrechtlichen Vorgaben verantwortlich und setzt sich im Falle der Nichtbeachtung Haftungsrisiken aus.

Im Folgenden werden wichtige Rechtsfragen des Datenschutzes bei der Nutzung von Cloud-Diensten durch Verbraucher erörtert. Dabei ist zwischen der Nutzung zur Verarbeitung eigener Daten, beispielsweise bei der Speicherung eigener Dokumente, und derjenigen zur Verarbeitung fremder Daten, beispielsweise beim Betrieb eines Blogs, zu unterscheiden.

2 Was ist Cloud Computing

Trotz der medial vermittelten, scheinbaren Allgegenwärtigkeit der Cloud-Dienste, ist häufig unklar, was genau unter Cloud Computing zu verstehen ist. Die Vielgestaltigkeit der verfügbaren Dienste erschwert zudem eine prägnante Definition des Begriffs.

Die bekannteste Definition des Begriffes Cloud Computing stammt aus dem Jahr 2009 und wurde vom US-amerikanischen „National Institute of Standards and Technology“ (NIST) entwickelt. Die Definition wurde seitdem mehrfach überarbeitet und liegt nun in der (vorerst) finalen Form vor: „Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. [...]” (Grance und Mell 2011).

Cloud Computing bezeichnet somit eine Kategorie von Diensten, die überall verfügbar ist und dem Nutzer je nach Bedarf die benötigten Ressourcen aus einem Gesamtpool zur Verfügung stellen kann. Die Dienste skalieren dabei automatisch mit den Anforderungen, ohne dass ein Eingreifen des Nutzers erforderlich wäre.

Die dynamische Anpassung an die Anforderungen des Nutzers wird dadurch erreicht, dass ein Anbieter seine Ressourcen einer Vielzahl von Nutzern zur Verfügung stellt, wobei jedem Nutzer Zugriff auf einen Teil der Hardware gestattet wird (BITKOM 2009, 49). Die Zuteilung erfolgt mittels Virtualisierung (BITKOM 2009, 71). Dem Nutzer wird ein abgegrenzter Teil der Gesamtinfrastruktur als virtuelle Maschine zugewiesen, für die nur er Zugriffsrechte hat (BITKOM 2009, 49). Die Zuteilung der Ressourcen ist dabei während des Betriebes jederzeit und fast augenblicklich veränderbar (Bundesamt für Sicherheit in der Informationstechnik 2012, 19; European Network and Information Security Agency 2009, 14). Die Abrechnung erfolgt meist auf Basis der Nutzungsintensität, wobei typischerweise nach Zeitdauer oder Umfang der genutzten Ressourcen abgerechnet wird (BITKOM 2009, 46).

Cloud Computing kann dem Nutzer von Cloud-Diensten erhebliche Vorteile gegenüber herkömmlicher Datenverarbeitung bieten. Der Nutzer hat jederzeit und – die entsprechende Datenverbindung vorausgesetzt – überall Zugriff auf die Ressourcen des Anbieters und muss bei kostenpflichtigen Diensten nur für die Leistungen bezahlen, die er auch in Anspruch genommen hat. Er kann leistungshungrige Anwendungen ohne entsprechend potente Hardware nutzen und kommt, sofern die Verarbeitung nur einmalig oder periodisch erfolgen muss, zudem ohne Vorhaltung entsprechender Ressourcen für den Bedarfsfall aus.

Seit der Einführung der ersten Cloud-Dienste hat sich eine Vielzahl von unterschiedlichen Services etabliert, die sich in verschiedene Kategorien einteilen lassen. Die Einordnung erfolgt zunächst danach, auf welcher Ebene der Nutzer Zugriff auf die ihm zugewiesene Hardware des Anbieters erhält. Dienste nach dem Muster „Infrastructure-as-a-Service" (IaaS) umfassen die Bereitstellung kompletter virtueller Maschinen, auf denen der Nutzer dann beliebige Software wie auf einem physikalisch vorhandenen Rechner ablaufen lassen kann (BSI 2012, 17). Diese Dienste stellen im Ergebnis vorrangig Rechenleistung und/oder Speicherplatz bereit (Arbeitskreise Technik und Medien 2011, 17; Borges und Brennscheidt 2012, 47; Grünwald und Döpkens 2011, 287; Heckmann 2011, Kap. 9 Rn. 588; Maisch und Seidl 2012, 7; Nägele und Jacobs 2010, 282; Niemann und Paul 2009, 445). Die Zugriffsrechte reichen hier sehr weit, so dass der Nutzer nicht auf ein bestimmtes Betriebssystem oder Ähnliches festgelegt ist. Wird dagegen eine vorgefertigte Umgebung, also z.B. ein Betriebssystem oder eine Entwicklungsumgebung angeboten, so spricht man von „Platform-as-a-Service" (PaaS) (Heckmann 2011, Kap. 9 Rn. 589; Maisch und Seidl 2012, 7; Nägele und Jacobs 2010, 282; Niemann und Paul 2009, 444). Die von Verbrauchern wohl am häufigsten genutzte Variante bildet das Modell „Software-as-a-Service" (SaaS).[1] Hierbei werden einzelne Anwendungen über den Anbieter bereitgestellt. Die für die Nutzung der Anwendung notwendigen Rechenprozesse und Datenspeicherungen erfolgen dann in der Cloud. Der Nutzer kann somit über das Internet die Anwendung nutzen, wobei seine Hardware lediglich für die Darstellung der Benutzeroberfläche ausrei-

1 Vor allem Dienste, die eine Datenspeicherung in der Cloud erlauben, erfreuen sich großer Beliebtheit – laut BITKOM (2012) speicherten im April 2012 vier von fünf Internetnutzern Daten in der Cloud.

chen muss (Nägele und Jacobs 2010, 282; Niemann und Paul 2009, 445). Dies erlaubt, eine Verarbeitung auch mit schwächeren Geräten durchzuführen, z.B. mit Mobiltelefonen oder Tablets. Weitere Dienste nach dem Schema „X-as-a-Service“[2] erwecken oftmals (durchaus gewollt) den Anschein einer neuen Dienstekategorie, lassen sich aber meist in eine der drei beschriebenen Kategorien einordnen.

Cloud-Dienste können außerdem als Public Cloud oder Private Cloud ausgestaltet sein. Im Rahmen einer Public Cloud teilen sich dabei mehrere Nutzer die beim Anbieter vorgehaltene Hardware, während Private Clouds speziell für einzelne Nutzer, typischerweise Unternehmen, betrieben werden. Private Clouds ähneln in ihrer Struktur dem klassischen Outsourcing (Birk und Wegener 2010, 642; Borges und Brennscheidt 2012, 47; Heidrich und Wegener 2010, 803). Für Verbraucher sind im Regelfall nur Public Clouds relevant, die mit anderen Nutzern gemeinsam genutzt werden.

Die wirtschaftliche Bedeutung des Cloud Computing wird allgemein als sehr hoch eingeschätzt.[3] Viele Unternehmen nutzen Cloud-Dienste, um ihre IT-Kosten zu senken. Der flexible Bezug von Rechenleistung im Wege des Cloud Computing ist insofern ein starker Wettbewerbsvorteil, schafft aber auch Abhängigkeiten in Bezug auf Verfügbarkeit und Sicherheit der Dienste. Je nach Anforderungen an die Unternehmens-IT stehen die Auslagerung von Prozessen, die Datenspeicherung und Verarbeitung oder die Nutzung externer Rechenleistung im Vordergrund. Auch der Trend zu mobiler Datenverarbeitung wäre ohne Cloud Computing kaum denkbar. Die begrenzten Ressourcen mobiler Endgeräte machen eine ausgelagerte Datenverarbeitung oftmals unumgänglich.

Längst verwenden auch viele Verbraucherinnen und Verbraucher täglich Cloud-Dienste. Social-Media-Plattformen wie Facebook und Twitter werden von Milliarden Menschen genutzt.[4] Online-Speicher wie Dropbox, Skydrive oder Google Drive werden dienstlich wie privat eingesetzt, um Dokumente

2 Auch „Everything-as-a-Service“; Beispiele sind „Business-Process-as-a-Service“, „Storage-as-a-Service“, „Security-as-a-Service“ und unzählige mehr.
3 Der BITKOM (2013) rechnet für den deutschen Markt in den kommenden Jahren mit einem jährlichen Wachstum von deutlich über 30 Prozent.
4 Allein Facebook soll im Mai 2013 ca. 1,1 Milliarden aktive Mitglieder gehabt haben (Kirch 2013).

immer und überall verfügbar zu machen. Cloud-basierte Textverarbeitung wie Office 365 oder Googles Texte und Tabellen machen die Anschaffung lokal vorgehaltener Software obsolet. E-Mail-Dienste wie Googles Gmail oder Microsofts Hotmail werden von jeher oft ausschließlich online genutzt und stellen einen der häufigsten Anwendungsfälle für Cloud Computing dar.

Einen neueren Anwendungsfall bilden Musik-Streaming-Dienste (Spotify, Google Music, Apple iCloud/iRadio), bei denen entweder eigene Musik hinterlegt werden kann, die zuvor erworben wurde, oder aber Fremdinhalte (werbefinanziert oder gegen monatliches Entgelt) zum Abruf bereitstehen.

Einen weiteren Trend bildet die Speicherung von Computerspielen und verwandten Inhalten. So wird die kommende Konsolengeneration (Playstation 4, XBOX One) die Cloud als Quelle für Spiele nutzen (T-Online 2013). Auch für Windows- und Mac-basierte Systeme gibt es mit Diensten wie Steam Cloud-basierte Plattformen, die den Bezug von Spielen, die Speicherung von Daten und die Kommunikation mit anderen Spielern ermöglichen (Valve 2013). Viele Anbieter arbeiten außerdem intensiv an einer Verknüpfung ihrer Dienste untereinander. So verknüpft z.B. Google seine Dienste dergestalt, dass mit den Google-Anwendungen erstellte Dokumente direkt in Google Drive gespeichert und ohne vorheriges Herunterladen mit Gmail versendet werden können (Google 2013).

3 Rechtlich relevante Strukturen und Beteiligte

Aus rechtlicher Sicht stellt sich die Nutzung eines Cloud-Dienstes im einfachsten Fall als Zweipersonenverhältnis dar. Der Cloud-Nutzer verwendet in diesem Falle die Dienste des Cloud-Anbieters, wobei zwischen den Parteien ein Vertragsverhältnis besteht, das die genaueren Nutzungsbedingungen regelt und gegebenenfalls durch gesetzliche Vorschriften ergänzt wird.

In der Praxis sind oftmals weitere Beteiligte einbezogen. Häufig werden nicht ausschließlich eigene Daten des Nutzers an den Cloud-Anbieter übermittelt. Vielmehr verarbeitet der Nutzer vielfach auch Daten Dritter mithilfe von Cloud-Diensten. Dabei sind auch die Rechtsbeziehungen zwischen Nutzer und Drittem zu beachten. Auch auf Seiten des Cloud-Anbieters werden meist weitere Akteure stehen, derer sich der Anbieter zur Erfüllung der vertraglichen Pflichten bedient (Borges und Brennscheidt 2012, 48f.). Gerade im Falle auftretender Lastspitzen müssen kleinere Anbieter häufig Kapazitäten externer Dritter abrufen (Niemann und Hennrich 2010, 691). In Bezug auf diese Unterauftragnehmer stellen sich insbesondere Fragen bezüglich der datenschutzrechtlichen Zulässigkeit der Weitergabe von Daten und der Gewährleistung der Datensicherheit.

4 Cloud Computing und Datenschutz

Der wohl rechtlich derzeit problematischste Aspekt des Cloud Computing liegt im Bereich des Datenschutzrechts, das auch von Verbrauchern beachtet werden muss, sofern Sie sich im Anwendungsbereich der Normen bewegen. Maßgeblich ist hier derzeit das Bundesdatenschutzgesetz (BDSG). Auf europäischer Ebene befindet sich die Datenschutz-Grundverordnung in Planung, die zukünftig europaweit das Datenschutzrecht vereinheitlichen soll und daher auch das BDSG ablösen wird. Diese wird aber voraussichtlich frühestens 2016 in Kraft treten.

4.1 Fallgruppen

Für Verbraucherinnen und Verbraucher, die Cloud-Dienste nutzen, ist das Datenschutzrecht in zwei grundsätzlich zu unterscheidenden Fällen relevant.

Nutzt der Verbraucher Cloud-Dienste, um ausschließlich eigene Daten zu verarbeiten, so ist nur er selbst von einer etwaigen datenschutzrechtlich relevanten Verarbeitung betroffen. So beispielsweise, wenn er Dokumente, die Angaben

über seine Person enthalten, in einen Cloud-Speicherdienst hochlädt. Er ist in diesem Fall Adressat der Schutzfunktion des Datenschutzrechts. Der Cloud-Anbieter ist als Verarbeiter der Daten für die Einhaltung der datenschutzrechtlichen Bestimmungen verantwortlich (1. Fallgruppe).

Anders sind Fälle zu beurteilen, in denen der Verbraucher fremde, personenbezogene Daten verarbeitet und dazu Cloud-Dienste nutzt, beispielsweise beim Betreiben eines Blogs unter Verwendung von Angaben über dritte Personen. Bei der Nutzung eines derartigen Dienstes ist der Verbraucher derjenige, der eine Datenverarbeitung durchführt und daher selbst dafür verantwortlich, die datenschutzrechtlichen Regelungen zu beachten (2. Fallgruppe).

Der Cloud-Anbieter ist bei letzterer Konstellation neben dem Verbraucher ebenfalls für die Einhaltung des Datenschutzrechts verantwortlich. Wird eine Auftragsdatenverarbeitung vereinbart (vgl. 4.5), so trifft ihn keine eigene Verantwortlichkeit gegenüber demjenigen, dessen Daten verarbeitet werden.

4.2 Der sachliche Anwendungsbereich des BDSG

4.2.1 Verarbeitung personenbezogener Daten

Das BDSG ist gemäß seinem § 1 Abs. 2 anwendbar, wenn personenbezogene Daten erhoben, verarbeitet oder genutzt werden. Unter den Begriff der Verarbeitung fallen gem. § 3 Abs. 4 BDSG auch die Speicherung und Übermittlung von Daten, die bei der Nutzung eines Cloud-Dienstes stets notwendig sind. Der Begriff des personenbezogenen Datums ist in § 3 Abs. 1 BDSG definiert. Es handelt sich dabei um all jene Daten, die „Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person“ enthalten. Die Person, der die Daten zugeordnet werden können, ist Betroffener i.S.d. § 3 Abs. 1 BDSG.

Bei einer Verarbeitung durch gewerbliche Nutzer ist das BDSG daher beispielsweise immer dann anwendbar, wenn Daten wie Adressen oder Vertragsdetails in Bezug auf Mitarbeiter, Kunden oder Dritte an den Cloud-Anbieter übermittelt werden. Dies ist jedenfalls dann der Fall, wenn ein Unternehmen die Verarbeitung oder Speicherung entsprechender Daten „in die Cloud“ auslagert.

Erfasst werden auch sämtliche Angaben über Privatpersonen sowie Bilder, Videos (Dammann 2011, § 3 BDSG Rn. 4) und Ortsangaben, die in Verbindung zu einer Person stehen (Dammann 2011, § 3 BDSG Rn. 11). Bei der Nutzung von Cloud-Diensten durch Verbraucher kommt es daher ebenfalls häufig zu einer Übermittlung und Verarbeitung personenbezogener Daten.

4.2.2 Ausnahme bei persönlichen oder familiären Tätigkeiten

Wenn Verbraucher personenbezogene Daten mithilfe von Cloud-Diensten verarbeiten, ist grundsätzlich Datenschutzrecht anwendbar. § 1 Abs. 2 Nr. 3 BDSG enthält allerdings eine Ausnahme vom Anwendungsbereich des BDSG, sofern die Daten nur für persönliche oder familiäre Tätigkeiten erhoben, verarbeitet oder genutzt werden. Dies stellt aber keine generelle Ausnahme privater Datenverarbeitung vom Anwendungsbereich des Datenschutzrechts dar. „Privat" in diesem Sinne meint eine Datenverarbeitung, die außerhalb einer unternehmerischen Tätigkeit erfolgt. Der EuGH hat die Anwendbarkeit des EU-Datenschutzrechts auf Grundlage der Datenschutz-Richtlinie[5] auch für eine private Tätigkeit bejaht (EuGH, Urt. v. 06.11.2003, Az.: C-101/01 – „Lindqvist"). Da auch das BDSG auf Grundlage der Richtlinie 95/46/EG erlassen wurde, ist daher die Ausnahme des § 1 Abs. 2 Nr. 3 BDSG in der Praxis so auszulegen, dass nicht jede private (nicht-unternehmerische) Tätigkeit als „persönliche oder familiäre Tätigkeit" angesehen werden kann. Vielmehr kommt es darauf an, ob nach der Verkehrsauffassung eine rein persönliche oder familiäre Nutzung vorliegt (Dammann 2011, § 1 BDSG Rn. 151). Anhaltspunkt kann z.B. der betroffene Personenkreis sein (Dammann 2011, § 1 BDSG Rn. 152). Auch Personen, die kein Unternehmen betreiben oder im privaten Bereich handeln, müssen daher bei der Datenverarbeitung in der Cloud die Bestimmungen des BDSG beachten, sofern sie den Rahmen des rein Persönlichen oder Familiären überschreiten.

Dies ist insbesondere auch beim eingangs erwähnten Beispiel der zweiten Fallgruppe zutreffend: Der Betrieb eines Blogs dient regelmäßig nicht ausschließlich persönlichen oder privaten Zwecken, sondern zielt gerade auch

5 Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. EG Nr. L 281 vom 23.11.1995, 31.

auf eine Außenwirksamkeit des Handelns ab. In derartigen Fällen ist daher keine Ausnahme vom sachlichen Anwendungsbereich des Datenschutzrechts gegeben.

4.2.3 Ermittlung der verantwortlichen Stelle

Wer für die Einhaltung der datenschutzrechtlichen Bestimmungen Sorge zu tragen hat, richtet sich danach, wer als verantwortliche Stelle i.S.d. § 3 Abs. 7 BDSG anzusehen ist.

Wenn ein Verbraucher persönliche Daten anderer Personen verarbeitet und diese Datenverarbeitung nicht mehr als persönliche oder familiäre Tätigkeit angesehen werden kann (2. Fallgruppe), ist er selbst eine verantwortliche Stelle i.S.d. § 3 Abs. 7 BDSG. Gibt er die Daten nun an den Cloud-Anbieter weiter, der diese im Wege der Auftragsdatenverarbeitung verarbeitet, so bleibt der Verbraucher weiterhin verantwortliche Stelle und muss die entsprechenden Bestimmungen beachten (siehe dazu noch unten, 4.5). Liegt keine Auftragsdatenverarbeitung vor, ist neben dem Verbraucher, der die Daten übermittelt, der verarbeitende Anbieter ebenfalls verantwortliche Stelle.[6]

Anders stellt sich die Situation dar, wenn der Verbraucher ausschließlich eigene Daten verarbeitet (1. Fallgruppe). Auch wenn die Definition der verantwortlichen Stelle insoweit keine Einschränkung vorsieht, kann der Betroffene bei Verarbeitung eigener Daten nicht verantwortliche Stelle sein (Dammann 2011, § 3 BDSG Rn. 226). Er darf seine Daten vielmehr uneingeschränkt selbst verarbeiten. Gibt er die Daten an einen Cloud-Anbieter weiter, so ist dieser grundsätzlich verantwortliche Stelle und muss die Einhaltung der datenschutzrechtlichen Anforderungen sicherstellen. Der Verbraucher ist dagegen Betroffener, da seine Daten verarbeitet werden.

6 Eine Mehrzahl verantwortlicher Stellen ist trotz des Wortlauts des § 3 Abs. 7 BDSG möglich (Dammann 2011, § 3 BDSG Rn. 226).

4.3 Internationaler Anwendungsbereich des BDSG

Bei der Beteiligung von internationalen Akteuren stellt sich außerdem die Frage nach dem internationalen Anwendungsbereich des deutschen Datenschutzrechts. Dieser ergibt sich aus § 1 Abs. 5 BDSG, wobei primärer Anknüpfungspunkt der Sitz der verantwortlichen Stelle gem. § 3 Abs. 7 BDSG ist, also desjenigen, der Daten selbst verarbeitet oder im Auftrag verarbeiten lässt.

4.3.1 Verbraucher als verantwortliche Stelle

Das BDSG folgt grundsätzlich dem so genannten Territorialitätsprinzip. Danach ist das Recht des Staates anwendbar, in dem die verantwortliche Stelle ihren Sitz hat, § 1 Abs. 2, 5 BDSG (Borges und Brennscheidt 2012, 58). Handelt es sich beim Verbraucher um die verantwortliche Stelle (2. Fallgruppe), so ist daher der Wohnort des Verbrauchers ausschlaggebend, das BDSG ist anwendbar, wenn der Verbraucher seinen Wohnsitz in Deutschland hat.

4.3.2 Cloud-Anbieter als verantwortliche Stelle

Ist der Cloud-Anbieter allein (1. Fallgruppe) oder neben dem Verbraucher (2. Fallgruppe, wenn keine Auftragsdatenverarbeitung vorliegt) verantwortliche Stelle, so ist auf dessen Unternehmenssitz abzustellen. Entsprechend des Territorialitätsprinzips ist das BDSG dann anwendbar, wenn der Cloud-Anbieter seinen Sitz in Deutschland hat. Zudem kommt aber auch eine Anwendbarkeit dann in Betracht, wenn der Anbieter seinen Sitz in einem anderen Staat der EU oder des Europäischen Wirtschaftsraums (EWR)[7] hat und die Daten durch eine Niederlassung im Inland verarbeitet (Borges und Brennscheidt 2012, 58).

Befindet sich der Sitz des Anbieters außerhalb der EU und des EWR, ist das BDSG dennoch anwendbar, wenn eine Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten in Deutschland erfolgt, § 1 Abs. 5 S. 2 BDSG.

---

7 Der Europäische Wirtschaftsraum (EWR) umfasst die Staaten der EU sowie Island, Liechtenstein und Norwegen.

Dies wurde bei klassischen Formen der Datenverarbeitung immer dann angenommen, wenn die zur Verarbeitung dienenden Server in Deutschland belegen sind (Borges und Brennscheidt 2012, 59). Im Falle des Cloud Computing hilft diese Betrachtungsweise jedoch nur begrenzt weiter. Häufig existiert eine Vielzahl von dynamisch miteinander verknüpften Servern in unterschiedlichen Staaten. Daher kann der genaue Belegenheitsort der Daten oft nicht ermittelt werden (Borges und Brennscheidt 2012, 59) oder er verschiebt sich im Rahmen der Neuzuweisung von Ressourcen. Teilweise wird daher vertreten, das deutsche Datenschutzrecht sei bereits dann anwendbar, wenn sich das Angebot des Cloud-Anbieters erkennbar an Internetnutzer im Inland richte (Nägele und Jacobs 2010, 290; Pötters 2013, 1056). Im Einzelnen besteht hier noch Klärungsbedarf.[8]

4.4 Rechtliche Rahmenbedingungen nach dem BDSG

Ist das BDSG anwendbar, so unterliegt die Verarbeitung personenbezogener Daten einer Reihe von Beschränkungen, die von der jeweils verantwortlichen Stelle, also dem Verbraucher bzw. Cloud-Anbieter, beachtet werden müssen. Dadurch soll sichergestellt werden, dass das Persönlichkeitsrecht und das Recht auf informationelle Selbstbestimmung der Betroffenen gewahrt bleiben (Gola und Schomerus 2012, § 4 BDSG Rn. 5).

Jede verantwortliche Stelle darf daher personenbezogene Daten nur dann verarbeiten, wenn die Voraussetzungen des BDSG erfüllt sind. Dies gilt einerseits für den Verbraucher, der Daten Dritter verarbeitet (2. Fallgruppe), andererseits auch für den Cloud-Anbieter, sofern er selbst verantwortliche Stelle ist (1. Fallgruppe bzw. 2. Fallgruppe bei Nichtvorliegen einer Auftragsdatenverarbeitung). Bei Verstößen gegen die Regelungen des BDSG drohen jeder verantwortlichen Stelle gem. §§ 43, 44 BDSG Bußgelder oder bis zu zwei Jahre Freiheitsstrafe.

8 Siehe ausführlich zur Anwendbarkeit des BDSG Borges und Brennscheidt (2012, 58 ff.).

4.4.1 Einwilligung des Betroffenen

Das BDSG erlaubt eine Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten gem. § 4 Abs. 1 BDSG grundsätzlich nur dann, wenn eine Rechtsvorschrift dies erlaubt oder eine Einwilligung des Betroffenen vorliegt, weshalb man auch von einem „Verbot mit Erlaubnisvorbehalt" spricht (Gola und Schomerus 2012, § 4 BDSG Rn. 3).

Bei einer Verarbeitung eigener personenbezogener Daten unter Nutzung von Cloud-Diensten muss der Verbraucher daher, da er selbst Betroffener der Datenverarbeitung ist (1. Fallgruppe), dem Cloud-Anbieter als verantwortliche Stelle seine Einwilligung zur Verarbeitung erteilen.

Verarbeitet der Verbraucher dagegen personenbezogene Daten Dritter (2. Fallgruppe), muss der Verbraucher, wenn er Cloud-Dienste zur Verarbeitung nutzt, grundsätzlich die Einwilligung der betroffenen Personen einholen. Dabei muss jeder Betroffene sowohl der Verarbeitung durch den Verbraucher (z.B. Nutzung der Daten im Blog des Verbrauchers) als auch derjenigen durch den Cloud-Anbieter (Übermittlung und Verarbeitung der Daten) zustimmen. Ist der Cloud-Anbieter in diesem Fall mangels Vorliegen einer Auftragsdatenverarbeitung ebenfalls verantwortliche Stelle, so trifft auch ihn die Verantwortlichkeit, wenn er Daten ohne wirksame Einwilligung verarbeitet. Für den Anbieter wird dabei aber nur selten nachvollziehbar sein, ob eine Einwilligung erteilt wurde. Diese Problematik stellt sich beim Vorliegen einer Auftragsdatenverarbeitung nicht, was deren Bedeutung verdeutlicht.

Die Einholung einer wirksamen Einwilligung ist in der Praxis oft problematisch, da diese hinreichend bestimmt und freiwillig erklärt worden sein muss (Simitis 2011, § 4a BDSG Rn. 62, 77). Die Bestimmtheit ist dabei nur gewahrt, wenn der konkrete Übermittlungsempfänger – im Falle der Nutzung eines Cloud-Dienstes durch den Verbraucher also der jeweilige Cloud-Anbieter – benannt werden kann (Simitis 2011, § 4a BDSG Rn. 82). Dem Anbieter muss wiederum eine Einwilligung für die Verarbeitung und Übermittlung an eventuelle Unterauftragnehmer erteilt werden. Dadurch wird die Flexibilität der Auslagerung in die Cloud entscheidend konterkariert. Teilweise wird das Datenschutzrecht daher als Hemmnis für Cloud Computing angesehen (Nägele und Jacobs 2010, 290).

4.4.2 Gesetzliche Erlaubnis

Liegt keine Einwilligung vor, so kann die Datenverarbeitung dennoch zulässig sein, wenn eine gesetzliche Erlaubnis zur Verarbeitung vorliegt. In Frage kommt dabei insbesondere § 28 BDSG, der in begrenztem Umfang eine Datenverarbeitung für eigene Geschäftszwecke erlaubt, sofern diese notwendig ist. Der Begriff des „Geschäftszwecks" ist insofern weit auszulegen und bildet den Gegenpol zu Daten, die ausschließlich zu familiären oder persönlichen Zwecken verarbeitet werden (Simitis 2011, § 28 BDSG Rn. 31).

Eine Erlaubnis nach § 28 BDSG liegt insbesondere dann vor, wenn fremde Daten notwendig im Rahmen eines Vertragsverhältnisses (§ 28 Abs. 1 Nr. 1 BDSG) oder zur Wahrung eigener berechtigter Interessen (§ 28 Abs. 1 Nr. 2 BDSG) verarbeitet werden. Bei einer Verarbeitung eigener Daten des Verbrauchers (1. Fallgruppe) kann sich für den Cloud-Anbieter eine gesetzliche Erlaubnis daraus ergeben, dass er sonst seine vertraglichen Verpflichtungen gegenüber dem Verbraucher nicht erfüllen kann.

Was gem. § 28 Abs. 1 Nr. 2 BDSG im berechtigten Interesse des Verbrauchers liegt, wenn dieser Daten Dritter unter Nutzung von Cloud-Diensten verarbeitet (2. Fallgruppe), ergibt sich nicht aus der Vorschrift und ist einzelfallabhängig zu bestimmen.[9] Teilweise wird insofern angenommen, dass schon eine Kostenersparnis des Cloud-Nutzers ein berechtigtes Interesse i.S.d. § 28 Abs. 1 S. 1 Nr. 2 BDSG darstellen und eine Datenverarbeitung rechtfertigen könne (so Niemann und Paul 2009, 449; Splittgerber und Rockstroh 2011, 2182; vgl. dazu auch Borges und Brennscheidt 2012, 71). Das Interesse an einer Kostenersparnis über das Bestimmungsrecht des Betroffenen zu stellen, wird allerdings zu Recht überwiegend abgelehnt (Gaul und Köhler 2011, 2232; Nägele und Jacobs 2010, 290; Schulz 2010, 78).

9 Eine Aufzählung von Beispielen findet sich u. a. bei Taeger (2010, § 28 BDSG Rn. 66).

4.4.3 Übermittlung in Drittstaaten

Neben dem Erfordernis einer Einwilligung oder gesetzlichen Erlaubnis sieht das BDSG zusätzliche Anforderungen vor, wenn Daten ins außereuropäische Ausland transferiert werden sollen. Viele große Cloud-Anbieter haben ihren Sitz in den USA oder einem anderen Staat außerhalb des EWR.

Eine Übermittlung der Daten in Drittstaaten außerhalb des Europäischen Wirtschaftsraums (EWR) darf gem. § 4b Abs. 2 BDSG im Regelfall nur dann erfolgen, wenn im Drittland ein angemessenes Datenschutzniveau besteht (Borges und Brennscheidt 2012, 71) oder wenn der Betroffene der Übermittlung in ein Drittland ohne entsprechendes Schutzniveau zustimmt. Um eine wirksame diesbezügliche Einwilligung zu erhalten, muss die verantwortliche Stelle den Betroffenen allerdings über die Risiken informieren, die bei einer Übermittlung bestehen (Simitis 2011, § 4c BDSG Rn. 9), was oftmals problematisch ist. Es ist daher für die verantwortliche Stelle – gleichgültig ob diese der Verbraucher oder Cloud-Anbieter ist – von großem Interesse, das Vorliegen eines angemessenen Datenschutzniveaus nachzuweisen. Dies kann auf verschiedene Arten erfolgen.[10]

Für einige Staaten hat die EU-Kommission das Vorliegen eines angemessenen Datenschutzniveaus gem. Art. 25 Abs. 6 Datenschutz-Richtlinie verbindlich festgestellt.[11] Gerade Anbieter aus den USA haben sich häufig den sogenannten „Safe Harbour Principles“ unterworfen und garantieren dadurch ein angemessenes Datenschutzniveau (Däubler 2010, § 4b BDSG Rn. 15; Simitis 2011, § 4b BDSG Rn. 70). Eine weitere Möglichkeit besteht in der Einbeziehung der von der Kommission veröffentlichten EU-Standardvertragsklauseln (ABl. EU Nr. L 39 vom 12.2.2010, 5 ff.), wobei diese Variante aber nur dann in Betracht kommt, wenn der Cloud-Anbieter eine derartige Option in seinen Verträgen anbietet. Verhandlungsspielraum besteht diesbezüglich für Verbraucher typischerweise nicht.

---

10 Zu den verschiedenen Möglichkeiten ausführlich auch Borges und Brennscheidt (2012, 72 f.).

11 Bisher wurde dies für Andorra, Argentinien, Australien, Färöer, Guernsey, Israel, die Insel Man, Jersey, Kanada, Neuseeland, die Schweiz und Uruguay festgestellt; die komplette Liste mit allen Entscheidungen der Kommission kann bei der Europäischen Kommission (2013) eingesehen werden.

4.5 Die Auftragsdatenverarbeitung beim Cloud Computing

4.5.1 Problemstellung

Nutzt der Verbraucher einen Cloud-Dienst um personenbezogene Daten Dritter zu verarbeiten (2. Fallgruppe), so muss er die Daten notwendigerweise an den Cloud-Anbieter übermitteln (Borges und Brennscheidt 2012, 62). Bereits die Übermittlung der Daten bedarf datenschutzrechtlich der Rechtfertigung. Gleiches gilt für die Verarbeitung, die der Cloud-Anbieter in technischer Hinsicht für den Verbraucher durchführt, z.B. indem er die vom Verbraucher übermittelten Texte automatisiert in den Blog des Verbrauchers integriert.

Der Verbraucher kann im Hinblick auf die Übermittlung und die vom Cloud-Anbieter durchgeführte Verarbeitung die Anforderungen an eine Einwilligung nur schwer erfüllen. In dieser müsste er nämlich genau darlegen, wie und von wem die Daten verarbeitet werden. Der Verbraucher hat aber meist keinen Einblick, in welcher Weise der Cloud-Anbieter, an den er beispielsweise die Daten Dritter zum Zweck der Aufnahme in seinen Blog übermittelt, mit den Daten verfährt oder an welche Subunternehmer die Daten im Zuge der Verarbeitung übermittelt werden.

4.5.2 Auftragsdatenverarbeitung als Privilegierung

Das Erfordernis der wenig praktikablen Einwilligung entfällt, wenn von der gesetzlichen Fiktion (Dammann 2011, § 3 BDSG Rn. 244) des § 3 Abs. 8 S. 3 BDSG Gebrauch gemacht wird. Innerhalb der Auftragsdatenverarbeitung ist der Auftragnehmer demnach gegenüber dem Auftraggeber nicht als Dritter anzusehen. Vielmehr ist gemäß § 11 Abs. 1 BDSG allein der Auftraggeber für die Einhaltung der datenschutzrechtlichen Vorschriften verantwortlich.

Nutzt der Verbraucher Cloud-Dienste zur Verarbeitung fremder personenbezogener Daten und liegt eine Auftragsdatenverarbeitung vor, so verbleibt die Verantwortlichkeit für die Datenverarbeitung beim Verbraucher. Der Cloud-Anbieter gilt ihm gegenüber nicht als Dritter. Den Anbieter trifft daher keine eigene Verantwortlichkeit, sondern er fungiert als „verlängerter Arm“ des Auftraggebers (Borges und Brennscheidt 2012, 63; Gola und Schomerus 2012, § 11

BDSG Rn. 3). Eine datenschutzrechtlich relevante Übermittlung findet demnach ebenfalls nicht statt (Petri 2011, § 11 BDSG Rn. 43). Die Situation ist insofern mit derjenigen vergleichbar, dass der Verbraucher die Daten ohne Beteiligung des Cloud-Anbieters selbst verarbeitet. Sind die Voraussetzungen einer Auftragsdatenverarbeitung erfüllt, ist somit keine gesonderte Einwilligung der Betroffenen mehr erforderlich. Der Verbraucher kann die Daten vielmehr wie bei einer internen Verarbeitung behandeln, so dass – abgesehen von den aus der Auftragsdatenverarbeitung erwachsenden Pflichten – kein zusätzlicher Aufwand entsteht, der die Vorteile einer Verarbeitung in der Cloud konterkarieren könnte.

4.5.3 Voraussetzungen der Auftragsdatenverarbeitung

Damit der Verbraucher bei der Verarbeitung von Daten Dritter eine Auftragsdatenverarbeitung mit dem Cloud-Anbieter wirksam vereinbaren kann, muss er den Anbieter gemäß § 11 Abs. 2 BDSG sorgfältig auswählen, wobei er die vom Anbieter getroffenen technischen und organisatorischen Maßnahmen berücksichtigen muss. Die entsprechenden Maßnahmen ergeben sich aus § 9 BDSG und der Anlage zu § 9 S. 1 BDSG. Sie beinhalten unter anderem Vorkehrungen zum Schutz der Daten vor Verlust, vor unbefugtem Zugriff und vor einer Verarbeitung, die von den Vorgaben des Auftraggebers abweicht.

Der Vertrag über die Auftragsdatenverarbeitung muss schriftlich geschlossen werden,[12] wobei die in § 11 Abs. 2 S. 2 Nr. 1 – 10 BDSG vorgegebenen Punkte geregelt werden müssen. Dazu zählen insbesondere „der Gegenstand und die Dauer des Auftrags“ (Nr. 1), „der Umfang, die Art und der Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten, die Art der Daten und der Kreis der Betroffenen“ (Nr. 2) und „die nach § 9 [BDSG] zu treffenden technischen und organisatorischen Maßnahmen“ (Nr. 3).

Bei einer Auftragsdatenverarbeitung außerhalb des EWR ergibt sich zusätzlich die Problematik, dass § 3 Abs. 8 S. 3 BDSG seinem Wortlaut nach eine

12 Dies soll eine gesetzliche Schriftform darstellen, die bei Fehlen gem. § 125 BGB zur Nichtigkeit des Vertrages führt (so Gola und Schomerus 2010, § 11 BDSG Rn. 17; Müglich 2009, 483; Petri 2011, § 11 BDSG Rn. 64; Wedde 2010, § 11 BDSG Rn. 32; a.A.: Gabel 2010, § 11 BDSG Rn. 54; vgl. zur Problematik des Schriftformerfordernisses auch Borges und Brennscheidt 2012, 65).

Auftragsdatenverarbeitung nur in der EU oder dem EWR zulässt. Nach einem Beschluss der EU-Kommission kann eine solche Verarbeitung außerhalb der EU oder dem EWR aber dennoch erfolgen, wenn der Anbieter die EU-Standardvertragsklauseln akzeptiert (ABl. EU Nr. L 39 vom 12.2.2010, 5 ff.). In der Literatur wird jedoch diskutiert, welche Voraussetzungen darüber hinaus erfüllt sein müssen. Teilweise wird die analoge Anwendung der Vorschriften über die Auftragsdatenverarbeitung befürwortet (Weichert 2010, 686), teilweise wird gefordert, dass die Voraussetzungen einer Übermittlung gem. §§ 4b, 4c BDSG erfüllt sein müssen (Borges und Brennscheidt 2012, 69). Nach beiden Ansichten muss jedenfalls festgestellt werden, dass im Empfängerland ein angemessenes Datenschutzniveau besteht (Borges und Brennscheidt 2012, 69; zur Übermittlung in Drittstaaten siehe oben, 4.4.3). Der Verbraucher muss insofern auch im Falle einer Auftragsdatenverarbeitung die für die Übermittlung in Drittstaaten geltenden Einschränkungen beachten.

4.5.4 Kontrollpflicht des Auftraggebers und Zertifizierung

Der Verbraucher hat sich in seiner Rolle als Auftraggeber gemäß § 11 Abs. 2 S. 4 BDSG außerdem von der Einhaltung der technischen und organisatorischen Maßnahmen regelmäßig zu überzeugen und das Ergebnis zu dokumentieren.

Bisher wurde überwiegend angenommen, dass zur Erfüllung dieser Kontrollpflicht eine Besichtigung und Überprüfung der Anlagen des Auftragnehmers vor Ort notwendig ist (Bergmann, Möhrle und Herb 2010, § 11 BDSG Rn. 48a). Dieses Erfordernis stellt allerdings den Cloud-Nutzer, insbesondere wenn es sich um einen Verbraucher handelt, oftmals vor beträchtliche Probleme. Gerade international agierende Cloud-Anbieter betreiben Rechenzentren in verschiedenen Erdregionen um Ausfallsicherheit zu gewährleisten und Latenzzeiten zu minimieren. Die Virtualisierung der Hardware führt wie beschrieben dazu, dass nicht zu ermitteln ist, wo genau die Daten physikalisch gespeichert und verarbeitet werden (Hennrich 2011, 552; Niemann und Hennrich 2010, 691; Pohle und Ammann 2009, 278; ähnlich Niemann und Paul 2009, 449). Daher müsste eine Kontrolle aller in Frage kommenden Anlagen durchgeführt werden (BITKOM 2009, 52; Heidrich und Wegener 2010, 806; im Ergebnis so auch Weichert 2010, 685). Zusätzlich fehlt dem Auftraggeber häufig die entsprechende

Expertise um selbst eine Kontrolle durchzuführen. Dies gilt umso mehr für kleinere Unternehmen und Verbraucher, die Cloud-Dienste nutzen.

Die Kontrolle muss allerdings nicht durch den Auftraggeber selbst durchgeführt werden (BITKOM 2009, 52; BSI 2012, 74; Eckhardt 2011, 187; Heckmann 2010, 107; Heidrich und Wegener 2010, 806; Niemann und Hennrich 2010, 691; Schuster und Reichl 2010, 42). So ist etwa die Überprüfung durch unabhängige, externe Dritte im Auftrag des Cloud-Nutzers ausreichend, wobei die Wirtschaftlichkeit dieses Ansatzes wegen der hohen Kosten aber fraglich ist (Borges und Brennscheidt 2012, 66 f.). Die derzeit gemeinhin favorisierte Lösung stellt die Zertifizierung von Cloud-Diensten dar (AG Rechtsrahmen des Cloud Computing 2012, 11 ff.; Arbeitskreise Technik und Medien 2011, 9; Borges und Brennscheidt 2012, 67; Duisberg et al. 2011, 40; Eckhardt 2011, 187; Heckmann 2010, 107; Hennrich 2011, 552; Marnau et al. 2011, 336; Schröder und Haag 2011, 149; Weichert 2010, 683). Unabhängige Dritte mit entsprechender Expertise bescheinigen dabei die Einhaltung der technischen und organisatorischen Voraussetzungen durch den Cloud-Anbieter und stellen ihm ein Zertifikat aus, mit dem er den entsprechenden Nachweis gegenüber seinen Nutzern erbringen kann. Die Zertifizierung erfolgt für jeden Anbieter einmalig anhand eines festen Prüfkataloges, teilweise sind anschließend wiederkehrende Überprüfungen vorgesehen.[13] Die Zertifizierung erfolgt auf Anfrage und Kosten des Cloud-Anbieters. Dieser erhält mit der Zertifizierung (angesichts der steigenden Sensibilität im Bereich des Datenschutzes) einen vermarktungsfähigen Mehrwert gegenüber nicht zertifizierten Wettbewerbern.

Der Verbraucher kann durch die Auswahl eines zertifizierten Anbieters sicherstellen, dass seiner Kontrollpflicht genüge getan ist (Borges und Brennscheidt 2012, 67) und die Übermittlung der Daten sowie deren externe Verarbeitung im Wege der Auftragsdatenverarbeitung keine selbstständige datenschutzrechtliche Relevanz besitzt.

Noch nicht abschließend geklärt ist, ob eine vorweggenommene Kontrolle den Anforderungen des § 11 Abs. 2 S. 4 BDSG genügen kann (vgl. Borges und Brenn-

13 Das „EuroCloud Star Audit SaaS“ ist beispielsweise 24 Monate lang gültig. Danach muss eine „Rezertifizierung“ durchgeführt werden (EuroCloud Deutschland_eco 2013).

scheidt 2012, 68; dies bejahend Weichert 2010, 683). Auch im Hinblick auf die kommende Datenschutz-Grundverordnung, die eine Zertifizierung vorsieht, erscheint diese aber derzeit als praktikables Mittel um eine wirksame Auftragsdatenverarbeitung zu gewährleisten (Borges und Brennscheidt 2012, 67 f.).

Wann es geeignete Zertifikate auf dem Markt geben wird, bleibt allerdings abzuwarten. Derzeit existieren zwar bereits diverse Cloud-Zertifikate,[14] diese bestätigen häufig aber nur die Einhaltung gewisser technischer Rahmenbedingungen, ohne konkret die Einhaltung datenschutzrechtlicher Bestimmungen zu garantieren. Teilweise sind die Prüfkriterien nicht vollständig offengelegt, so dass die Nachvollziehbarkeit der Überprüfung wegen fehlender Transparenz problematisch ist. Zertifizierungen, die von Datenschutzbehörden angeboten werden, sind insofern problematisch, als dass Zertifizierender und Kontrollinstanz identisch sind, was zu Interessenkonflikten führen kann.

5 Fazit und Handlungsempfehlungen

Wenn Verbraucher Daten mithilfe von Cloud-Diensten verarbeiten, müssen grundsätzlich zwei Konstellationen unterschieden werden:

Zunächst kann der Verbraucher selbst Betroffener sein, wenn er eigene Daten an einen Cloud-Anbieter zur Verarbeitung übermittelt. Er muss dem Cloud-Anbieter dann eine Einwilligung erteilen, damit der Anbieter seine Daten verarbeiten darf. Bei Erteilung seiner Einwilligung sollte der Verbraucher besonders aufmerksam sein und darauf achten, dass die Daten zu keinen anderen Zwecken als den für die Verarbeitung notwendigen verwendet werden dürfen. Insbesondere sollte keine Weitergabe an Dritte zulässig sein, die nicht

14 Beispiele sind das EuroCloud Star Audit SaaS (EuroCloud Deutschland_eco 2013), die Cloud Security Zertifizierung des TÜV Rheinland (TÜV Rheinland 2013) oder das Datenschutz-Gütesiegel des ULD Kiel (Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein 2013).

notwendig in den Verarbeitungsprozess einbezogen sind. Ohne Einwilligung kommt häufig auch eine Rechtfertigung des Cloud-Anbieters nach § 28 Abs. 1 Nr. 1 BDSG in Betracht, nach der aber die Daten nur in dem Maße verarbeitet werden dürfen, wie es zur Erfüllung der vertraglichen Pflichten des Anbieters erforderlich ist.

Die Verantwortung für die Einhaltung der datenschutzrechtlichen Bestimmungen trifft bei dieser Fallgruppe den Cloud-Anbieter. Für den Verbraucher ist zum Schutz der eigenen Daten aber dennoch wichtig, schon bei der Auswahl des Cloud-Anbieters darauf zu achten, dass der Anbieter ein angemessenes Datenschutzniveau garantieren kann. Gerade bei Anbietern, deren Sitz in einem Land außerhalb des EWR und nicht in einem Land liegt, für das von der europäischen Kommission ein vergleichbares Datenschutzniveau festgestellt wurde, kann dies nur bei einer erfolgten Selbstverpflichtung des Anbieters oder durch vertragliche Verpflichtung erfolgen.

Wenn der Verbraucher selbst unter Nutzung von Cloud-Diensten fremde personenbezogene Daten verarbeitet, wird er unter Umständen selbst zur verantwortlichen Stelle und muss die Vorgaben des Datenschutzrechts beachten. Hierbei muss er im Regelfall die Einwilligung der betroffenen Personen einholen, wobei sich diese auf die Verarbeitung der Daten durch den Verbraucher, die Übermittlung an und die Verarbeitung durch den Cloud-Anbieter beziehen muss. Zudem muss der Verbraucher sicherstellen, dass beim Cloud-Anbieter ein angemessenes Datenschutzniveau herrscht. Anders als bei erstgenannter Fallgruppe liegt dies hier allerdings nicht ausschließlich im eigenen Interesse, sondern ist notwendig, um eine Haftung gegenüber den Betroffenen zu vermeiden.

Eine wesentliche Vereinfachung für den Verbraucher ergibt sich, wenn der Cloud-Anbieter Auftragsdatenverarbeiter ist. Für die Übermittlung an und die Verarbeitung beim Anbieter ist dann keine gesonderte Einwilligung erforderlich. Die Wirksamkeit dieser zusätzlichen Einwilligung kann der Verbraucher aufgrund der begrenzten ihm zur Verfügung stehenden Informationen häufig nicht sicherstellen und setzt sich daher dem Risiko einer Haftung für die unzulässige Verarbeitung aus. Falls möglich, sollte der Verbraucher für derartige Verarbeitungsprozesse daher Cloud-Dienste nutzen, bei denen eine Auftragsdatenverarbeitung vereinbart werden kann.

Der Verbraucher hat dann dafür zu sorgen, dass die Voraussetzungen der Auftragsdatenverarbeitung vorliegen. Diese umfassen auch die Einhaltung der vom Cloud-Anbieter zu treffenden technischen und organisatorischen Maßnahmen gem. § 9 BDSG. Um sicherzustellen, dass die entsprechenden Anforderungen gewahrt sind, sollte der Verbraucher auf passende Zertifizierungen des Cloud-Anbieters achten, dessen Dienst er nutzen möchte. Da die verfügbaren Zertifizierungen momentan noch sehr uneinheitliche Bewertungskriterien aufweisen, sollte er zudem stets hinterfragen, ob eine vorhandene Zertifizierung explizit auch die Einhaltung der entsprechenden technischen und organisatorischen Maßnahmen beinhaltet.

Literatur

AG Rechtsrahmen des Cloud Computing. 2012. *Datenschutzrechtliche Lösungen für Cloud Computing: Ein rechtspolitisches Thesenpapier der AG Rechtsrahmen des Cloud Computing*. Berlin: Kompetenzzentrum Trusted Cloud. http://trusted-cloud.de/documents/Datenschutzrechtliche-Loesungen-fuer-Cloud-Computing.pdf (Zugriff: 28.10.2013).

Arbeitskreise Technik und Medien. 2011. Orientierungshilfe – Cloud Computing. http://www.datenschutz.rlp.de/downloads/oh/ak_oh_cloudcomputing.pdf (Zugriff: 16.10.2013).

Bergmann, Lutz, Roland Möhrle und Armin Herb. 2010. *Datenschutzrecht: Handkommentar, Bundesdatenschutzgesetz, Datenschutzgesetze der Länder und zum Bereichsspezifischen Datenschutz (41. Ergänzungslieferung)*. Stuttgart: R. Boorberg.

Birk, Dominik und Christoph Wegener. 2010. Über den Wolken: Cloud Computing im Überblick. *Datenschutz und Datensicherheit* 33: 641–645.

BITKOM. 2009. *Leitfaden Cloud Computing*. Berlin: BITKOM. http://www.bitkom.org/files/documents/BITKOM-Leitfaden-CloudComputing_Web.pdf (Zugriff: 16.10.2013).

—. 2012. Privatverbraucher treiben Cloud Computing. (1. April). http://www.bitkom.org/de/presse/74532_71699.aspx (Zugriff: 16.10.2013).

—. 2013. Umsatz mit Cloud Computing steigt auf fast 8 Milliarden Euro. (6. März). http://www.bitkom.org/de/presse/8477_75301.aspx (Zugriff: 16.10.2013).

Borges, Georg und Kirstin Brennscheidt. 2012. Rechtsfragen des Cloud Computing – ein Zwischenbericht. In: *Daten- und Identitätsschutz in Cloud Computing, E-Government und E-Commerce*, hg. von Georg Borges und Jörg Schwenk, 43–77. Berlin: Springer.

Bundesamt für Sicherheit in der Informationstechnik. 2012. Eckpunktepapier Cloud Computing. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindestanforderungen/Eckpunktepapier-Sicherheitsempfehlungen-CloudComputing-Anbieter.pdf?__blob=publicationFile (Zugriff: 16.10.2013).

Däubler, Wolfgang, Thomas Klebe, Peter Wedde und Thilo Weichert. 2010. *Bundesdatenschutzgesetz*. 3. Auflage. Frankfurt am Main: Bund-Verlag.

Dammann, Ulrich. 2011. In: *Bundesdatenschutzgesetz*. hg. von Spiros Simitis. 7., neu bearbeitete Auflage. Baden-Baden: Nomos.

Duisberg, Alexander, Jens Eckhardt, Waldemar Grudzien, Wulf Hartmann, Sven Hermerschmidt, Jörg Kebbedies, Günther Otte, Gabriele Sieck, Martina Vomhof, Matthias Weber und Andreas Weiss. 2011. IT-Gipfel 2011 – Rechtliche Anforderungen an Cloud Computing. (15. November). http://www.eurocloud.de/wp-content/blogs.dir/5/files/anford_recht_beicloud-computing_v1.pdf (Zugriff: 16.10.2013).

Eckhard, Jens. 2011. Rechtliche Aspekte des Cloud Computing. In: *Cloud Computing: Neue Optionen für Unternehmen: strategische Überlegungen, Konzepte und Lösungen, Beispiele aus der Praxis*, hg. von Christiana Köhler-Schute, 229–260. Berlin: KS-Energy-Verlag.

EuroCloud Deutschland_eco. 2013. EuroCloud Star Audit. http://www.saas-audit.de/428/faq/ (Zugriff: 16.10.2013).

Europäische Kommission. 2013. Commission decisions on the adequacy of the protection of personal data in third countries. http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm (Zugriff: 16.10.2013).

European Network and Information Security Agency (ENISA). 2009. Cloud Computing - Benefits, risks and recommendations for information security. http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment/at_download/fullReport (Zugriff: 16.10.2013).

Gabel, Detlev. 2010. In: *Kommentar zum BDSG und zu den Datenschutzvorschriften des TKG und TMG*. hg. von Jürgen Taeger und Detlev Gabel. Frankfurt am Main: Verlag Recht und Wirtschaft.

Gaul, Björn und Lisa-Marie Koehler. 2011. Mitarbeiterdaten in der Computer Cloud: Datenschutzrechtliche Grenzen des Outsourcing. *Betriebs-Berater* 66, Nr. 36: 2229–2236.

Gola, Peter, Christoph Klug, Barbara Körffer und Rudolf Schomerus. 2012. *Bundesdatenschutzgesetz*. München: Beck.

Google. 2013. Google Drive. http://www.google.com/drive/about.html (Zugriff: 16.10.2013).

Grance, Timothy und Peter Mell. 2011. *The NIST Definition of Cloud Computing*. Gaithersburg, MD: National Institute of Standards and Technology. http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf (Zugriff: 17.10.2013).

Grünwald, Andreas und Harm-Randolf Döpkens. 2011. Cloud Control? - Regulierung von Cloud Computing-Angeboten. *MultiMedia und Recht* 14, Nr. 5: 287–290.

Heckmann, Dirk. 2010. Cloud Computing in der öffentlichen Verwaltung? – Rechtliche Grenzen für eine Lockerung staatlicher Datenherrschaft. In: *Innovationen im und durch Recht*, hg. von Hermann Hill und Utz Schliesky, 97–111. Baden-Baden: Nomos.

Heckmann, Dirk, Hrsg. 2011. *juris Praxiskommentar Internetrecht*. 3. Auflage. Saarbrücken: juris.

Heidrich, Joerg und Christoph Wegener. 2010. Sichere Datenwolken - Cloud Computing und Datenschutz. *MultiMedia und Recht* 13, Nr. 12: 803–807.

Hennrich, Thorsten. 2011. Compliance in Clouds: Datenschutz und Datensicherheit in Datenwolken. *Computer und Recht* 27, Nr. 8: 546–552.

Kirch, Nico. 2013. Quartalszahlen: Immer mehr Menschen nutzen Facebook nur noch mobil. (6. Mai). http://www.socialmediastatistik.de/facebook-immer-mehr-menschen-nutzen-ausschliesslich-mobil/ (Zugriff: 16.10.2013).

Maisch, Michael Marc und Alexander Seidl. 2012. Cloud Government: Rechtliche Herausforderungen beim Cloud Computing in der öffentlichen Verwaltung. *Verwaltungsblätter für Baden-Württemberg* 33, Nr. 1: 7–12.

Marnau, Ninja, Norbert Schirmer, Eva Schlehan und Matthias Schunter. 2011. TClouds - Herausforderungen und erste Schritte zur sicheren und datenschutzkonformen Cloud. *Datenschutz und Datensicherheit* 35, Nr. 5: 333–337.

Müglich, Andreas. 2009. Datenschutzrechtliche Anforderungen an die Vertragsgestaltung beim eShop-Hosting – Anspruch, Wirklichkeit und Vollzugsdefizit. *Computer und Recht* 25, Nr. 7: 479–484.

Nägele, Thomas und Sven Jacobs. 2010. Rechtsfragen des Cloud Computing. *Zeitschrift für Urheber- und Medienrecht* 54, Nr. 4: 281–292.

Niemann, Fabian und Thorsten Hennrich. 2010. Kontrollen in den Wolken? – Auftragsdatenverarbeitung in Zeiten des Cloud Computings. *Computer und Recht* 26, Nr. 10: 686–691.

Niemann, Fabian und Jörg Alexander Paul. 2009. Bewölkt oder wolkenlos – rechtliche Herausforderungen des Cloud Computings. *Kommunikation & Recht* 12, Nr. 7/8: 444–452.

Petri, Thomas B. 2011. In: *Bundesdatenschutzgesetz*, hg. von Spiros Simitis. 7., neu bearbeitete Auflage. Baden-Baden: Nomos.

Pötters, Stephan. 2013. Beschäftigtendaten in der Cloud. *Neue Zeitschrift für Arbeitsrecht* 30, Nr. 19: 1055–1059.

Pohle, Jan und Thorsten Ammann. 2009. Über den Wolken... – Chancen und Risiken des Cloud Computing. *Computer und Recht* 25, Nr. 5: 273–278.

Schröder, Christian und Nils Christian Haag. 2011. Neue Anforderungen an Cloud Computing für die Praxis – Zusammenfassung und erste Bewertung der „Orientierungshilfe – Cloud Computing". *Zeitschrift für Datenschutz* 1, Nr. 4: 147–153.

Schulz, Sönke E. 2010. Cloud Computing in der öffentlichen Verwaltung - Chancen – Risiken – Modelle. *MultiMedia und Recht* 13, Nr. 2: 75–80.

Schuster, Fabian und Wolfgang Reichl. 2010. Cloud Computing & SaaS: Was sind die wirklich neuen Fragen? - Die eigentlichen Unterschiede zu Outsourcing, ASP & Co liegen im Datenschutz und der TK-Anbindung. *Computer und Recht* 26, Nr. 1: 38–43.

Simitis, Spiros. 2011. In: *Bundesdatenschutzgesetz*. hg. von Spiros Simitis. 7., neu bearbeitete Auflage. Baden-Baden: Nomos.

Splittgerber, Andreas und Sebastian Rockstroh. 2011. Sicher durch die Cloud navigieren - Vertragsgestaltung beim Cloud Computing. *Betriebs-Berater* 66, Nr. 36: 2179–2185.

T-Online. 2013. Die PS4 nutzt ebenfalls Cloud-Computing. (14. Juni). http://www.t-online.de/spiele/id_63847642/playstation-4-ps4-nutzt-wie-xbox-one-auch-cloud-computing.html (Zugriff: 16.10.2013).

Taeger, Jürgen. 2010. In: *Kommentar zum BDSG und zu den Datenschutzvorschriften des TKG und TMG*, hg. von Jürgen Taeger und Detlev Gabel. Frankfurt am Main: Verlag Recht und Wirtschaft.

TÜV Rheinland. 2013. Cloud Zertifizierung. http://www.tuv.com/de/deutschland/gk/consulting_informationssicherheit/strategische_informationssicherheit/zertifizierungen_cloud_security/zertifizierungen_cloud_security.html (Zugriff: 16.10.2013).

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein. 2013. Häufig gestellte Fragen zum Datenschutz-Gütesiegel des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein. https://www.datenschutzzentrum.de/faq/guetesiegel.htm (Zugriff: 16.10.2013).

Valve. 2013. Willkommen bei Steam. http://store.steampowered.com/about/ (Zugriff: 16.10.2013).

Vander, Sascha. 2010. Auftragsdatenverarbeitung 2.0? – Neuregelungen der Datenschutznovelle II im Kontext von § 11 BDSG. *Kommunikation & Recht* 13, Nr. 5: 292–298.

Wedde, Peter. 2010. In: Däubler, Wolfgang, Thomas Klebe, Peter Wedde und Thilo Weichert. 2010. *Bundesdatenschutzgesetz*. 3. Auflage. Frankfurt am Main: Bund-Verlag.

Weichert, Thilo. 2010. Cloud Computing und Datenschutz. *Datenschutz und Datensicherheit* 34, Nr. 10: 679–687.

Wybitul, Tim und Armin Fladung. 2012. EU-Datenschutz-Grundverordnung - Überblick und arbeitsrechtliche Betrachtung des Entwurfs. *Betriebs-Berater* 67, Nr. 8: 509–515.

Smart Meter: Strom sparen – Daten verschwenden?

Ulrich Greveler

Abstract

Intelligente Stromzähler (Smart Meter) erlauben es Stromkunden, detaillierte Informationen über den Stromverbrauch zu erhalten und zeit- und lastvariable Tarife zu nutzen. Für Energieversorger und Netzbetreiber können Metering-Daten die Abrechnungsprozesse erheblich vereinfachen, zudem können die Smart Meter wichtige Netzzustandsdaten liefern, die zur Stabilisierung und effizienten Nutzung eines intelligenten Energieverteilnetzes benötigt werden.

Metering-Daten sind jedoch nicht nur personenbezogene Abrechnungsdaten, sie erlauben erhebliche Einblicke in die private Lebensgestaltung der Stromkunden bis hinein in die Intimsphäre. Wird die Sensibilität der Daten unterschätzt oder ignoriert, werden datenschutz- und datensicherheitsfördernde Technologien nicht im erforderlichen Maße eingesetzt.

Der Beitrag zeigt die Sensibilität der Metering-Daten auf, ordnet diese in einen Rahmen rechtlicher wie technischer Eckpunkte ein und leitet daraus Empfehlungen an die verbraucherpolitischen Akteure ab.

1 Hintergrund

Die Bereitstellung eines effizienten und hoch verfügbaren Stromnetzes gehört zu den zentralen strompolitischen Zielen in Deutschland. Die Zähl- und Messtechnik unterliegt aktuell einem Technologiewandel, nachdem die Strom- und Gaszähler seit 2010 den neuen Anforderungen des Energiewirtschaftsgesetzes entsprechen müssen. Zudem werden zeit- und lastvariable Tarife absehbar den zukünftigen Energiemarkt im Zuge der Energiewende bereichern.

Die verstärkte Nutzung erneuerbarer Energien führt zu einer stärker fluktuierenden Stromerzeugung. Das Angebot muss mit der ebenfalls schwankenden Nachfrage in Deckung gebracht werden, um die Netzinfrastruktur effizient nutzen zu können und Netzinstabilitäten zu vermeiden.

Stromkunden können mithilfe von intelligenten Stromzählern (Smart Metern) detaillierte Informationen über ihren Stromverbrauch erhalten und sind – abhängig von der Qualität der ihnen zur Verfügung gestellten Daten – in der Lage, den Stromverbrauch zu optimieren, das heißt Energieabnahme und damit Kosten zu senken.

Der Einsatz von Smart Metering erlaubt zudem eine automatisierte Übertragung von Stromverbrauchsdaten an Energieversorger bzw. an Abrechnungsdienste. Die Rechnungsstellung kann dann in kleinen Intervallen und zeitnah zum Stromverbrauch erfolgen, ohne dass eine aufwändige manuelle Ablesung erfolgen muss.

Smart-Metering-Daten sind jedoch auch für Übertragungsnetzbetreiber (Energietransport zwischen Verteilnetzen) und Verteilnetzbetreiber (Energieverteilung zum Letztverbraucher) interessant. Aus granularen Verbrauchsdaten lassen sich grundsätzlich Netzzustandsdaten gewinnen, die zur Stabilisierung des Stromnetzes verwendet werden. Beispielsweise kann bei einem Überangebot an Energie durch Nutzung von Energiespeichern und steuerbaren Geräten ein Ausgleich vorgenommen werden. Beim zukünftigen intelligenten Stromnetz (Smart Grid) ist eine solche kommunikative Vernetzung von Stromerzeugern und -abnehmern integraler Bestandteil.

Aus den verschiedenen Nutzungsszenarien für Smart Meter ergeben sich unterschiedliche Anforderungen an die zu erhebenden Daten: Eine Messung des Stromverbrauchs und die Übertragung der Daten kann in großen Abständen (zum Beispiel monatlich) erfolgen, um eine Abrechnung gemäß starrer Tarife zu ermöglichen. Wird jedoch ein zeit- oder lastvariabler Tarif zugrundegelegt, muss die Messung in kurzen Abständen erfolgen (zum Beispiel stündlich oder viertelstündlich). Zur Gewinnung von Netzzustandsdaten ist unter Umständen eine feingranulare Messung und Datenübertragung bis in den Sekundentakt vorgesehen. Diese feingranularen Daten können aber auch für den Verbraucher selbst interessant sein, der bei hoher Datenauflösung in seinem Verbrauchsprofil einzelne Geräte und Verbrauchsaktivitäten und damit Hochenergieverbraucher identifizieren kann. Dadurch werden ihm energie- und damit kostenintensive Aktivitäten stärker bewusst und er kann darauf mit einer Verhaltensänderung reagieren.

2 Personenbezogenheit und Sensibilität der Daten

Die von Smart Metern erhobenen Daten zum Stromverbrauch stellen wie alle auf einen Haushalt bezogenen Verbrauchsdaten (zum Beispiel Gas, Wasser) grundsätzlich personenbezogene Daten dar. Das Recht auf informationelle Selbstbestimmung wird tangiert, wenn Stromverbrauchsdaten gemessen, übermittelt oder verarbeitet werden. Beim Datenschutzrecht wird von einem Verbot mit Erlaubnisvorbehalt ausgegangen. Die Erlaubnis kann durch Rechtsvorschrift oder Einwilligung des Betroffenen erfolgen.

Die Erlaubnis zur Datenerhebung und -verarbeitung ist beim Smart Metering entweder durch explizite Zustimmung im Rahmen eines Vertrages mit dem Energieversorger oder Messstellenbetreiber gegeben – oder liegt aufgrund des Energiewirtschaftsgesetzes (§21g) vor, das Erhebung, Verarbeitung und

Nutzung personenbezogener Daten mit Hilfe eines Smart Meters für bestimmte Zwecke (zum Beispiel Abrechnung, Netzzustandsbestimmung) erlaubt.

Während der Personenbezug der erhobenen Daten unstrittig und bei den beteiligten Akteuren bekannt ist, geht die Wahrnehmung der Sensibilität der erhobenen Daten auseinander. Eine Auswertung von Metering-Daten erlaubt viel mehr als nur eine Feststellung, welche Energiemenge eine Person (oder ein Haushalt) verbraucht. Je nach Auflösung der Daten können Rückschlüsse auf Lebensgewohnheiten (zum Beispiel Anwesenheitszeiten) oder identifizierbaren Aktivitäten (zum Beispiel kochen, duschen, schlafen) vorgenommen werden (Molina-Markham u. a. 2010).

So können bei einer Messauflösung von 15 Minuten folgende Lebensgewohnheiten einer im Haushalt lebenden Person ermittelt werden (Müller 2010):

- Zu welcher Uhrzeit geht sie zu Bett?
- Zu welcher Uhrzeit steht sie auf?
- Gibt es nächtliche Toilettenbesuche?
- Wie häufig wird gekocht?
- Wann verlässt sie das Haus, wann kehrt sie zurück?
- Verändern sich die Lebensgewohnheiten (Nachwuchs, Besuch)?

Bei feingranularen Daten (Aufzeichnung in Sekundenintervallen) sind sogar Rückschlüsse auf Bewegungsverhalten im Haushalt bis hin zur Identifizierung von eingeschalteten Fernsehprogrammen oder abgespielten Videofilmen aufgrund der Abhängigkeit des Energieverbrauchs von Bildschirmhelligkeitswerten möglich (Greveler, Justus und Löhr 2012a). Letztlich kann über die Identifizierung aller elektrischen Geräte und ihrer Parameter (Greveler, Justus und Löhr 2012b) der gesamte persönliche Lebensbereich, soweit er sich im Haushalt abspielt, rekonstruiert werden, und Einblicke bis in die Intimsphäre werden möglich:

- Welcher Film wurde zu einem bestimmten Zeitpunkt abgespielt? (Helligkeitsprofil)
- War ein Film zum Konsumzeitpunkt schon als DVD erschienen? (Abgleich des Zeitstempels)

- Geht nachts jemand an den Kühlschrank? (kurze Brenndauer des identifizierbaren Lämpchens)
- Wurden Lebensmittel eingekauft? (lange Brenndauer des Lämpchens)
- Ist Besuch gekommen? (elektrische Türklingel)
- Wurde der Besuch hereingelassen? (elektrischer Türöffner)
- Welche Person hat übernachtet? (Erkennung personenspezifischer Parameter zum Beispiel anhand des Lastprofils eines Durchlauferhitzers beim morgendlichen Duschen, ggf. Abgleich mit Facebook-Freundesliste, um einen ausreichend kleinen Suchraum zu gewinnen)
- Wird der PC eingeschaltet und genutzt – oder läuft nur der Bildschirmschoner? (Lastprofil der CPU)
- Hat die Haushaltshilfe staubgesaugt? Ist sie früher gegangen als abgerechnet?
- Feierten die Kinder eine Party? Bis wann?
- War die Ehefrau abends länger weg, als der Mann auf Dienstreise war? (Überwachung des eigenen Partners anhand der grafischen Übersichten, die den Stromkunden bereitgestellt werden)
- Ist eine Person erkrankt? (Verhaltensänderung, Erkennung medizinischer Geräte und ihrer Parameter)

Eine zusätzliche Brisanz erfährt der Einblick in private Lebensgewohnheiten, wenn die Daten mit anderen Datensammlungen verknüpft werden. So ließe sich beispielsweise aus den zusammengefassten Metering-Daten der Bewohner einer Stadt eine Liste von verdächtigen Personen generieren, die immer dann nach Hause gekommen waren, als eine bestimmte Deliktart verübt wurde (zum Beispiel Fahrzeug-Brandstiftung). Eine solche „Metering-Rasterfahndung“ wäre also mit geringem Personalaufwand allein durch geeignete Datenbankabfragen möglich.

3 Handlungsempfehlungen

Da im Rahmen der Schriftenreihe, in der dieser Beitrag erscheint, die Formulierung konkreter Handlungsempfehlungen vorgesehen ist, werden nun unter Bezugnahme auf die im vorherigen Abschnitt dargestellte Sensibilität der erhobenen Metering-Daten Empfehlungen an die verbraucherpolitischen Akteure abgeleitet.

3.1. Klassifikation analog zu Vorratsdaten vornehmen

Metering-Daten, insbesondere feingranulare Energieverbrauchsdaten, sind von Gesetzgeber ähnlich wie Telekommunikationsverkehrsdaten als besonders sensible Daten zu klassifizieren, da sie bis in die Intimsphäre hineinreichende inhaltliche Rückschlüsse erlauben. Dieser Bezug auf die Intimsphäre war ein wesentliches Merkmal, das das Bundesverfassungsgericht bewogen hatte, im Jahre 2010 die gesetzlichen Regelungen zur Vorratsdatenspeicherung zu kippen. Es sind daher dieselben Anforderungen an die Speicherung und Übermittlung von Metering-Daten zu stellen, wie sie das Bundesverfassungsgericht in seinem Urteil zur Vorratsdatenspeicherung für die Speicherung und Verarbeitung von Telekommunikationsverkehrsdaten festgelegt hat (Bundesverfassungsgericht 2010):

- Übermittlung und Nutzung der gespeicherten Daten ist grundsätzlich unter Richtervorbehalt zu stellen
- Gewährleistung eines besonders hohen Standards hinsichtlich der Datensicherheit
- Sanktionensystem, das bei Verstößen greift
- eine Speicherung über den Verwendungszweck hinaus ohne gesetzliche Grundlage, technisches Durchsetzen von Löschvorgaben

Metering-Daten dürfen daher ohne besondere gesetzliche Grundlage auch nicht auf Vorrat gespeichert und einer späteren rückwirkenden Auswertung zugänglich gemacht werden.

3.2 Privacy By Design berücksichtigen

Die Konzeption von Smart Grids (hier insbesondere die Integration von Netzsensoren) und von Metering-Infrastrukturen muss Anforderungen an den Datenschutz und die Kontrollmöglichkeiten der Letztverbraucher bereits in der Entstehungsphase berücksichtigen. Nachträgliche Reparaturen an der Infrastruktur (Privacy-Updates) sind ineffizient und fehlerbehaftet. Hier könnten sowohl der Gesetzgeber wie auch Branchenverbände aktiv werden, um einheitliche Mindestanforderungen an die Konzeption zu verabschieden. Diese sollten folgende Systemeigenschaften erzwingen:

- Selbstauskunftmöglichkeit des Letztverbrauchers über die ihn betreffenden gespeicherten Daten, ihre Sensibilität und weitere Verarbeitung bis hin zur Löschungsbestätigung
- Protokollierung jeder Weitergabe und Verarbeitung der Daten in einer Weise, die dem Letztverbraucher Einsichtnahme ermöglicht
- automatische Löschung der Daten bei Wegfall des Erhebungszweckes (zum Beispiel nach Generierung einer Rechnung oder nach Auswertung des Netzzustandes)
- pseudonymisierte Weitergabe an Abrechnungsdienstleister (zum Beispiel Rechnung anhand einer Zählernummer erstellen, die dann im verschlossenen Umschlag einem Kunden zugeordnet und weitergeleitet wird)
- anonyme Weitergabe von Netzzustandsdaten
- Auswertung von feingranularen Daten nur beim Letztverbraucher (im lokal installierten Smart Meter); Übertragung in Datenbanken auf abrechnungsrelevante Daten beschränken

3.3 Verbindliche Vorgaben an die IT-Sicherheit nicht nur beim Smart Meter

Neben organisatorischen Maßnahmen auf Seiten der beteiligten Akteure spielt die IT-Sicherheit der Metering-Komponenten eine entscheidende Rolle bei der Durchsetzung von Datenschutzanforderungen. Das Bundesamt für Sicherheit in der Informationstechnik hat mit der Definition eines *Schutzprofils für ein Smart Meter Gateway* bereits einen ersten wichtigen Schritt getan, um Anforderungen an die Sicherheitsarchitektur intelligenter Netze aufzustellen (BSI

2013). Sicherheitsvorgaben dürfen sich jedoch nicht allein auf das Gateway beschränken, das die Daten vom elektronischen Stromzähler an eine zentrale Stelle weiterleitet. Ebenso wichtig ist die Absicherung der Daten dort, wo sie in Datenbanken überführt und verarbeitet werden. Es ist daher ein ähnliches Schutzprofil für Systeme bei Abrechnungsdiensten, Netzbetreibern und Energieversorgern vorzusehen, die Metering-Daten speichern und verarbeiten.

3.4 Anforderungen an die Zustimmungspflicht beachten

Alle geschäftsfähigen Personen, die in einem Messstellenbereich leben oder sich dort regelmäßig aufhalten, müssen der Datenerhebung und -weitergabe zustimmen! Dies betrifft auch Ehepartner und Familienmitglieder von Vertragspartnern in Privathaushalten. Es genügt nicht, dass derjenige, der den Stromliefervertrag mit Erlaubnis der Datenerhebung und -weitergabe unterzeichnet, eine Einwilligung gibt. Weitere im Haushalt lebende Personen sind ebenfalls in ihrem Recht auf informationelle Selbstbestimmung tangiert. Hier ist insbesondere zu berücksichtigen, dass mit feingranularen Metering-Daten auch eine Überwachung durch den Ehepartner oder durch Mitbewohner ermöglicht wird. Der Vertragsnehmer könnte beispielsweise kontrollieren, wann Personen das Haus verlassen haben oder ob jemand zu Besuch gekommen ist.

Wird der Smart Meter in einem betrieblichen Umfeld eingesetzt, werden Rechte der Arbeitnehmer verletzt, wenn Datenauswertungen ohne explizite Zustimmung erfolgen. Metering-Daten sind grundsätzlich geeignet, Arbeitnehmer zu überwachen, beispielsweise festzustellen, wer seinen PC längere Zeit nicht nutzt oder wann welches Büro betreten wurde.

3.5 Keine Auswertung von zusammengeführten Daten mehrerer Haushalte

Werden Metering-Daten mehrerer Haushalte in eine Datenbank überführt, können Personen nach Lebensgewohnheiten gerastert und gemäß frei wählbaren Kriterien aus der Datenbasis herausgefiltert werden (zum Beispiel Abgleich von Tatzeiten mit Abwesenheitszeiten). Dies wäre ein schwerwiegender Eingriff in die informationelle Selbstbestimmung, da beliebige Verdächtigungen

unter faktischer Aufhebung der Unschuldsvermutung im Hinblick auf die herausgefilterte Teilmenge der Letztverbraucher konstruiert werden können.

Das Bundesverfassungsgericht hat präventive polizeiliche Rasterfahndungen auf eine konkrete Gefahr für hochrangige Rechtsgüter wie den Bestand oder die Sicherheit des Bundes oder für Leben oder Freiheit einer Person beschränkt (Bundesverfassungsgericht 2006). Um diese starke Gebot nicht auszuhöhlen, dürfen feingranulare Metering-Daten – wenn sie schon nicht aufgrund fehlender Zweckbindung gelöscht werden – erst nach vollständiger Anonymisierung zu einer haushaltsübergreifenden Datenbasis zusammengefasst werden.

4 Fazit

Die Smart-Meter-Technologie bietet sowohl dem Verbraucher wie auch dem Energieversorger und Netzbetreiber vorteilhafte Funktionen zur effizienteren Nutzung von elektrischer Energie. Smart Meter können zur Senkung sowohl der Verbrauchskosten wie auch der Bereitstellungskosten, beispielsweise bei der Abrechnung des Energieverbrauchs, in erheblichem Maße beitragen.

Metering-Daten sind jedoch personenbezogene Daten, die neben der Zustimmung zu ihrer Erhebung und Verarbeitung eines besonderen Schutzes bedürfen, da tiefe Einblicke in den privaten Lebensbereich ermöglicht werden. Konkrete Handlungsempfehlungen an die Akteure betreffen daher in erster Linie die Klassifikation und den technischen Schutz dieser Daten. Nur durch ein Zusammenwirken der Schutzvorgaben, die bei allen beteiligten datenverarbeitenden Stellen anzuwenden sind, kann ein wirksamer Datenschutz beim Energie-Letztverbraucher umgesetzt werden.

Literatur

Bundesamt für Sicherheit in der Informationstechnik. 2013. BSI: Schutzprofil für ein Smart Meter Gateway (BSI-CC-PP-0073). https://www.bsi.bund.de/DE/Themen/SmartMeter/Schutzprofil_Gateway/schutzprofil_smart_meter_gateway_node.html (Zugriff: 16. Juli 2013).

Bundesverfassungsgericht, 2006. Urteil (zur Rasterfahndung) vom 4. April 2006, 1 BvR 518/02.

Bundesverfassungsgericht, 2010. Urteil (zur Vorratsdatenspeicherung) vom 2. März 2010, 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08.

Greveler, Ulrich, Benjamin Justus und Dennis Löhr. 2012. Forensic content detection through power consumption. In: *IEEE International Workshop on Security and Forensics in Communication Systems*, 6759–6763. Ottawa (Kanada): IEEE, Juni. doi:10.1109/ICC.2012.6364822, http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=6364822 (Zugriff: 16. Juli 2013).

Greveler, Ulrich, Benjamin Justus und Dennis Löhr. 2012. Identifikation von Videoinhalten über granulare Stromverbrauchsdaten. In: *Sicherheit 2012 – Sicherheit, Schutz und Zuverlässigkeit. 7.-9. März 2012 in Darmstadt ; Konferenzband der 6. Jahrestagung des Fachbereichs Sicherheit der Gesellschaft für Informatik e.V. (GI)*, hg. von Neeraj Suri und Michael Waidner, 35–45. GI Proceedings, 195. Bonn: Ges. für Informatik. http://subs.emis.de/LNI/Proceedings/Proceedings195/P-195.pdf.

Molina-Markham, Andrés, Prashant Shenoy, Kevin Fu, Emmanuel Cecchet und David Irwin. 2010. Private memoirs of a smart meter. In: *Proceedings of the 2nd ACM Workshop on Embedded Sensing Systems for Energy-Efficiency in Building*, hg. von Antonio Ruzzelli, 61–66. BuildSys '10. New York, NY: ACM. doi:10.1145/1878431.1878446.

Müller, Klaus J. 2010. Gewinnung von Verhaltensprofilen am intelligenten Stromzähler. *Datenschutz und Datensicherheit* 34, Nr. 6: 359–364. doi:10.1007/s11623-010-0107-2.

Der gläserne Patient – Chance oder Risiko?

Britta Böckmann

Im Gesundheitswesen existiert bezüglich des Themas Datenschutz ein Interessenkonflikt: Einerseits ist es im Interesse des Patienten, dass die an der Behandlung Beteiligten alle notwendigen Informationen über die Erkrankung, Vorgeschichte, Medikation, etc. zur Verfügung haben. Gleichzeitig steigt durch die demografische Entwicklung und die Kostenexplosion der Druck, Technologien einzusetzen, die mehr Effizienz versprechen. Der Beitrag stellt drei dieser Technologien vor – Ambient Assisted Living (AAL), die Pille mit Sensor und personalisierte Medizin –, skizziert die Entwicklung in anderen europäischen Ländern (Dänemark und Spanien) und zeigt Wege aus dem Interessenkonflikt auf.

1 Einleitung

Das Gesundheitswesen ist momentan in Deutschland, aber auch international bezogen auf Industrieländer von zwei wesentlichen Trends geprägt: Demografie und Kostendruck. Abbildung 1 zeigt die Alterspyramide in Deutschland im Vergleich von 2010 zu 2030 (prognostiziert). Da also einerseits die Menschen immer älter werden, andererseits die Gesundheitsausgaben im Alter steigen, brauchen wir in der Gesundheitsversorgung adaptierte Konzepte für diese demografische Veränderung.

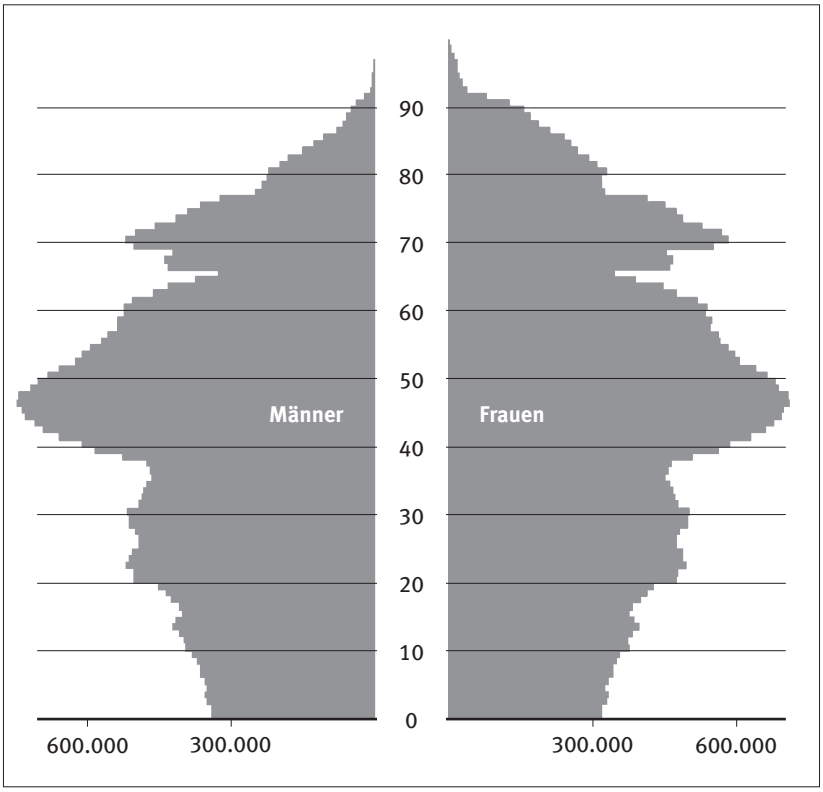

Abbildung 1a: Alterspyramide 2010
Quelle: Statistisches Bundesamt. 2009. 12. koordinierte Bevölkerungsvorausberechnung. https://www.destatis.de/bevoelkerungspyramide/.

Denn bereits der Blick auf die letzten zehn Jahre zeigt, welche Kostendimension sich abzeichnet: Zwischen 2001 und 2010 stiegen die Gesundheitsausgaben in Deutschland laut Statistischem Bundesamt von 220,8 Milliarden Euro im Jahr 2001 auf 287,3 Milliarden im Jahr 2010. Im gleichen Zeitraum stiegen die Pro-Kopf-Ausgaben von 2.680 Euro/Jahr auf 3.510 Euro/Jahr. Neben neuen Medikamenten und Therapien, also medizinischem Fortschritt, ist dieser Anstieg vor allem der Demografie geschuldet.

Technologien, die mehr Effizienz versprechen, die einem möglichen Mangel an Ärzten und Pflegepersonal begegnen oder helfen, die vorhandenen Ressourcen besser und zielgerichteter einzusetzen, werden dringend gebraucht.

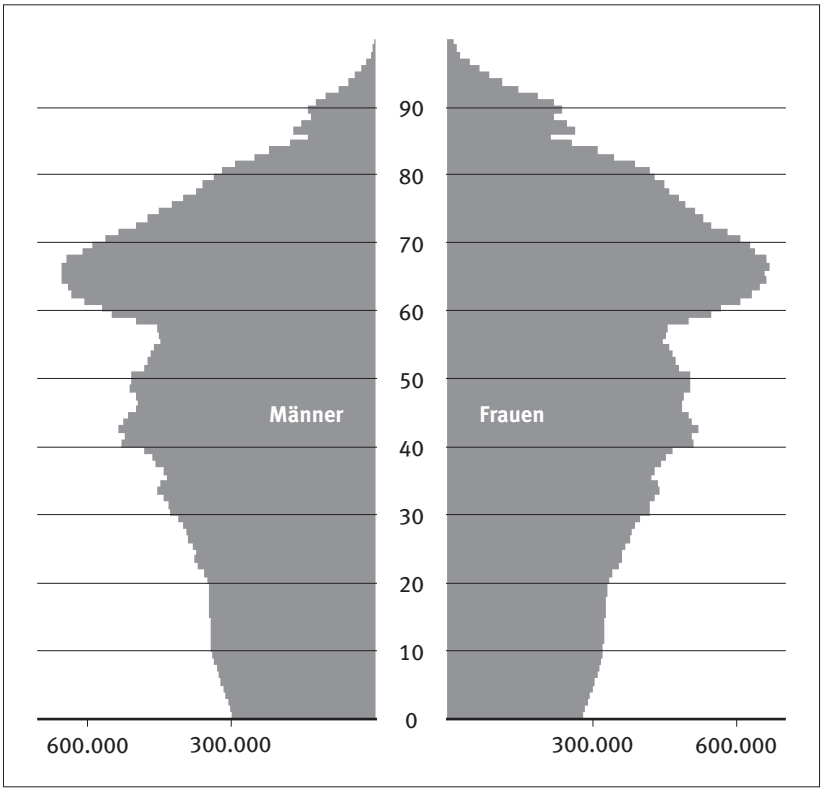

Abbildung 1b: Alterspyramide 2030
Quelle: Statistisches Bundesamt. 2009. 12. koordinierte Bevölkerungsvorausberechnung. https://www.destatis.de/bevoelkerungspyramide/.

Wenn die flächendeckende Einführung erst dann angegangen wird, wenn die Ressourcen bereits signifikant verknappt sind, steht auch dafür kaum noch Zeit und Geld zur Verfügung. Parallel dazu werden in diesem Spannungsfeld die gesetzlichen und finanziellen Spielregeln in Form von Gesundheitsreformen circa alle vier Jahre verändert bzw. angepasst. Allein die Einführung der elektronischen Gesundheitskarte – geplant seit 2001! – wurde seitdem bezüglich des Inhalts, der Form und des Zeitplan so oft modifiziert, dass von der ursprünglichen Idee und Innovation kaum etwas geblieben ist.

Beim Thema Datenschutz stehen sich zwei vitale Interessen der Verbraucherinnen und Verbraucher gegenüber. Einerseits ist es im ureigenen Interesse jedes Patienten, dass jeder an seiner Behandlung Beteiligte alle notwendigen Informationen über die Erkrankung, Vorgeschichte, Medikation etc. zur Verfügung hat, um bestmögliche Entscheidungen treffen zu können. Auch sind mit dem Einsatz von Informationstechnologie völlig neue therapeutische Möglichkeiten gegeben, ob in der Telemedizin oder der Pharmazie. Andererseits sind gerade Gesundheitsdaten ein besonders schützenswertes Gut und die Sorge, diese sensiblen Daten könnten in falsche Hände geraten, ist ähnlich groß wie im Finanzsektor.

In diesem Beitrag wird zunächst an einigen Beispielen aufgezeigt, welche technologischen Möglichkeiten es bereits heute gibt bzw. wohin sich die Forschung gerade entwickelt. Anschließend wird die Situation in Deutschland verglichen mit internationalen Entwicklungen und abschließend werden Handlungsempfehlungen abgeleitet.

2 Trends aus der Forschung

Um deutlich zu machen, welchen Herausforderungen sich der Datenschutz und der Umgang mit Daten im Gesundheitswesen in Zukunft stellen müssen, werden hier drei Forschungsbereiche skizziert, die mit sehr unterschiedlichen

Themen und Akteuren dennoch alle das Thema „gläserner Patient“ aus verschiedenen Perspektiven beleuchten.

2.1 AAL – ambient assisted living

Ambient Assisted Living (AAL) befasst sich mit der demografisch bedingten alternden Gesellschaft und entwickelt Lösungsansätze für intelligente Assistenzsysteme, die älteren Menschen den Alltag erleichtern und deren Lebensqualität verbessern sollen. Es handelt sich dabei um altersgerechte Assistenzsysteme der Mikrosystemtechnik und Informationstechnik in Kombination mit Dienstleistungsangeboten.

In AAL-Konzepten wird das Wohnen in der eigenen Wohnung ebenso unterstützt wie das vernetze Wohnen in Heimen und die Überwachung von Kranken und Demenzkranken, verbunden mit schneller Hilfe in Notfällen. Es berücksichtigt die Anforderungen von älteren Menschen hinsichtlich der Funktionalität, Bedienung und dem Design von AAL-Systemen. Zu den Anwendungsszenarien von Ambient Assisted Living gehören u.a. sicherheitsrelevante Funktionen, Überwachungsfunktionen und die Beschäftigung oder Unterhaltung der Haus-Patienten. Die einzelnen Funktionen können mit Sensoren erfasst und mittels Aktoren umgesetzt werden.

Es folgt ein Anwendungsbeispiel, das verdeutlicht, welche Auswirkungen diese Entwicklungen auf das Thema „gläserner Patient“ haben. Man stelle sich einen übergewichtigen Patienten vor, der mit seinem Hausarzt eine Gewichtsabnahme vereinbart durch Reduktion der täglich aufgenommenen Kalorien und mehr Bewegung. Dieser Patient bekommt einen Sensor, den er tagsüber trägt und der erfasst, wie viel er sich bewegt. Außerdem steht im Badezimmer eine Waage, die täglich das aktuelle Gewicht misst. Diese Daten (Gewicht und Bewegung) werden an eine zentrale Stelle übermittelt, wo eine intelligente Software anhand der verbrauchten Kalorien und der Soll-Ist-Entwicklung des Gewichts einen täglich angepassten Diätplan mit Einkaufsliste errechnet. Anhand des Kühlschrank-Bestands könnte sogar direkt elektronisch bestellt und geliefert werden. Ein Szenario, das technisch machbar ist – aber auch gewollt? Und wenn ja – wer darf dann was sehen?

2.2 Pharmakologie – die Pille mit Sensor

Ein Bereich der Forschung, der für die Pharma-Industrie interessant ist, aber auch die Gesundheitsversorgung verändern kann, sind die biologischen Sensoren. Heute kann niemand kontrollieren, ob ein Patient seine Medikation wirklich eingenommen hat. Das ist sicher einerseits ein Thema von Compliance, also der Frage, wie therapietreu der Patient ist, andererseits aber häufig auch von Kompetenz, etwa bei Demenz, von der hohen Anzahl verschiedener Medikamente, die ein Patient nehmen muss, oder ähnlichen Hürden.

„Technologisch" ist es bereits heute möglich, eine Pille mit einem biologisch abbaubaren Sensor zu versehen. Einmal geschluckt, sendet der Sensor ein Signal an einen mit einem Pflaster fixierten Empfänger. Dieser wiederum gibt die Information weiter an ein mobiles Endgerät, im Beispiel ein iPhone. Damit ist das iPhone in der Lage, beispielsweise jemanden zu benachrichtigen oder eine Erinnerung zu verschicken, wenn im Vergleich zu einem dort vorhandenen Medikationsplan Abweichungen festgestellt werden.

Kontrolle pur? Gläserner Patient? – Das vorgestellte Beispiel ist im Piloteinsatz zur Behandlung schizophrener Patienten. Dort gibt es ein typisches Verhaltensmuster: Wird eine Tablette nicht pünktlich eingenommen, führt das Fehlen des Wirkstoffs dazu, dass das Krankheitsbild sich zeigt, das heißt, der Patient zieht sich zurück, geht aus dem Kontakt und nimmt auch keine Medikation mehr zu sich. Mit der oben vorgestellten Entwicklung ist ein weitgehend „normales" Leben möglich.

2.3 Personalisierte/individualisierte Medizin

Der Begriff der personalisierten Medizin ist umstritten, diese Diskussion soll hier nicht aufgegriffen werden. Hier betrachten wir die ursprüngliche Herkunft und ihre Anwendungen respektive Versprechungen. Die grundlegende Idee der personalisierten Medizin ist es, dass mit der Entschlüsselung des menschlichen Genoms und den gefundenen individuellen Merkmalen eine auf den einzelnen Menschen angepasste Medizin möglich ist. Nach dem Bericht des Büros für Technikfolgenabschätzung beim Deutschen Bundestag (TAB) von 2009 gehört dazu im Einzelnen:

- biomarkerbasierte Stratifizierung (Gruppenbildung)
- genombasierte Informationen über Gesundheitsmerkmale
- Ermittlung individueller Erkrankungsrisiken
- differenzielle Interventionsangebote
- therapeutische Unikate (Implantate oder individuell angepasste Prothesen)

Auch dieser Forschungsbereich wirft spannende Frage auf bezüglich des Umgangs mit Daten. Gibt es eine Informationspflicht? Wenn sich aus einer Biomarkeranalyse beispielsweise ein erhöhtes Risiko für ein Mammakarzinom ergibt – ist es sinnvoll, dass die Patientin das weiß? Gehören solche individuellen Informationen aus dem Genmaterial in eine Patientenakte? Und wenn nicht – verschenken wir dann therapeutische Möglichkeiten?

Die Beispiele in diesem Kapitel sollen das Spannungsfeld verdeutlichen, in dem sich das Thema Umgang mit Daten und Datenschutz in der Medizin bewegt. So absolut schützenswert diese Daten sind, so lebensbedrohlich kann es sein, wenn sie nicht an der richtigen Stelle zur Verfügung stehen. Man denke nur an einen Unfall, bei dem es lebensrettend sein kann, sofort zu wissen, dass es sich um einen Bluter handelt – oder lebensrettend für die Ärzte, dass der Patient HIV-infiziert ist.

3 Ein Blick über die Grenzen

International gibt es zahlreiche Beispiele, wie neue Technologien eingesetzt werden können, zwei sollen auf den folgenden Seiten dargestellt werden.

3.1 E-Health in Dänemark

In Dänemark wurde bereits Ende der 1990er-Jahre konsequent auf eine E-Health-Strategie gesetzt. Es gibt ein nationales Portal, geteilt in einen öffentlichen und einen geschützten Bereich (sundhek.dk). Dort stehen für jeden Patienten unter anderem folgende Funktionen bereit:

- Zugang zur eigenen Gesundheitsakte (mit Befunden, Arztbesuchen etc.)
- verschiedene E-Services (Terminbuchung, neues Rezept anfordern, elektronische Kommunikation mit dem Arzt)
- Zugang zu Ratings von Krankenhäusern
- krankheitsorientierte Patientenforen
- krankheitsorientierte Handbücher für Patienten mit qualitätsgesicherter Information zu Erkrankung, Diagnose und Therapie

Für Ärzte erlaubt das Portal Zugriff auf Patientendaten, die nicht im eigenen System gespeichert sind, eigene Handbücher mit profundem Wissen zu Krankheiten, mit Videoanimationen etc.

Zum Grad der Realisierung digitaler Kommunikation sei auf Tabelle 1 verwiesen.

Type of message	% digital
Discharge letters from hospitals to GPs	99
Referrals from GPs to hospitals	81
Lab results from laboratories to GPs	99
Lab test orders from GPs to laboratories	99
e-Prescriptions from GPs to pharmacies	85
Reimbursement from GPs to public health insurance	99
Notifications of admission/ Notifications of discharge from hospitals to municipalities	98
Rehabilitation plans from hospitals to municipalities	80
Source: MedCom	

Tabelle 1: Digitalisierung in Dänemark.
Quelle: Ministeriet for Sundhed og Forebyggelse. 2012. *eHealth in Denmark*. Kopenhagen: Danish Ministry of Health, 13. http://www.sum.dk/~/media/Filer - Publikationer_i_pdf/2012/Sundheds-IT/Sundheds_IT_juni_web.ashx (Zugriff: 27. August 2013).

Zurzeit in Realisierung befindet sich der Aufbau einer zentralen Datenbank, in der die Medikation eines jeden Patienten während der letzten zwei Jahre gespeichert wird. Diese soll dann für alle Ärzte und den Patienten zugänglich sein, so dass es für die Prüfung von Kontraindikationen und Unverträglichkeiten eine valide Datenbasis gibt.

Die geplante Endausbaustufe zeigt Abbildung 2.

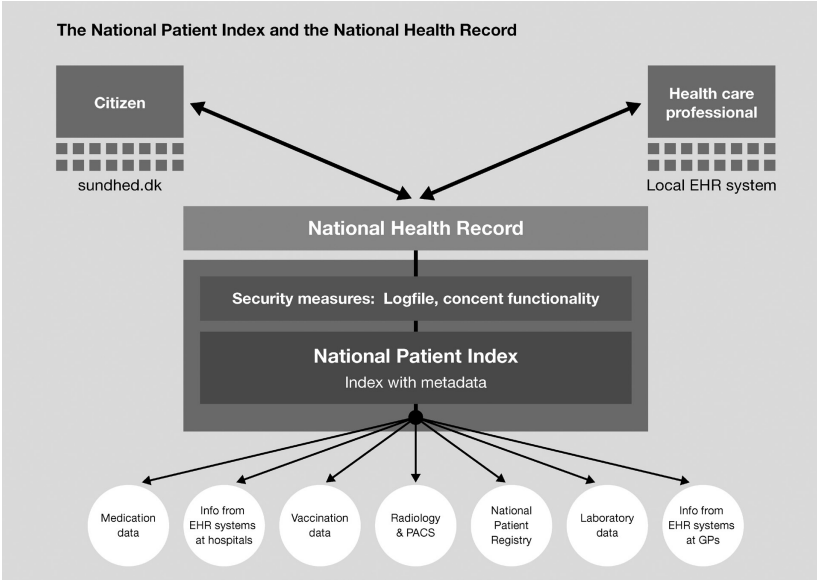

Abbildung 2: Endausbau E-Health in Dänemark.
Quelle: Ministeriet for Sundhed og Forebyggelse. 2012. *eHealth in Denmark*. Kopenhagen: Danish Ministry of Health, 26. http://www.sum.dk/~/media/Filer - Publikationer_i_pdf/2012/Sundheds-IT/Sundheds_IT_juni_web.ashx (Zugriff: 27. August 2013).

3.2 Telemedizin in Valencia, Spanien

In Valencia wurde unter der Regie des Gesundheitsministeriums in einer Public Private Partnership mit Telefonica, einem der in Spanien führenden Anbieter von Telekommunikation, ein Projekt gestartet und umgesetzt mit dem Ziel,

telemedizinische Services als Bestandteil der Regelversorgung zu etablieren. Im Gegensatz zu den üblichen Ansätzen, in denen Telemedizin im Pilotversuch läuft, zusätzlich zu etablierter Versorgung und begrenzt auf bestimmte Patientengruppen, umfasst dieses Projekt die Bevölkerung von Valencia als Grundgesamtheit. Diese wird basierend auf Informationen der Hausärzte in drei Risikogruppen verteilt, wobei ein hohes Risiko beispielsweise gegeben ist bei Herzinsuffizienz, einigen Typen von Diabetes oder ähnlichen vor allem chronischen Krankheiten.

Je nach Risikostufe wird dem Patienten dann eine bestimmte Form der telemedizinischen Unterstützung angeboten, von qualifizierter Information über eine Webseite (bei geringem Risiko) bis hin zu Devices, mit denen Vitalwerte wie EKG oder Gewicht beständig überwacht werden. Begleitet wird die Implementierung von umfangreichem Training und Ausbildung der Beteiligten sowie Evaluationen von Key Performance Indikatoren (zum Beispiel die Anzahl der Krankenhauseinweisungen, Arztbesuche, Zufriedenheit der Patienten). Erste Ergebnisse zeigen eine hohe Compliance der versorgten Patienten sowie eine tendenzielle Abnahme der Arztbesuche bzw. einen Ersatz durch periodisch stattfindende Videokonferenzen.

Eine Beschreibung des gesamten Projektes würde hier den Rahmen sprengen, weiterführende Informationen finden sich unter https://webgate.ec.europa.eu/eipaha/initiative/index/show/id/286.

4 Handlungsempfehlungen

Vor dem beschriebenen Hintergrund sind die Grenzen der weitgehenden Steuerung des Gesundheitswesens durch die Selbstverwaltung in Deutschland erreicht. In den letzten 15 Jahren wurden zahlreiche Pilotprojekte gestartet, oft öffentlich gefördert, die sich mit dem Datenaustausch im Kontext der integrierten Versorgung beschäftigen, mit telemedizinischen Anwendungen, mit Telemonitoring oder Technologien, die das selbst bestimmte Leben im Alter

unterstützen (AAL – ambient assisted living). In keinem der hier genannten Bereiche, die nur einen kleinen Ausschnitt der technologischen Möglichkeiten anreißen, hat es Fortschritte gegeben, die entwickelten Lösungen einer breiten Bevölkerungsschicht als Regelversorgung zur Verfügung zu stellen. Damit ist Deutschland im internationalen Vergleich deutlich zurückgefallen.

Die Regel ist immer noch, dass ein Krankenhaus keinen Zugriff auf die Vorbefunde und die Medikation eines Patienten hat, dass es keine Stelle gibt, an der sich die gesamte Patientengeschichte konsistent einsehen lässt, dass telemedizinische Leistungen nur wenigen Auserwählten zur Verfügung stehen und die meisten nicht einmal wissen, was das ist. Und das, obwohl es sicher mehr als zehn Definitionen und Initiativen für eine einheitlichen Patientenakte gibt.

Um diesen gordischen Knoten zu durchtrennen, sind eine stärkere Regulierung und die Umsetzung folgender Maßnahmen notwendig.

4.1 Telematikinfrastruktur, Datenaustausch

Anlass, Art und Umfang übermittelter Daten muss festgelegt werden, bundeseinheitlich inklusive der zu verwendenden Standards. Für jeden behandelnden Arzt, für jeden Anbieter von Praxen- oder Krankenhaussoftware, für jede Apotheke muss klar sein, wer an wen zu welchem Anlass Informationen übermittelt, in welchem Format das passiert und wer für die Richtigkeit und Vollständigkeit der Daten haftet. Der Betrieb der Telematikinfrastruktur muss in öffentlicher Hand bzw. Verantwortung liegen.

4.2 Datenschutz

Die gesetzlichen Regelungen zum Datenschutz sind in praktische Umsetzungsleitlinien zu überführen, die einen klaren verständlichen Rahmen definieren, wer wann unter welchen Umständen Zugriff auf Daten erhält, wofür die Zustimmung des Patienten einzuholen ist und wer haftet, wenn Daten nicht oder nicht in ausreichendem Umfang zur Verfügung stehen oder fehlerhaft sind. Diese Klarstellungen sind notwendig, um nicht nur das Vertrauen der Bürgerinnen und Bürger, sondern auch das der Ärzte, der Pflege und anderer

im Gesundheitswesen tätigen Berufsgruppen zu gewinnen. Auch können so Projekte erheblich beschleunigt werden, da nicht jedes Mal von Neuem grundlegende Fragen zu klären sind.

4.3 Orientierung an international erfolgreichen Konzepten

Andere Länder wie Dänemark oder auch Australien haben in verschiedenen Handlungsfeldern erfolgreiche Konzepte umgesetzt. So existiert in Dänemark beispielsweise seit Jahren eine zentrale Patientenakte. Von diesen Konzepten kann man einerseits lernen, andererseits ist es auch vor dem Hintergrund immer mobilerer Menschen sinnvoll, international kompatible Lösungen zu entwickeln.

4.4 Beteiligung der Betroffenen

Patientenorganisationen und Verbraucherschutz sind angemessen an diesem Prozess zu beteiligen und in Aufklärungs- und Informationskampagnen einzubinden. Wenn es nicht gelingt, die betroffenen Bürgerinnen und Bürger mit ihren berechtigten Ängsten und Ansprüchen ernst zu nehmen und zu überzeugen, wird das Grundvertrauen sich nicht entwickeln können. Durch die lange Historie und die bisherige Stimmungsmache ist viel verspielt worden, insbesondere auch die Chance, frei von Vorbehalten aufzuklären.

4.5 Evaluation der Maßnahmen

Die Evaluation muss sich lösen von der Sicht auf einzelne Projekte. Wichtigstes Kriterium einer guten Gesundheitsversorgung ist das Ergebnis, also bessere Gesundheit und höhere Lebensqualität bei vertretbaren Kosten. Dazu ist die Evaluation sektorübergreifend und outcome-orientiert aufzubauen.

Bitcoin – Anonym Einkaufen im Internet?

Artus Krohn-Grimberghe und Christoph Sorge

Abstract

Mit Bitcoin ist vor wenigen Jahren ein dezentral organisiertes Bezahlsystem entstanden, das auf geschickte Weise kryptographische Verfahren kombiniert und somit auf einen zentralen Server verzichten kann. Obwohl das Bitcoin-System nicht professionell vermarktet wird, ist es über den Status einer wissenschaftlichen Spielerei hinausgewachsen und ist auch außerhalb der Informatik auf Interesse gestoßen.

Dienstleistungen im Rahmen des Bitcoin-Systems werden in der Regel nicht von bereits längerfristig etablierten Anbietern erbracht, sondern von innovationsgetriebenen Neugründungen. Eine Reihe von Zwischenfällen, bei denen Bitcoins abhandengekommen sind, gibt Anlass, auch die Risiken der Bitcoin-Anwendung zu betrachten. Bitcoin wird somit zum Thema für den Verbraucherschutz. Der Beitrag gibt einen Überblick über die Thematik, diskutiert Risiken und Regulierungsbedarf und gibt Empfehlungen zum Umgang mit Bitcoin.

1 Was ist Bitcoin?

Laut Bitcoin-Wiki www.bitcoin.it sind Bitcoins eine elektronische „Währung“ auf Basis eines Peer-to-Peer-Systems. Die zentralen technischen Konzepte wurden im November 2008 auf einer Kryptographie-Mailingliste vorgestellt (Nakamoto 2008). Im Januar 2009 folgte die Veröffentlichung der ersten Client-Software für Benutzer und die ersten Bitcoins wurden erzeugt. Der Autor des Bitcoin-Konzepts und des ersten Clients ist unbekannt; man kennt sie oder ihn lediglich unter dem Namen Satoshi Nakamoto, der wahrscheinlich ein Pseudonym ist.

Jeder kann am Bitcoin-Ökosystem teilnehmen und Bitcoins empfangen oder überweisen. Hierzu gibt es mehrere kostenfreie Bitcoin-Client-Programme (O.A. 2013b). Weiterhin unterstützt eine Vielzahl an Informationsseiten die Bitcoin-Nutzer. So liefert z.B. bitcoincharts.com eine Übersicht über das Bitcoin-Netzwerk und vor allem auch den aktuellen Preis pro Bitcoin auf diversen Anbieterseiten. Die führenden Handelsanbieter für Bitcoins sind Mitte Juni 2013 mtgox.com und bitstamp.net. Daneben bieten Foren wie bitcointalk.org eine Gelegenheit, sich über Neuigkeiten im Bitcoin-Land zu informieren und Fragen zu stellen.

2 Das Konzept Bitcoin

Frühere anonyme Bezahlverfahren, welche hauptsächlich aus akademischen Forschungsvorhaben stammten (z.B. Chaum, Fiat und Naor 1988), verwenden oft das Konzept elektronischer Münzen. Bei Bitcoin gibt es, anders als der Name glauben machen könnte, hingegen keine „Münzen“, sondern ausschließlich Überweisungen. Damit funktioniert Bitcoin ähnlich wie Buchgeld (Giralgeld) auf einem Bankkonto: Die Clientanwendung zeigt dem Nutzer den aktuellen Kontostand an und erlaubt es, vom Guthaben Bitcoinbeträge zu

anderen Bitcoin-Empfängern zu überweisen. Die Identifikation der „Kontoinhaber“ erfolgt dabei durch öffentliche Schlüssel, welche die Rolle von Kontonummern übernehmen. Die zugehörigen (und geheim zu haltenden) privaten Schlüssel ermöglichen das Tätigen von Überweisungen. Hierbei ist hervorzuheben, dass man in aller Regel etliche Bitcoin-„Konten“ (Bitcoin-Adressen) unterhält – gegebenenfalls sogar eins pro Transaktion. Den Bitcoin-Nutzer muss dies allerdings nicht unbedingt interessieren, da die Verwaltung der „Konten“ von der Software übernommen wird.

Bitcoin existiert aktuell als reines Peer-to-Peer-Verfahren, bei dem keine Mittler wie Banken erforderlich sind. Jeder Nutzer kann jedem anderen Nutzer, von dem er die zugehörige Bitcoin-Adresse kennt, Bitcoins überweisen. Dieses System ist jedoch wahrscheinlich in der aktuellen Form nicht skalierbar, da es die Speicherung der kompletten Transaktionshistorie auf den Rechnern der aktiven Teilnehmer (so genannte Miner) erfordert. Hier bestehen zwar noch Optimierungsmöglichkeiten, aber gänzlich vermeiden lässt sich das Vorhalten der Transaktionshistorie nicht. Sie wird benötigt, um nachvollziehen zu können, dass kein Betrag mehrfach ausgegeben wurde.

Daneben sieht Bitcoin auch vor, alle Transaktionen allen aktiven Teilnehmern des Systems zu übermitteln. Bei Erreichen der Transaktionszahl von VISA – angeblich 2000 Transaktionen pro Sekunde (O. A. 2013a) – würde dies ein Datenvolumen von ca. 8 Mbit/s erzeugen; momentan werden etwa 0,6 Transaktionen pro Sekunde durchgeführt (Blockchain 2013a). Langfristig ist daher das Etablieren von Intermediären wie „Banken“ nötig, falls Bitcoin weiter existiert.

3 Bitcoin im Handel

Während Bitcoin im Ruf stand, ursprünglich überwiegend für „zwielichtige“ Angebote verwendet worden zu sein, zeigt sich mittlerweile eine steigende Akzeptanz durch seriöse Anbieter. Unter https://en.bitcoin.it/wiki/Trade sind mittlerweile viele Anbieter aufgelistet, die Bezahlungen in Bitcoin entgegen-

nehmen. Die Angebote selbst sind sehr technikzentriert, es überwiegen Internet- und mobile Dienstleistungen wie VPN, (Web-)Hosting und Programmierung. Moderne Zahlungsdienste wie Bitinstant und BitPay ermöglichen sogar den Erwerb von Waren via Amazon bei Bezahlung mit Bitcoin.

Daneben sind Handelsplattformen nach dem Prinzip von eBay entstanden, und erste Restaurants sowie andere Realwelt-Geschäfte haben sich entschlossen, Bitcoins zu akzeptieren. Der Charme von Bitcoin liegt darin, dass weltweit Transaktionen zum gleichen Preis durchführbar sind. Die Transaktionsgebühr ist optional und beschleunigt aktuell lediglich die Festschreibung der Transaktionen. Zahlungen werden technisch erst nach mehreren Minuten festgeschrieben,[1] was eine Risikoabwägung bei Instant-Geschäften notwendig macht (für Transaktionen mit hohem Gegenwert wird empfohlen, 60 Minuten abzuwarten, bis sich hinreichend viele Bestätigungen für die Durchführung gefunden haben). Dennoch sind Überweisungen mittels Bitcoin wesentlich schneller – und meist wesentlich günstiger – als klassische Überweisungen.

Als Bitcoin-Nutzer sollte man jedoch im Hinterkopf behalten, dass der Bitcoin-Preis sehr stark schwankt. Preisveränderungen im Bereich von 10-15 Prozent pro Tag sind keine Seltenheit. Dies macht die Wertaufbewahrung schwierig bzw. riskant, ist für eine reine Zahlungsabwicklung jedoch meist kein Problem.

4 Mögliche Angriffe auf Bitcoin

Ein potentielles Sicherheitsproblem ist bereits in der Grundidee von Bitcoin angelegt: Die Transaktionshistorie wird benötigt, um das mehrfache Ausgeben eines Betrags zu verhindern. Da Bitcoin bewusst auf eine vertrauenswürdige Instanz verzichtet, die die Echtheit (Authentizität) einer Transaktionshistorie bestätigen könnte, muss ein alternativer Mechanismus eingesetzt werden. Der

1 Wir werden im nächsten Abschnitt auf den technischen Hintergrund dieser Bestätigungen eingehen.

Ansatz, der hierfür gefunden wurde, funktioniert (vereinfacht dargestellt) wie folgt: Wenn ein Teilnehmer eine Transaktion durchführen will, gibt er diese im Bitcoin-System allen aktiven Teilnehmern bekannt. Diese nehmen die Transaktion (eigentlich: mehrere, in einem Block zusammengefasste Transaktionen) in die Transaktionshistorie auf und berechnen einen Arbeitsbeweis[2] – das bedeutet, dass sie nachweisen, Rechenleistung für die Bestätigung der Transaktionshistorie aufgebracht zu haben. Da der Arbeitsbeweis sich stets auf alle vorhandenen Transaktionen bezieht, fließt ständig mehr Rechenleistung in die Bestätigung älterer Transaktionen. Liegen mehrere Versionen der Transaktionshistorie vor, gilt diejenige als korrekt, in die die meiste Rechenleistung geflossen ist. Es ist also schwierig, eine alte Transaktion „verschwinden" zu lassen: Dazu müsste man eine neue Transaktionshistorie berechnen, die diese alte Transaktion nicht enthält – der Angreifer müsste mehr Rechenleistung erbringen als alle ehrlichen Teilnehmer zusammengenommen. Dies ist zwar nicht ausgeschlossen, doch hat sich das Risiko des Angriffs bislang auch nicht realisiert.

Es gab dennoch bereits diverse erfolgreich durchgeführte Angriffe auf Bitcoin. Dabei konnten jedoch bislang keine Protokollschwächen bei Bitcoin selbst gefunden oder gar ausgenutzt werden (sofern man die oben erklärte Annahme, dass kein Angreifer mehr Rechenleistung hat als die ehrlichen Teilnehmer zusammengenommen, nicht als Protokollschwäche ansieht). Hingegen nutzten die Angreifer meist die teils groben Sicherheitslücken bei den verschiedenen Bitcoin-Dienstleistern oder die Leichtgläubigkeit der Nutzer aus. Bekannte und bestätigte Diebstähle durch Angriffe summieren sich mittlerweile auf umgerechnet über 3 Millionen US-Dollar. Insgesamt ist anzumerken, dass die Marktteilnehmer oft erstaunlich naiv agieren. So waren Nutzer bereit, tausende Bitcoins der Online-Geldbörse MyBitcoin anzuvertrauen, deren Betreiber mitsamt den Bitcoins abtauchte (später wurden knapp fünfzig Prozent der Bitcoins zurückerstattet). Andere gaben in Summe wohl über 100.000 Bitcoins einem Nutzer namens Pirate@40, welcher etliche Prozent Zinsen pro Woche versprach und sich letztlich mitsamt den Bitcoins davonstahl. Ein großer Bitcoin-Handelsplatz ging insolvent, weil er keine Sicherung (Backup) der privaten Schlüssel seiner Bitcoins hatte, ein anderer, weil er mit seinen Kunden-

2 Konkret werden hashbasierte Arbeitsbeweise nach dem Vorbild von Back (2002) verwendet.

geldern spekulierte, einem anderen wurden in einer spektakulären Serie über 100.000 Bitcoins gestohlen. Auch kommen immer wieder potentiell dubiose Techniken auf den verschiedenen Bitcoin-Handelsplätzen zum Einsatz, mit denen unerfahrene Anleger bei plötzlichen Preisbewegungen sehr viel Geld verlieren. Hier sollte vor allem beachtet werden, dass lediglich 22 Prozent aller Bitcoins sich in Zirkulation befinden und dass das Handelsvolumen noch sehr klein ist. Dies ermöglicht es wohlhabenden Individuen mit einer guten Kenntnis des Marktes theoretisch, einen nicht unerheblichen Einfluss auf den Bitcoin-Preis zu nehmen.

5 Kritik am Energiebedarf

Da die Sicherheit von Bitcoin darauf basiert, dass viel Rechenleistung in die Bestätigung einer Transaktionshistorie investiert wird, entsteht durch das System auch ein hoher Energiebedarf. Auf diese Problematik haben Becker et al. (2012) hingewiesen, die auch eine Schätzung der benötigten Rechenleistung und des daraus folgenden CO2-Ausstoßes geben. Eine Schätzung der Webseite blockchain.info (2013b) geht von einem Bedarf von ca. 2600 Megawattstunden für eine 24-Stunden-Periode aus. Sie kann nur eine grobe Annäherung darstellen, doch ist die Kritik durchaus ernst zu nehmen. Die durchgeführten Berechnungen dienen ausschließlich dem Nachweis, Ressourcen investiert zu haben; es werden keine sinnvollen Werte berechnet, die sich für andere Zwecke weiterverwenden ließen.

6 Anonymität und Datenschutz

Wenn man als Bitcoin-Nutzer seine Anonymität wahren will, steht man vor dem Grundproblem der vollständig öffentlichen Transaktionsgeschichte. Jeder Nutzer hat eine Kopie davon in seinem Client-Programm oder kann sie zumindest unter blockchain.info einsehen. Anonymität war entgegen anderslautender Informationen kein wesentliches Entwurfsziel. Bitcoin erreicht lediglich Pseudonymität: Auch wenn sich jeder Nutzer beliebig viele Bitcoin-Adressen (öffentliche Schlüssel) erzeugen kann, ist immer noch ein Verstecken der Zuordnung zwischen einer Bitcoin-Adresse und der entsprechenden Person notwendig. Das Erreichen der Pseudonymität wird dabei zusätzlich durch immer fortschrittlichere Analysewerkzeuge erschwert. Beispielsweise ermittelten Wissenschaftler im Mai letzten Jahres, dass WikiLeaks mindestens 83 Schlüssel besitzt und über diese ca. 2605 BTC an Spenden erhalten hat (Ron und Shamir 2012). Aktuell kann als Tipp lediglich das Generieren eines neuen Schlüsselpaares für jede Transaktion in Kombination mit dem Durchführen von Pseudo-Transaktionen und dem Verschleiern der eigenen IP-Adresse empfohlen werden.

Auf der anderen Seite bietet Bitcoin im Gegensatz zum E-Geld aktuell noch die Möglichkeit, mehr als hundert Euro pro Monat anonym in Bitcoin umzuwandeln, um damit beispielsweise elektronische Dienstleistungen und Waren zu bezahlen. Hierbei muss jedoch angemerkt werden, dass zwischenzeitlich mit mtgox.com auch der größte Bitcoin-Handelsplatz eine Identitätsverifikation bei Auszahlungen in Realwährung verlangt; wirklich anonym sind nur Kauf und Verkauf gegen Bargeld. Daneben gibt es grundsätzlich noch die Möglichkeit, selbst Bitcoins per so genannten Mining zu erzeugen. Dies bedeutet, dass man selbst Arbeitsbeweise berechnet. Ist man dabei erfolgreich (das heißt, man hat einen Arbeitsbeweis als erster aktiver Teilnehmer abgeschlossen), darf man sich einen festgelegten Bitcoin-Betrag selbst gutschreiben. Aktuell ist dies nur noch mit spezialisierter Hardware und mit hohem Energieaufwand möglich.

7 Rechtslage

Bitcoin wird in Deutschland als Rechnungseinheit angesehen und ist somit gemäß §1 Abs. 11 Satz 1-3 des Gesetzes über das Kreditwesen ein Finanzinstrument (Bundesanstalt für Finanzdienstleistungsaufsicht 2011). Hieraus folgt, dass das gewerbsmäßige Erbringen gewisser Dienstleistungen mit Bitcoins aufsichtspflichtig sein und einer Erlaubnis durch die Bundesanstalt für Finanzdienstleistungsaufsicht bedürfen kann. Bitcoins stellen hingegen kein E-Geld und (zumindest strafrechtlich) auch kein Geld dar, wenngleich Bitcoin etliche der klassischen Geldfunktionen durchaus zu erfüllen vermag (dazu ausführlich die Autoren dieses Artikels in Sorge und Krohn-Grimberghe 2012). Die Verwendung von Bitcoins als Zahlungsmittel ist in Deutschland nicht umsatzsteuerpflichtig. Auch der An- und Verkauf von Bitcoins ist in Deutschland im Gegensatz zu anderen EU-Ländern aufgrund der Eigenschaft als Finanzinstrument nach Auffassung der Autoren nicht umsatzsteuerpflichtig.

8 Fazit und Handlungsempfehlungen

Als Peer-to-Peer-System ermöglicht es Bitcoin, dass Nutzer anderen Nutzern ohne Mittelsmann „Geld“ überweisen. Für die Zukunft ist jedoch ggf. ein Zwei-Schichten-Modell mit zwischengeschalteten „Banken“ zu erwarten. Dies zeichnet sich bereits durch die Einführung sogenannter White-Lists ab, die Adressen von vertrauenswürdigen Instanzen beinhalten, welche Überweisungen deutlich schneller abwickeln können, da sie nicht etliche Bestätigungen benötigen, bis sie gemeinhin als gültig angesehen werden.

Trotz der augenscheinlichen Anonymität sollten Nutzer sich bewusst sein, dass Bitcoin lediglich „pseudonyme“ Transaktionen ermöglicht und echte Anonymität nur schwer zu erreichen ist.

Daneben darf auch nicht übersehen werden, dass Überweisungen „irreversibel" sind und die insbesondere bei Schecks und Kreditkartenentgegennahme bekannten Chargebacks nach einer gewissen Anzahl von Minuten als ausgeschlossen anzusehen sind.

Nach dem gegenwärtigen Stand der Forschung ist das Bitcoin-Protokoll als sicher zu betrachten. Die sich im Bitcoin-Ökosystem tummelnden Dienstleister sind dies jedoch eher noch nicht, und insgesamt ist ein erstaunlich hohes Maß an Fahrlässigkeit zu beobachten. Zum Spekulieren mit Bitcoins ist anzumerken, dass der Preis noch immer unverhältnismäßig stark schwankt und der Markt von versierten Tradern dominiert wird. Aus diesem Grund empfehlen die Autoren das längerfristige Halten und Spekulieren mit Bitcoins lediglich erfahrenen Börsenveteranen und Devisenhandelsexperten. Bitcoins zum Bezahlen und für kostengünstige Überweisungen – insbesondere ins Ausland – einzusetzen halten die Autoren jedoch für eine gute Idee und einen denkbaren Einstieg in dieses spannende Thema. Einen großen Gegenwert in Bitcoins auf dem eigenen Rechner oder gar in der Cloud abzulegen, kann insbesondere Einsteigern aufgrund des hohen Verlustrisikos nicht empfohlen werden.

Angesichts der Risiken für den Verbraucher, die ohne hinreichende Informationen die Risiken oft nicht einschätzen können, kann aktuell zumindest eine Beobachtung der Entwicklungen im Bitcoin-Ökosystem empfohlen werden. Über bereits getroffene Maßnahmen hinaus erscheint ein weitergehendes Eingreifen durch Aufsichtsbehörden nach dem momentanen Stand nicht notwendig; dies mag sich aber im Fall einer weiteren Verbreitung von Bitcoin ändern.

Literatur

Back, Adam. 2002. Hashcash – A Denial of Service Countermeasure. *hashcash.org*. http://www.hashcash.org/papers/hashcash.pdf (Zugriff: 20.6.2013).

Becker, Jörg, Dominic Breucker, Tobias Heide, Justus Holler, Hans Peter Rauer und Rainer Böhme. 2012. Geld stinkt, Bitcoin auch – Eine Ökobilanz der Bitcoin Block Chain. In: *Was bewegt uns in der, die Zukunft? 42. Jahrestagung der Gesellschaft für Informatik e.V. (GI), 16. bis 21.9.2012, TU Braun-*

schweig, hg. von Ursula Goltz, Marcus Magnor, Hans-Jürgen Appelrath, Herbert K. Matthies, Wolf-Tilo Balke und Lars Wolf, 39–50. Lecture Notes in Informatics (LNI) - Proceedings, P-208. Bonn: Gesellschaft für Informatik.

Blockchain. 2013a. Bitcoin Anzahl der Transaktionen pro Tag. *Blockchain.info*. http://blockchain.info/de/charts/n-transactions (Zugriff: 20. Juni 2013).

Blockchain. 2013b. Bitcoin Statistics. *Blockchain.info*. http://blockchain.info/en/stats (Zugriff: 20. Juni 2013).

Bundesanstalt für Finanzdienstleistungsaufsicht. 2011 *Merkblatt – Hinweise zu dem Gesetz über die Beaufsichtigung von Zahlungsdiensten* (Zahlungsdiensteaufsichtsgesetz - ZAG), 22. Dezember. http://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Merkblatt/mb_111222_zag.html (Zugriff: 20.6.2013).

Chaum, David, Amos Fiat und Moni Naor. 1990. Untraceable Electronic Cash. In: *Advances in Cryptology — CRYPTO' 88*, hg. von Shafi Goldwasser, 319–327. Lecture Notes in Computer Science, 403. New York: Springer. http://dx.doi.org/10.1007/0-387-34799-2_25.

Nakamoto, Satoshi. 2008. Bitcoin: *A Peer-to-Peer Electronic Cash System*. http://bitcoin.org/bitcoin.pdf (Zugriff: 20.6.2013).

O A. 2013a. Scalability. *Bitcoin wiki*. https://en.bitcoin.it/wiki/Scalability (Zugriff: 20. Juni 2013).

O A. 2013b. Software. *Bitcoin wiki*. https://en.bitcoin.it/wiki/Software (Zugriff: 20. Juni 2013).

Ron, Dorit und Adi Shamir. 2012. *Quantitative Analysis of the Full Bitcoin Transaction Graph*. Cryptology ePrint Archive, Report 2012/584, http://eprint.iacr.org/2012/584.pdf.

Sorge, Christoph und Artus Krohn-Grimberghe. 2012. Bitcoin: Eine erste Einordnung. *Datenschutz und Datensicherheit* 36, Nr. 7: 479–484.

Zusammenfassende Thesen

Kompetenzzentrum Verbraucherforschung NRW

Dieses Thesenpapier fasst die Essenz der Vorträge und der Diskussion im Rahmen des Workshops „Der gläserne Verbraucher: Wird Datenschutz zum Verbraucherschutz?“ aus Sicht der Veranstalter zusammen.

1 Thesen zur Ausgangssituation und zum Handlungsbedarf

These 1.1: Die Privatsphäre der Verbraucherinnen und Verbraucher ist heute gefährdeter denn je.

Die rasante Entwicklung der Informations- und Telekommunikationstechnologien hat eine Vielzahl an neuen Anwendungen hervorgebracht, ohne die man sich den Alltag kaum noch vorstellen kann. Beispiele hierfür sind die Informationsrecherche im Internet, eine grenzenlose Kommunikation, Downloads von Musik und Büchern aus dem Internet, Einkaufen rund um die Uhr oder mobiles Internet. Allerdings hat diese Entwicklung auch einen Preis. Denn viele Dienste funktionieren nur, wenn Verbraucherinnen und Verbraucher ihre Daten preisgeben.

These 1.2: Vom Abwehrrecht zum Recht auf informationelle Selbstbestimmung.

Während das deutsche Datenschutzrecht in den 1970er-Jahren primär als Abwehrrecht der Bürgerinnen und Bürger gegen Eingriffe staatlicher Institutionen in die Privatsphäre konzipiert wurde, müssen Verbraucherinnen und Verbraucher heute im besonderen Maße vor einem Ausspähen durch private Akteure geschützt werden. Ihre Hoheit über ihre Daten, ihre informationelle Selbstbestimmung muss gewährleistet werden. Die Herausforderung hierbei besteht darin, dass viele Services, wie soziale Netzwerke, auf der Preisgabe von persönlichen Daten beruhen. Zudem „vergisst“ das Internet nichts. Eine einmal unbedacht geäußerte Aussage bleibt für ewig mit der Person verbunden und ist global auffindbar.

These 1.3: Viele Verbraucherinnen und Verbraucher verlieren zunehmend den Überblick und verhalten sich ambivalent.

Für Verbraucherinnen und Verbraucher gestaltet es sich zunehmend schwierig, den Überblick darüber zu behalten, welches Unternehmen, in welchem Umfang und zu welchen Zwecken persönliche Daten über sie erhebt, speichert und verarbeitet. So ist den wenigsten Anwendern bekannt, dass Social Plug-Ins von Facebook wie der „Gefällt mir"-Button auch die Datenübermittlung von Anwendern ermöglicht, die nicht bei Facebook registriert sind. Während viele Verbraucherinnen und Verbraucher diese Entwicklung mit Sorge betrachten und Unternehmen im Umgang mit personenbezogenen Daten misstrauen, gehen sie selbst oft sorglos mit persönlichen Daten um. Untersuchungen zeigen, dass Verbraucherinnen und Verbraucher immer wieder selbst sensibelste Daten auf Nachfrage oder im Rahmen eines Gewinnspiels preisgeben.

These 1.4: Die Rechtsetzung und -durchsetzung läuft den Entwicklungen hinterher.

Die rasante Entwicklung der Internet- und Telekommunikationstechnologien und -dienstleistungen macht es dem Gesetzgeber schwer, Schritt zu halten. Die Diskussion um Google-Street-View oder eine automatische Gesichtserkennung bei Facebook zeigen das rasante Tempo, in dem sich die Technik weiterentwickelt. Gleichzeitig werden die Grenzen der Rechtsdurchsetzung offenbar. So sind die Datenschutzaufsichtsbehörden personell unzureichend ausgestattet und ein nationales Datenschutzrecht kommt an Grenzen, wenn es gegen international agierende Unternehmen angewendet werden soll.

2 Erkenntnisse zum Daten- und Verbraucherschutz aus der Forschung

These 2.1: Das Datenschutzrecht hat auf Cloud-Anwendungen keine ausreichenden Antworten.

Zentraler Akteur im Datenschutzrecht ist die jeweils verantwortliche Stelle. Die verantwortliche Stelle ist verpflichtet, die gesetzlichen Regelungen im Datenschutz einzuhalten. Cloud-Anwendungen stellen das Datenschutzrecht jedoch vor eine Herausforderung. Hier laden Verbraucherinnen und Verbraucher beispielsweise Fotos auf Plattformen hoch, auf denen Personen abgebildet sind, die keine Zustimmung zur Veröffentlichung gegeben haben. Während das deutsche Bundesdatenschutzgesetz nicht auf persönliche oder familiäre Tätigkeiten anwendbar ist, hat der Europäische Gerichtshof geurteilt, dass das europäische Datenschutzrecht durchaus auf private Tätigkeiten anzuwenden ist. Es ist allerdings höchst fraglich, ob es sinnvoll und möglich ist, Verbraucherinnen und Verbrauchern ähnliche Pflichten im Datenschutz aufzuerlegen wie beispielsweise Unternehmen. Gleichzeitig kann dem Cloud-Anbieter allerdings auch nicht die Pflicht übertragen werden, etwa bei jedem Bild zu prüfen, ob Einwilligungen vorliegen. Wie eine angemessene Pflichtenverteilung aussehen könnte und sollte, ist noch völlig ungeklärt.

These 2.2: Unternehmen offenbaren immer wieder einen verantwortungslosen Umgang mit personenbezogenen Daten.

Smart Meter spielen in der derzeitigen energiepolitischen Diskussion eine wichtige Rolle. Zum einen können sie das Bewusstsein von Verbraucherinnen und Verbrauchern für ihren Energieverbrauch schärfen. Hierdurch können sie einen Beitrag für Energiekostenreduktionen und den Klimaschutz leisten. Zum anderen kann eine intelligente Steuerung der Stromnachfrage Spitzen im Stromverbrauch reduzieren und somit einen Beitrag für das Gelingen der Energiewende leisten. Die ersten Pilotprojekte offenbaren allerdings, dass Un-

ternehmen in der Entwicklung dieser Technologie dem Datenschutz und der Datensicherheit immer wieder zu wenig Aufmerksamkeit schenken. So wurden in einer Lösung die Verbrauchsdaten unverschlüsselt übertragen, obwohl das Unternehmen in den Verträgen eine verschlüsselte Übertragung zugesichert hat. Diese Stromverbrauchsdaten erlauben tiefe Einblicke etwa in TV-Gewohnheiten, Copyrightverstöße und Lebensgewohnheiten.

These 2.3: Der Schutz der Privatsphäre läuft Gefahr, zu einem Luxusgut zu werden.

Einige Untersuchungen – etwa bei Online-Kreditmärkten – weisen darauf hin, dass gerade einkommensschwächere Verbraucherinnen und Verbraucher mehr personenbezogene Daten über sich preisgeben als einkommensstärkere. Dies lässt sich insbesondere in den Fällen beobachten, in denen Verbraucherinnen und Verbraucher etwa bei optionalen Fragestellungen oder Freitextfeldern auf Online-Kreditportalen Informationen eingeben können. In diesem Sinne verstärkt ein Datenschutz, wenn er optional ist, die Unterschiede zwischen unterschiedlichen Einkommensschichten. Während einkommensschwächere Haushalte versuchen, ihr Stigma durch mehr persönliche Informationen zu überwinden, können es sich einkommensstärkere Haushalte leisten, wenige Informationen preiszugeben. Wenn Datenschutz jedoch allgemein verbindlich ist, dann hat er eine nivellierende Wirkung. In diesem Sinne hat der Datenschutz auch Auswirkungen auf die Verteilungsgerechtigkeit.

These 2.4: In einigen Fällen kann Regulierung und nicht die Selbstregulierung einen wesentlichen Erfolgsfaktor für neue Dienstleistungen darstellen.

Gerade im Gesundheitsbereich kann der Einsatz von Informationstechnologien wesentlich für ein Mehr an Lebensqualität der Betroffenen und zu Einsparungen für das Gesundheitssystem beitragen. Allerdings setzen Anwendungen wie eine Pille mit Sensor, die Informationen über die Einnahme liefert, oder ein elektronischer Informationsaustausch zwischen Patienten, Ärzten, Krankenkassen, Apotheken und Krankenhäusern voraus, dass Verbraucherinnen und Verbraucher der Technologie auch vertrauen. Es gibt allerdings Hinweise, dass

das Markt- und Selbstregulierungsprinzip im Gesundheitsbereich versagt. Um sinnvolle Anwendungen im Gesundheitsbereich zum Erfolg zu führen, ist daher eine staatliche Regulierung notwendig. Diese muss gesetzliche Anforderungen in einer verständlichen Form formulieren. Gleichzeitig ist sicherzustellen, dass im politischen Prozess auch Patienten- und Verbraucherinteressen systematisch mit einbezogen werden.

These 2.5: Neue Anwendungen wie Bitcoins können den Datenschutz verbessern, allerdings weisen sie (noch) teils gravierende Schwächen auf.

In den vergangenen Jahren haben Bitcoins – eine digitale Währung – eine immer größere Bedeutung erlangt. Bitcoins ermöglichen es Verbraucherinnen und Verbrauchern, global und kostengünstig Überweisungen tätigen zu können. Das System wird dezentral und ohne eine übergeordnete Kontrollinstanz betrieben. Aus Datenschutzsicht sind Bitcoins interessant, da sie die Anonymität der Nutzerinnen und Nutzer weitgehend wahren. Allerdings weisen Bitcoins noch gravierende Schwächen auf. So hat es eine Reihe von Betrugsfällen und Diebstählen gegeben. Auch ist das System von erheblichen „Währungsschwankungen“ betroffen, sodass der Eintausch der Bitcoins in „reale“ Währungen mit hohen Verlustrisiken verbunden sein kann.

3 Thesen zu den Implikationen für den Datenschutz und die Verbraucherpolitik

These 3.1: Das Datenschutzrecht muss modernisiert und an die Herausforderungen des 21. Jahrhunderts angepasst werden.

Die Europäische Kommission hat einen Regulierungsvorschlag vorgestellt, um ein europaweites Datenschutzrecht einzuführen. Ein solcher Schritt ist notwendig und überfällig. Insbesondere würde das neu eingeführte Marktortprinzip den Missstand abstellen, dass derzeit auf internationale Unternehmen nur schwer zugegriffen werden kann. Allerdings muss dafür Sorge getragen werden, dass hohe Datenschutzstandards, wie wir sie aus Deutschland kennen, nicht nach unten hin nivelliert werden. Auch ist sicherzustellen, dass das Datenschutzrecht als ein Teil des Verbraucherschutzrechts anerkannt wird. Denn nur dann können Verbraucherorganisationen ihre Verbandsklagerechte einsetzen, um etwa irreführende Datenschutzerklärungen abzumahnen. Dies ist ihnen heute nicht möglich.

These 3.2: Für einen präventiven Datenschutz müssen Aufsichtsbehörden ausreichend ausgestattet sein.

Unternehmen binden die Datenschutzaufsichtsbehörden bereits heute in die Entwicklung neuer Technologien ein. Hierdurch können die Datenschutzbehörden schon in der Entwicklung von Produkten und Dienstleistungen Einfluss darauf nehmen, wie diese ausgestaltet sind. In diesem Sinne können die Aufsichtsbehörden wesentlich flexibler und zügiger auf neue Entwicklungen reagieren als es der Gesetzgeber kann. Allerdings besteht ein finanzielles und personelles Ungleichgewicht zwischen Aufsichtsbehörden und Unternehmen.

These 3.3: Guter Datenschutz beginnt mit Privacy by Design und Datensparsamkeit.

In der Entwicklung von Produkten und Dienstleistungen sind der Datenschutz und die Datensparsamkeit von Anfang an konsequent zu berücksichtigen. So stellt sich beispielsweise bei Smart Metern die Frage, ob die Daten nicht vor Ort ausgewertet werden können, oder ob es nicht ausreicht, die Daten im 15-Minuten-Rhythmus anstelle eines 2-Sekunden-Takts zu übermitteln. Je weniger Daten erhoben und verarbeitet werden, desto geringer ist das Missbrauchsrisiko. Hier sind die Unternehmen gefordert, datensparsame Lösungen zu entwickeln und das Prinzip des Privacy by Design konsequent umzusetzen.

These 3.4: Datenschutz muss für Verbraucherinnen und Verbraucher einfach sein (Privacy by Default).

Die verhaltenswissenschaftliche Forschung zeigt, dass sich Verbraucherinnen und Verbraucher zumeist am Status-Quo und an Voreinstellungen orientieren. Häufig sind diese Voreinstellungen heute so ausgelegt, dass Verbraucherinnen und Verbraucher etwa bei sozialen Netzwerken möglichst viele Informationen über sich offenbaren. Einstellungsmöglichkeiten, um das Datenschutzniveau anzuheben, sind zwar vorhanden, aber nur schwer auffindbar. Anstatt Verbraucherinnen und Verbraucher den Selbstschutz zu erschweren, sollte die datensparsame Voreinstellung zur Standardeinstellung gemacht werden (Privacy by Default).

These 3.5: Technologien zur Gewährleistung der Datensicherheit existieren, sie müssen jedoch auch konsequent eingesetzt werden.

Die Datensicherheit kann in vielen Fällen durch Verschlüsselungen und Signierungen gewährleistet werden. So kann ausgeschlossen werden, dass unbefugte Dritte auf dem Transportweg einen Einblick in die Daten erhalten, oder Daten verfälscht und manipuliert werden. Allerdings müssen Unternehmen diese Technologien auch konsequent einsetzen.

These 3.6: Forschungsbedarf besteht insbesondere bei der Frage nach dem Zusammenhang zwischen Datenschutz und Verteilungsfragen.

Die Forschung im Bereich des Datenschutzes sollte in der Zukunft verstärkt die Frage aufgreifen, welche Auswirkungen unterschiedliche Datenschutzpraktiken auf die Verteilungsgerechtigkeit haben. Gerade Entwicklungen hin zu dynamisch auf die jeweiligen Verbraucherinnen und Verbraucher abgestimmte Suchergebnislisten und individualisierte Preise können sich negativ auf die Verteilungsgerechtigkeit auswirken.

Autorenverzeichnis

Dipl.-Jur. Sascha Adler ist Wissenschaftlicher Mitarbeiter und Doktorand am Lehrstuhl für Bürgerliches Recht, deutsches und internationales Wirtschaftsrecht, insbesondere IT-Recht an der Juristischen Fakultät der Ruhr-Universität Bochum.

Dr. Christian Bala ist Wissenschaftlicher Mitarbeiter des Kompetenzzentrums Verbraucherforschung NRW (KVF NRW).

Prof. Dr. Britta Böckmann vertritt das Lehrgebiet Medizinische Informatik an der Fachhochschule Dortmund, Fachbereich Informatik, und ist Leiterin der Arbeitsgruppe medizinische Informatik am IMIBE, Universität Duisburg-Essen.

Prof. Dr.-Ing. Rainer Böhme, M. A. ist Juniorprofessor für Wirtschaftsinformatik, insbesondere IT-Sicherheit an der Westfälischen Wilhelms-Universität Münster, Institut für Wirtschaftsinformatik.

Prof. Dr. Georg Borges ist Inhaber des Lehrstuhls für Bürgerliches Recht, deutsches und internationales Wirtschaftsrecht, insbesondere IT-Recht an der Juristischen Fakultät der Ruhr-Universität Bochum, Richter am Oberlandesgericht Hamm, Sprecher des Vorstands der Arbeitsgruppe Identitätsschutz im Internet (a-i3), Vorstandsmitglied des Horst-Görtz-Instituts für IT-Sicherheit (HGI) und Leiter der Arbeitsgruppe „Rechtsrahmen des Cloud Computing“ im Technologieprogramm „Trusted Cloud“ des BMWi.

Prof. Dr. Ulrich Greveler lehrt im Aufgabengebiet Angewandte Informatik an der Hochschule Rhein-Waal, Fakultät für Kommunikation und Umwelt.

Prof. Dr. Artus Krohn-Grimberghe ist Juniorprofessor für Analytische Informationssysteme und Business Intelligence am Department Wirtschaftsinformatik der Fakultät für Wirtschaftswissenschaften der Universität Paderborn.

Sebastian Luhn, MSc ist Wissenschaftlicher Mitarbeiter bei der Juniorprofessur für Wirtschaftsinformatik, insbesondere IT-Sicherheit an der Westfälischen Wilhelms-Universität Münster, Institut für Wirtschaftsinformatik.

Klaus Müller ist Vorstand der Verbraucherzentrale NRW.

Prof. Dr. Christoph Sorge ist Juniorprofessor für die Sicherheit in Netzwerken am Institut für Informatik der Fakultät Elektrotechnik, Informatik und Mathematik der Universität Paderborn.

Impressum

Verbraucherzentrale Nordrhein-Westfalen e. V.
Mintropstraße 27, 40215 Düsseldorf
Telefon: (02 11) 38 09-0, Telefax: (02 11) 38 09-235
www.vz-nrw.de

Die „Beiträge zur Verbraucherforschung“ werden von Dr. Christian Bala (für das Kompetenzzentrum Verbraucherforschung NRW) und Klaus Müller (für die Verbraucherzentrale Nordrhein-Westfalen e. V.) herausgegeben.

Das KVF NRW ist ein Kooperationsprojekt der Verbraucherzentrale NRW e. V. mit dem Ministerium für Klimaschutz, Umwelt, Landwirtschaft, Natur- und Verbraucherschutz (MKULNV) und dem Ministerium für Innovation, Wissenschaft und Forschung (MIWF) des Landes Nordrhein-Westfalen.

Die in diesem Band versammelten Beiträge geben die Meinung und die wissenschaftlichen Erkenntnisse der Autorinnen und Autoren wieder und müssen nicht mit den Meinungen und Positionen des KVF NRW, der Verbraucherzentrale NRW e. V., des MKULNV und des MIWF übereinstimmen.

Kontakt: Kompetenzzentrum Verbraucherforschung NRW (KVF NRW)
der Verbraucherzentrale Nordrhein-Westfalen e. V.
Mintropstraße 27, 40215 Düsseldorf
Telefon: (02 11) 38 09-0
E-Mail: verbraucherforschung@vz-nrw.de
www.verbraucherforschung-nrw.de

Lektorat:	Brigitte Schöning, www.plankundschoening.de
Gestaltung:	punkt8, Braunwald+Walter GbR, www.punkt8-berlin.de
Druck:	Stürtz GmbH, Würzburg

Gedruckt auf 100 Prozent Recyclingpapier.

Redaktionsschluss: Dezember 2013