§ Telemedicus

Sommerkonferenz

»Zwei Schritte vorwärts: Die Zukunft des Internetrechts«

Telemedicus e.V. (Hrsg.)

Zwei Schritte vorwärts: Die Zukunft des Internetrechts
Tagungsband zur Telemedicus Sommerkonferenz 2015

Telemedicus-Schriftenreihe
Band 2

Impressum
Verlag: epubli GmbH, Berlin
www.epubli.de

Alle Fundstellen, soweit sie ins Internet verweisen, wurden zuletzt überprüft am 15.05.2016.

Vorwort

„Die Zukunft des Internetrechts“ – mit der zweiten Telemedicus Sommerkonferenz 2015 hätten wir kaum ein größeres Thema wählen können. Und doch hätte kaum ein anderes Thema besser zu dem Konzept passen können, das wir mit der Sommerkonferenz verfolgen: Wir möchten querdenken, über die kurzfristig erreichbaren politischen Ziele hinaus schauen und Entwicklungen möglichst umfassend und interdisziplinär betrachten.

Mit dem Ergebnis sind wir ausgesprochen zufrieden. Mit insgesamt mehr als 150 Besuchern konnten wir Themen und Blickwinkel diskutieren, die auf juristischen Konferenzen häufig kaum eine Rolle spielen: Wie lässt sich Grundrechtsschutz technisch gewährleisten? Welche Rolle spielen Standards bei Regulierung im Internet und wie entstehen sie? Wie steht es um das europäische Datenschutzrecht jenseits aller Diskussionen um die Datenschutzgrundverordnung?

Im Namen des Telemedicus e.V. bedanke ich mich bei allen Speakern und Autoren dieses Tagungsbandes für ihre spannenden und bereichernden Beiträge und vor allem für die wertvollen Denkanstöße, mit denen sie unsere Konferenz bereichert haben. Ich danke auch den Teilnehmern unserer Konferenz für die engagierten und ausführlichen Diskussionen und die ausführlichen Wortbeiträge, die zum Teil selbst das Potenzial für einen eigenen Programmpunkt gehabt hätten und ihr Vertrauen, ihr wertvolles Wochenende in unsere Konferenz zu investieren.

Die Telemedicus Sommerkonferenz ist ein einzigartiges Gemeinschaftsprodukt vieler engagierter Menschen und Institutionen, die ohne Gewinnerzielungsabsicht und mit viel persönlichem und privatem Engagement die Konferenz stemmen: Ein besonderer Dank gilt deshalb auch unserem Organisationsteam,

das über fast ein Jahr einen gigantischen Aufwand betrieben hat, in seiner Freizeit und nach Feierabend im Vollzeitjob unsere Konferenz zu organisieren. Besonders hervorheben möchte ich dabei Lorena Jaume-Palasi, Rebecca Sieber und Hans-Christian Gräfe, ohne deren Organisationstalent die Sommerkonferenz sicher nicht hätte stattfinden können. Selbiges gilt auch für unsere Partner und Sponsoren, die den finanziellen Rahmen für die Sommerkonferenz durch monetäre wie durch ideelle Unterstützung geschaffen haben, namentlich BridgehouseLaw Germany (heute DWF Germany), das Deutsche Institut für Vertrauen und Sicherheit im Internet (DIVSI), HÄRTING Rechtsanwälte, die großartige Kommunikation & Recht, LEXEA Rechtsanwälte das Internet & Gesellschaft Collaboratory, das Alexander von Humboldt Institut für Internet und Gesellschaft, die Humboldt Law Clinic Internetrecht und – last but certainly not least – unsere Gastgeber, die Gemeinnützige Hertie Stiftung sowie die Hertie School of Governance.

Wir freuen uns bereits auf die Telemedicus Sommerkonferenz 2016 am 3. und 4. September 2016 in Berlin zum Thema „Die Macht der Plattformen“ – ein weiteres Thema, das aktueller und komplexer kaum sein könnte. Wir hoffen, Sie auch diesmal wieder begrüßen zu dürfen.

Adrian Schneider, Vorstand Telemedicus e.V.

Inhaltsverzeichnis

Thomas Söbbing

Das Berliner Gedankenexperiment

Zur Neuordnung des Urheberrechts in der digitalen Welt

Till Kreutzer

1 Einleitung

Man kann viel kritisieren am geltenden Urheberrecht und Kritik ist auch fast jeden Tag in den Medien zu lesen. Sie kommt von allen Seiten. Urheber beklagen sich darüber, dass sie von ihrer kreativen Arbeit nicht (mehr) leben können, unter anderem, weil sie von ihren Auftraggebern zu schlecht bezahlt werden. Plattenfirmen und Filmvertriebe und mitunter auch Urheber schimpfen über die bösen »Piraten«. Gemeint sind vorwiegend junge Leute, die das Netz dazu nutzen, wofür es gemacht wurde: zum Kommunizieren und zum Teilen (*sharing*) von Inhalten und Informationen. Die Bürger klagen über unfaire Regelungen und Massenabmahnwellen. Lehrer, Unidozenten und Museumsmitarbeiter darüber, dass ihnen das Urheberrecht die Arbeit unmöglich macht.

Die Frage, warum gerade das Urheberrecht derart viele Konflikte auslöst, ist gar nicht so leicht zu beantworten. Auf den ersten Blick handelt es sich um ein einleuchtendes Konzept: Wer kreative Leistungen (die Urheber) erbringt, soll mit einem Recht belohnt werden. Dieses soll ihnen ermöglichen, darüber zu entscheiden, wer ihre Werke zu welchen Konditionen nutzen darf. Das Recht versetzt sie in die Lage, Veröffentlichungen zu erlauben (oder zu verbieten), hierfür Geld oder andere Gegenleistungen zu verlangen. Dieser Ansatz ist im Grundsatz richtig und notwendig. Allerdings sind die Fragen, die vom Urheberrecht beantwortet werden sollen, gerade in der digitalen Welt viel komplexer. An kulturellen Leistungen – wie sie vom Urheberrecht geschützt werden – bestehen vielfältige Interessen. Urheber benötigen den genannten Werkschutz. Unternehmen wollen mit den Werken, die nicht sie, sondern die Urheber erzeugen, Geld verdienen. Die Gesellschaft ist an ihrer Nutzbarkeit und daran interessiert, auf sie zugreifen zu können. Öffentliche Einrichtungen wie Museen, Archive oder Universitäten müssen sie ausstellen oder präservieren, im Unter-

richt oder zur Forschung nutzen können, um ihren gesamtgesellschaftlichen Auftrag zu erfüllen. Kurzum: Das Urheberrecht ist nicht lediglich ein »Recht für den Urheber«, sondern es ist ein komplexes Instrument, mit dem vielfältige Interessen ausgeglichen werden müssen. Nicht nur, dass dieser Interessenausgleich sehr sensibel ist. Er muss auch immer wieder überprüft und gegebenenfalls angepasst werden, wenn sich die Zeiten, die Nutzungsmöglichkeiten und -gewohnheiten ändern. Noch nie war dieser Anpassungsdruck so groß, wie beim Übergang in die digitale Welt. Das Problem ist jedoch: Diese Anpassung ist bis heute – ca. 20 Jahre, nachdem das World Wide Web entstanden ist – nicht erfolgt. Das hat viele Gründe, von denen ein wesentlicher darin zu liegen scheint, dass sich niemand vorstellen kann, wie alternative Konzepte zum Urheberrecht aussehen könnten.

Dem soll das »Berliner Gedankenexperiment« Abhilfe schaffen. Hierbei handelt es sich um ein von einer kleinen und unabhängigen Expertengruppe entwickeltes neues Modell für das, was heute als Urheberrecht bekannt ist. Die dahinter stehenden Autoren stammen aus verschiedensten Berufen, es sind Juristen, Musikwirtschafts- und Verlagsexperten, Soziologen. Sie sollten in dem von mir ins Leben gerufenen Projekt folgende Frage beantworten: Angenommen, es gäbe kein Urheberrecht. Wie würde man ein Instrument konzipieren, das den Schutz, die Nutzung und den Umgang mit kreativen Schöpfungen in der digitalen Welt regelt, das praktikabel, effizient und zukunftsträchtig ist? Hierbei sind interessante Erkenntnisse entstanden, die hier kurz zusammengefasst werden (das vollständige Papier ist unter http://irights.info/wp-content/uploads/2015/08/Gedankenexperiment.pdf abrufbar).

2 Systematik: Trennung verschiedener Interessengruppen

Um die in sich verwobenen und überschneidenden Interessen an Unterhaltungs- und Kulturgütern zu entflechten, differenziert das Gedankenexperiment zunächst zwischen vier Akteursgruppen, und stellt in diesbezüglichen eigenständigen Abschnitten Regeln über ihre Rechte und Pflichten auf. Diese Interessengruppen sind: Urheber, Verwerter, Nutzer und Vermittler (Online-Intermediäre). Kollidieren die Interessen der einen mit einer anderen Gruppe, ergibt sich der Interessenausgleich aus dem Verhältnis des einen Rechts zu dem jeweils anderen. Ein Beispiel: Haben Nutzer ein Recht zu zitieren, können Zitate nicht verboten werden, weder vom Urheber noch vom Verwerter. Das Zitatrecht ist also – anders als im geltenden Urheberrecht – keine Ausnahme vom ausschließlichen Urheber- oder Verwerterrecht, sondern es ist ein eigenes Recht der Nutzer, das von den Ausschließlichkeitsrechten nicht erfasst wird. Einer der Effekte ist, dass Zitate nicht vertraglich (durch AGB, Nutzungsbedingungen) oder sonst wie (z. B. durch Kopierschutzsysteme) ausgeschlossen werden können. Der Nutzer könnte sein Zitatrecht sogar aktiv vor Gericht einklagen.

3 Urheber- und Verwerterrecht

Der Antwort auf die Frage, wie das Verhältnis zwischen Urhebern und Verwertern auszugestalten ist, lag eine elementare Erkenntnis zugrunde: Das Urheberrecht leidet an einem Geburtsfehler. Es heißt zwar Urheberrecht, wird aber in den weitaus meisten Fällen gar nicht vom Urheber, sondern einem Verwerter, also einem kommerziellen Unternehmen, wahrgenommen. Zwar entsteht das Urheberrecht stets beim Urheber und kann von diesem auch nicht abgetreten werden. Faktisch kann der Urheber aber durch einen einzigen Handstreich, seine Unterschrift unter einen Vertrag oder einen Klick auf die »Autorenbedingungen« in einem Online-Formular, mehr oder weniger alle Rechte weggeben. Exklusiv und für alle Zeiten. Das nennt man total-buyout. Und das tun ganz viele Urheber ständig, weil ihnen gar nichts anderes übrig bleibt. Natürlich gibt es Musiker oder Schriftsteller, die Verträge aushandeln und eigene Bedingungen durchsetzen können. Natürlich gibt es auch Urheber, die sich selbst verlegen, eigene Labels und Musikverlage gründen oder im Selbstverlag publizieren. Im Verhältnis zu den Abermillionen Kreativschaffenden, die in (häufig: prekären) Abhängigkeitsverhältnissen zu Presseverlagen, Grafikagenturen oder Produktionsfirmen arbeiten, sind aber die Urheber, die tatsächlich über ihre Rechte verfügen können, eine kleine Minderheit.

Hierdurch kommt es zu einer Inkonsistenz zwischen dem was das Urheberrecht sein soll und dem was es meistens ist. Offiziell wird das Urheberrecht an den Bedürfnissen des Kreativschaffenden ausgerichtet. Faktisch liegt es aber in den weitaus meisten Fällen in den Händen von Wirtschaftsunternehmen. Wenn nicht der Künstler, dem das Urheberrecht zustehen und von Nutzen sein soll, es ausübt, sondern ein Unternehmen, erfolgt eine faktische Umwidmung mit erheblichen Folgen. Firmen haben andere Interessen und daher andere Anforderungen an ein solches Recht und sie gehen auch anders damit um. Man stelle

sich etwa folgende Fragen: Würden hunderttausende deutsche Haushalte jedes Jahr abgemahnt, wenn hierüber die Musiker entscheiden würden? Würden die Autoren massiv gegen Regelungen lobbyieren, die Hochschullehrern Nutzungen zu wissenschaftlichen Zwecken erlauben oder Archiven, das kulturelle Erbe zu erhalten, ohne hierfür Rechte klären zu müssen? Ist es zu rechtfertigen, dass Filmkonzernen über vom Urheber abgeleitete exklusive Nutzungsrechte verfügen, die ihnen über hundert Jahre lang Exklusivität gewähren?

Um ein wirkliches Urheberrecht zu sein, fehlt es dem Urheberrecht an einem wesentlichen Mechanismus: Dass die hieraus fließenden Befugnisse des Urhebers nicht auf ein Unternehmen übertragen werden können. Nur dann ist sichergestellt, dass die auf ihn ausgerichteten Schutzrechte nicht entgegen ihrer Rechtfertigung und ihrer Zielrichtung verwendet werden können. Diesen Mechanismus führt das Gedankenexperiment ein. Die Urheber erhalten ein Recht, das nur ihnen zustehen kann und das daher der Realität entsprechend an ihren Bedürfnissen ausgestaltet ist. Die Verwerter erhalten eigene Rechte, die wiederum auf sie zugeschnitten sind. Anders als im Vergleich der heutigen Urheber- und Leistungsschutzrechte werden sich Urheber- und Verwerterrechte dabei grundlegend unterscheiden. Das Urheberrecht wird nach wie vor relativ lange Schutzfristen und im Anschluss wirtschaftliche Beteiligungsansprüche vorsehen, um die Alimentations- und Vergütungsinteressen kreativer Menschen zu schützen. Das Verwerterrecht ist dagegen – seiner eigentlichen Bestimmung entsprechend – als Investitionsschutzrecht mit relativ kurzen Exklusivrechten und gewissen Verlängerungsmöglichkeiten nach Registrierung konzipiert. Vorbild hierfür ist das Patentrecht.

4 Nutzerrecht und Vermittler

Wie gesagt weist das Gedankenexperiment den Nutzern eigene Rechte zu. Der angestrebte Effekt ist ähnlich wie beim Urheberrecht. Die momentane Situation ist so: Die Gesetzgeber schaffen in aufwändigen Prozessen ausgewogene Nutzungsfreiheiten. Diese werden dann – handstreichartig – millionenfach durch nicht-verhandelbare Standardverträge wie AGB wieder ausgeschlossen und/oder durch technische Schutzmaßnahmen ausgehebelt. Dadurch wird der gesetzlich vorgesehene Interessenausgleich unterminiert und die Interessenkonstellation einseitig durch die Verwerter zu ihren eigenen Gunsten abgeändert. Bei unveränderbaren und durchsetzbaren Nutzerrechten wäre dies unmöglich.konzipiert.

Die Regeln über Vermittler, wie Plattformanbieter, soziale Netzwerke oder Host-Provider werden ebenfalls in einem Abschnitt geregelt. Das bisherige Urheberrecht sieht solche Regelungen nicht vor, obwohl solche Dienste bei der Nutzbarmachung von Werken in der digitalen Welt eine gewaltige Rolle spielen. Das Gedankenexperiment sieht Vermittler dabei weder als Rechteinhaber noch als Nutzer, sondern als eine vierte eigenständige Interessengruppe. Da auch deren Tätigkeit zu Kollisionen mit den Interessen anderer Akteure führen kann – man denke nur an die Auseinandersetzung zwischen der GEMA und YouTube – müssen sie in dem Regelungsmodell eine Rolle spielen.

Das Konzept sieht vor, Vermittler in verschiedene Gruppen einzuteilen, um das unterschiedliche Kollisionspotenzial mit den Interessen von Urhebern, Verwertern und Nutzern entsprechend zu gewichten. Grundsätzlich werden Vermittler mit Komplementär- und Konkurrenzangebot unterschieden. Bei ersteren ist davon auszugehen, dass ihre Dienste nicht mit den Angeboten von Rechteinhabern konkurrieren, sondern diese eher ergänzen und daher potenziell nützlich

sind. Hierunter fallen z. B. Internet-Zugangsprovider oder Suchdienste. Potenzielle Konkurrenzangebote von Vermittlern sollen dagegen in den Interessenausgleich einbezogen werden. Sind sie klar darauf ausgerichtet, Rechtsverletzungen zu fördern, können sie gänzlich verboten werden. Handelt es sich dagegen um Infrastrukturdienste, die Nutzern (auch) dazu dienen, geschützte Inhalte Dritter zu teilen, sollen ihnen von den Nutzern abgeleitete Vergütungspflichten auferlegt werden können. Dies würde sich z. B. auf Videoplattformen oder u. U. auch soziale Netzwerke beziehen. Das Konzept ähnelt den Geräte- und Leermedienabgaben. Zwar kopieren die Hersteller und Händler von USB-Sticks oder Festplatten keine Werke. Weil aber ihre Kunden dies tun und sie davon auch profitieren, werden sie gewissermaßen zum Inkasso für die Tantiemen verpflichtet, die eigentlich die Nutzer zahlen müssten. Bei Plattformprovidern ist die Situation letztlich genauso.

5 Ausblick

Wie der Name schon sagt, verkündet das Gedankenexperiment keine Wahrheiten. Viele der hier entwickelten konzeptionellen Ideen müssen diskutiert, weiterentwickelt oder letztlich vielleicht auch wieder verworfen werden. Es versteht sich als Diskussionsbeitrag für eine Debatte, die sich seit Jahrzehnten nicht um grundlegende Aspekte, sondern nur um Feinkorrekturen dreht. Eines sollte dabei klar sein: Das Urheberrecht ist heute eines der bei der Bevölkerung am wenigsten akzeptierten Regelungsfelder. Ohne Akzeptanz wird es keinen wirksamen Schutz entfalten, schon gar nicht in der digitalen Welt. Es ist daher höchste Zeit, ernsthaft über Alternativen zu diskutieren und hierbei auch grundlegende Änderungen zu untersuchen, abzuwägen und zu diskutieren. Das wäre im Sinne aller Akteure, der Urheber, Verwerter und Nutzer.

Hinweis: Dieser Beitrag erschien zuerst in Neue Rundschau, Heft 4 2015, S. 95 ff.

Internetrecht der Dinge

Sven-Erik Heun/Simon Assion

In viele Gegenstände des täglichen Lebens werden mittlerweile Speichermedien, Prozessoren und Kommunikationseinrichtungen eingebaut, z.B. SIM-Karten oder RFID-Chips.[1] Einfache Gegenstände erlangen die Fähigkeit, mit ihrer Umwelt zu interagieren, werden zu „Smart Devices". Typische und vielgenannte Beispiele sind Smart Cars, Smart Meters oder Wearables.

Von wirtschaftlicher Bedeutung ist aber auch die „Industrie 4.0": Ganze Produktionsprozesse werden durch die Kommunikations- und Interaktionsfähigkeit der eingesetzten Maschinen und Werkstücke umgestaltet. Es gibt z.B. „smarte" Container, Bahnweichen oder ganze Energienetze, die mit intelligenten Netzkomponenten ausgestattet sind (Smart Grids).

Am schnellsten geht es in der Konsumentenelektronik: Etwa jeder zweite Deutsche hat mittlerweile ein Smart Phone, und auch Smart Watches und sonstige Wearables werden in absehbarer Zeit ein Alltagsphänomen sein.[2] Auch bei der Heimelektronik geht es schnell: Im Jahr 2015 waren bereits 20,1 % der in den Haushalten aufgestellten TV-Geräte sog. „Smart TV".[3]

---

[1] Der vorliegende Vortrag wurde in einer anderen Variante bereits in CR veröffentlicht (CR 2015, 812). Die Autoren danken Herrn *Valerian Jenny* und Herrn *Baris Batur* für Unterstützung und Ideen.

[2] Pressemitteilung von *Bitkom* vom 25.03.2015, abrufbar unter https://www.bitkom.org/Presse/Presseinformation/44-Millionen-Deutsche-nutzen-ein-Smartphone.html.

[3] Die Medienanstalten, Digitalisierungsbericht 2015, abrufbar unter http://www.die-medienanstalten.de/publikationen/digitalisierungsbericht.html, S. 49.

Die zunehmende Relevanz des „Internet der Dinge“ führt dazu, dass die klassischen Disziplinen des Internetrechts (Immaterialgüterrecht, Datenschutzrecht, Telekommunikationsrecht) auf Sachverhalte treffen, die früher fast ausschließlich im Sachenrecht behandelt wurden. Es entstehen somit ganz neue juristische Konstellationen. Denn im „Internet der Dinge“ sind die physischen Gegenstände nicht nur „Sachen“, sondern auch Träger von immaterialgüterrechtlich geschützten Inhalten und personenbezogenen Daten. Und häufig sind die Smart Devices, die an das Internet der Dinge angeschlossen sind, auch Teile eines Telekommunikationsdienstes im Sinn des TKG und unterfallen deshalb der telekommunikationsrechtlichen Regulierung.

1 Das Internet der Dinge als rechtliche Herausforderung

Was zeichnet einen zum „Internet der Dinge“ gehörenden Gegenstand („Smart Device“) aus? Abstrakt formuliert: Die Fähigkeit, Daten aufzunehmen, zu speichern, zu verarbeiten und auf Basis der Datenspeicherungs- oder Datenverarbeitungsergebnisse mit der Umwelt zu kommunizieren. Kennzeichnend für das Phänomen „Internet der Dinge“ ist, dass diese Fähigkeit sich nicht mehr nur auf Computer und Kommunikationsgeräte beschränkt, sondern auf Alltagsgegenstände ausweitet.

Diese Beschreibung zeichnet bereits vor, welche Rechtsfragen sich stellen: Während Alltagsgegenstände dem darauf zugeschnittenen „Alltagsrecht“ unterfallen, also dem allgemeinen Sachen- und Schuldrecht, ändert sich dieses Bild, wenn die Alltagsgegenstände zu informations- und kommunikationstechnischen Einrichtungen werden.

Denn einerseits gilt für „Dinge“ primär das Sachenrecht. Also eines der ältesten Rechtsgebiete überhaupt, das die Zuordnung von beweglichen und unbeweglichen körperlichen Gegenständen („Sachen”) zu ihrer Umwelt betrifft. Wenn die „Dinge“ aber auch Daten speichern und verarbeiten und mit ihrer Umwelt kommunizieren, können sie auch dem klassische Kanon des Internetrechts unterfallen: Urheberrecht, Datenschutzrecht, Telemedienrecht, Telekommunikationsrecht. Also alles Rechtsgebiete, bei denen es darum geht, Unkörperliches rechtlich zu erfassen – Informationen und Kommunikationsvorgänge.

Im „Internetrecht der Dinge” treffen deshalb erstmals Rechtsgebiete aufeinander, die bisher wenig miteinander zu tun hatten. Das daraus entstehende Konflikt- und Konkurrenzverhältnis ist bisher nur wenig erschlossen.

Beispielhaft sei hier die Debatte erwähnt, die sich um intelligente Fahrzeuge entsponnen hat.[4] Denn an diesen „Smart Cars" machen die Hersteller teils noch Rechte geltend, auch nachdem die Fahrzeuge den Besitzer (und oftmals auch Eigentümer) gewechselt haben. Rechtlich gesehen erfolgt diese Behauptung nicht ganz zu Unrecht, denn die auf den Fahrzeugen gespeicherte Software ist als solche urheberrechtlich geschützt; diese Rechtsstellung wird mit Übereignung des Fahrzeugs nicht aufgehoben. Die aus dem Urheberrecht abgeleiteten Rechte können mit sachenrechtlichen Wertungen kollidieren. Das Fachmagazin Wired inspirierte eine solche Auseinandersetzung zu der Überschrift „We can´t let John Deere Destroy the very Idea of Ownership".[5]

Ein anderes Beispiel für einen (potenziell rechtlichen) Konflikt im „Internet der Dinge" ist die Debatte um intelligente Spielzeuge, insbesondere Puppen. Beispielsweise wurde bezogen auf die sog. Furbys behauptet, diese würden in Wohnungen „spionieren".[6] Dies stellte sich später als Falschmeldung heraus. Heute gibt es allerdings eine Barbie-Puppe, die derartige Funktionen hat.[7]

Es kann im „Internet der Dinge" dazu kommen, dass an einem Gegenstand mehrere Personen oder Institutionen Verfügungsrechte haben. Smart Devices „gehören" also häufig nicht nur einer Person, sondern mehrere Personen haben verschiedene Kontroll- und Verfügungsbefugnisse – und diese Rechte ergeben sich aus verschiedenen Rechtgebieten.

---

[4] *Grosskopf* IPRB 2011, 259; *Weisser/Färber* MMR 2015, 506; *Hornung/Goeble* CR 2015, 265

[5] *Wired* vom 21.04.2015, abrufbar unter http://www.wired.com/2015/04/dmca-ownership-john-deere/.

[6] Statt vieler World News Daily Report vom 7. April 2014, http://worldnewsdailyreport.com/snowden-revelation-nsa-used-furbies-for-domestic-spying/.

[7] Zur sog. „Hello Barbie" *Wiebusch*, Tagungsband DSRI Herbstakademie 2015, 157.

Wir erörtern in im Folgenden zunächst die Fragen, wem ein Smart Device eigentlich „gehört“ (dazu Abschnitt 2) und wie das „Internet der Dinge“ sich aus Sicht des Telekommunikationsrechts beurteilt (Abschnitt 3). Im Anschluss erörtern wir Praxisfälle und die zugehörigen Lösungsansätze (Abschnitt 4). Abschnitt 5 enthält eine Zusammenfassung und Schlussbemerkung.

2 Wem „gehört“ ein Smart Device?

Die Grundfrage ist, wem ein Device – und speziell die darauf enthaltenen bzw. davon produzierten Daten – eigentlich „gehören“. Wer bestimmt, was das Gerät „tut”, was es „kann”, was es nicht kann? Dies hängt vor allem der aufgespielten Software ab, aber auch von den zur Verfügung gestellten Daten und der Verknüpfung mit Dienstleistungen, die zur Unterstützung des Device angeboten werden (z.B. die Zurverfügungstellung von Clous-Speicher, Cloud-Rechenkapazität oder Konnektivität). An dieser Software, an den Daten, an den zur Verfügung gestellten Dienstleistungen bestehen unterschiedliche Rechtspositionen. Je nach Perspektive können diese Fragen also unterschiedlich beantwortet werden.

Rechtlich gesehen geht es um *rechtliche Handlungsbefugnisse* betreffend das Device bzw. der Daten.[8] Derartige Handlungsbefugnisse können sich aus ganz unterschiedlichen Rechtsgebieten ergeben.[9]

In der Praxis ist bisher vor allem die Frage von hoher Relevanz, wem die *Daten* eines solchen Smart Device gehören, denn derartige Daten können sehr wertvoll sein. Beispielsweise können die Bewegungsdaten von intelligenten Fahrzeugen für die Steuerung des Straßenverkehrs, für Verkehrsmeldungen im Radio und für Navigationsempfehlungen (Routenplanung) relevant sein. Telemetriedaten von Landfahrzeugen geben Auskunft über die Ertragsstärke bestimmter geografischer Gebiete. Sensor- und Benutzungsdaten von intelligenten Fertigungsmaschinen (Stichwort „Industrie 4.0“) helfen deren Herstel-

[8] *Zech,* CR 2015, 137 (139); im wirtschaftlichen Kontext lässt sich auch von Verwertungsrechten sprechen, vgl. *Schefzig*, Tagungsband DSRI-Herbstakademie 2015, 551 (560).
[9] Zu rechtlichen Vermögenszuweisungen an Daten *Schefzig,* K&R Beih. 3/2015 zu Heft 3, 3; *Peschel/Rockstroh,* MMR 2014, 571; *Dorner,* CR 2014, 617.

lern bei der Weiterentwicklung, aber auch deren Eigentümern bei der Früherkennung von Mängeln und der Festlegung von Wartungsintervallen. Und die Kommunikations- und Nutzungsdaten, die von Wearables oder Smartphones über ihre Benutzer erhoben werden, sind Grundlage ganz unterschiedlicher Geschäftsmodelle, z.B. zum Targeted Advertising, zur Generierung von Produktempfehlungen oder zur Ermöglichung und Verbesserung von Dienstleistungsprodukten (z.B. Fitnessprogrammen).

Zu dieser Frage sind bereits einige Meinungen vertreten worden.[10] Häufig konzentrieren sich diese Auseinandersetzungen einseitig auf bestimmte Rechtsgebiete, z.B. das Strafrecht. Richtigerweise kann aber (wie unten noch darzustellen ist) nur eine Gesamtbetrachtung aller in Frage kommenden Rechtsnormen zu einer korrekten Lösung führen.

2.1 Das Sachenrecht: Die Rechte am physischen Gegenstand

Die Rechte am physischen Gegenstand selbst bestimmen sich nach den grundlegenden Prinzipien des Sachenrechts. Das Sachenrecht ist das Recht der „Sachen", d.h. der körperlichen Gegenstände. Auf informationsrechtliche Zusammenhänge nimmt es keine Rücksicht. Vielmehr regelt es, wer im Bezug auf bewegliche und unbewegliche Sachen dingliche (d.h. gegen jedermann wirkende) Herrschaftsrechte geltend machen kann.

---

[10] *Zech* CR 2015, 137; *ders*. GRUR, 2015,1151; *Schefzig* K&R 2014, 772; *ders*. Tagungsband DSRI-Herbstakademie 2015, 551; *Peschel/Rockstroh* MMR 2014, 571; *Dorner* CR 2014, 617; *Hoeren* MMR 2013, 486; *Kraus* Tagungsband DSRI-Herbstakademie 2015, 537; *Hornung/Goeble* CR 2015, 265; *Krätzschmar* Tagungsband DSRI-Herbstakademie 2015, 753; *Arkenau/Wübbelmann* Tagungsband DSRI-Herbstakademie 2015, 95; *Heun/Assion* CR 2015, 812 ff.; *Hoppen* CR 2015, 802 f.; *Vogelgesang* jM 2016, 2.

Sachenrechtlich geschützte Rechtspositionen gibt es vielerlei. Wir beschränken uns an dieser Stelle auf die zwei wohl wichtigsten, nämlich das Eigentum und den Besitzschutz.

2.1.1 Eigentum

Das Eigentum ist das grundlegende Sachenrecht. Es liegt als „Mutterrecht“[11] allen anderen Sachenrechten zugrunde und regelt – soweit nicht andere, vorrangige Rechtspositionen bestehen – wem eine Sache „gehört“. Ein Eigentümer kann insbesondere, „soweit nicht das Gesetz oder Rechte Dritter entgegenstehen, mit der Sache nach Belieben verfahren und andere von jeder Einwirkung ausschließen“ (§ 903 Satz 1 BGB). Aus dem Eigentum leiten sich eine Reihe von Anspruchsgrundlagen ab, u.a. der Anspruch auf Unterlassung und Beseitigung von Störungen (§ 1004 BGB), der Herausgabeanspruch nach § 985 BGB und ein Schadensersatzanspruch (§ 823 Abs. 1 BGB).

Betreffend Daten, die von einem Device erzeugt werden, ist vertreten worden, diese seien „Früchte” der Sache (§ 99 BGB).[12] Dies ist zurückzuweisen, weil Daten als rein immaterielle Vermögensvorteile dem Regime des § 99 BGB nicht sinnvollerweise unterfallen können. Das heißt allerdings nicht, dass jeder sachenrechtliche Zugang zu dem Thema versperrt wäre. Denn auch für unkörperliche Erzeugnisse sieht das Sachenrecht eine Kategorie vor: Sie lassen sich als *Nutzungen* der Sache (§ 100 BGB) behandeln.[13] Nutzungen sind auch „sonstige Vorteile“, müssen also keine körperlichen Gegenstände sein. Ihr wirtschaftlicher Wert wird u.a. im Bereicherungsrecht erfasst: Gem. § 818 BGB sind auch „gezogene Nutzungen” herauszugeben bzw. hierfür Wertersatz zu leisten. Soweit keine spezialgesetzliche Regelung eingreift, gebühren Nutzungen dem

[11] *Wilhelmi,* in Erman, BGB, 14. Aufl. 2014, Vorbemerkung (vor §§ 903 ff.), Rn. 2.
[12] *Grosskopf* IPRB 2011, 259.
[13] *Zech* CR 2015, 137, 142.

Eigentümer.[14] Die unberechtigte Nutzungsziehung kann der Eigentümer, soweit sie mit einer Integritätsverletzung des Eigentums einhergeht, untersagen (§ 1004 BGB).[15]

Diese Rechtsgedanken lassen sich auch auf Daten anwenden. Die unberechtigte Datenentnahme kann ein Eigentümer verbieten;[16] die unberechtigt gezogenen Daten bzw. deren Wert kann er als rechtsgrundlose Bereicherung herausverlangen. Dies führt aber nicht zu einem allgemeinen „Dateneigentum". Denn zwar mag die individuell verkörperte Manifestation von Daten auf dem Device (oder dem von ihm bespielten Datenträger) eine „Nutzung" sein.

Die vorstehende Überlegung lässt sich allerdings nicht auf Daten übertragen, deren Erzeugung sich nicht einem konkreten „Smart Device" zuordnen lässt, denn hier greift dann auch nicht mehr der Zuweisungsgehalt des Eigentums. Dasselbe gilt für Informationen (d.h. weitere Daten), die aus den vom Device erzeugten Rohdaten abgeleitet werden. Es gibt also kein aus dem Eigentum abgeleitetes Ausschließlichkeitsrecht an Daten in dem Sinn, wie es z.B. das Urheberrecht verleiht. Insofern bleibt es, wenn keine andere Rechtsposition eingreift, beim Know How-Schutz (dazu unten, Abschnitt 2.2.3).

2.1.2 Besitzschutz

Der Besitzschutz betrifft, anders als das Eigentum, keine Rechtsposition, sondern schützt die tatsächliche Sachherrschaft (§ 854 Abs. 1 BGB). Der Besitzer hat ebenfalls die Befugnis, Störungen in Form von Unterlassungs- und Beseitigungsansprüchen abzuwehren (§ 862 BGB). Der Besitz ist ein i.S.d. § 823 Abs. 1

---

[14] *Stresemann*, in: MüKo BGB, 7. Aufl. 2015, § 100 Rz. 8; vgl. auch § 903, § 446 Satz 2 und die § 987 ff. BGB.
[15] *Zech* CR 2015, 137, 142.
[16] *Zech* CR 2015, 137, 142.

BGB geschütztes absolutes Recht,[17] berechtigt bei Besitzstörungen also auch zu Schadensersatzansprüchen.

Ein allgemeines Recht auf *Nutzungsziehung* ergibt sich aus dem sachenrechtlichen Besitzschutz nicht. Allerdings ergibt sich ein Recht auf Nutzungsziehung häufig, wenn ein Besitzer auch schuldrechtlich zum Besitz berechtigt ist. Z.B. ist der Mieter einer Wohnung auch berechtigt, diese zu nutzen. Die Nutzungsvorteile der Wohnung gebühren (in dem vertraglich zugewiesenen Umfang) ihm. Gleiches gilt im Grundsatz auch für „Smart Devices“: Wenn deren Eigentümer das Recht auf Nutzungsziehung betreffend Daten schuldrechtlich einem anderen als dem Besitzer zugewiesen hat, dann gebührt der Erstzugriff bzw. das Verwertungsrecht der Daten zunächst diesem Dritten.

2.2 Das Informationsrecht: Rechte an Informationen

Mit dem Sachenrecht – das im Grundsatz an den *physischen* Gegenstand anknüpft – kollidieren im „Internet der Dinge“ die Rechtsgebiete des *Informations*rechts. Dies sind insbesondere das Datenschutzrecht (Abschnitt 2.2.1), das Urheberrecht (Abschnitt 2.2.2) und der subsidiäre Know-How-Schutz (Abschnitt 2.2.3). Teils wird auch versucht, aus dem Information- bzw. Datenstrafrecht einen eigenständigen und zusätzlichen Immaterialgüterrechtlichen Schutz herzuleiten (Abschnitt 2.2.4).

2.2.1 Datenschutzrecht

Das Datenschutzrecht schützt trotz seines irreführenden Namens keine „Daten”, sondern Menschen. Geschützt sind deshalb nur Daten, die personenbezo-

[17] Zur nicht unproblematischen Herleitung nur *Wagner* in MüKo, BGB, 6. Aufl. 2013, § 823 Rn. 220.

gen sind, aus denen sich also Informationen konkret bezogen auf einzelne Menschen ableiten lassen (§ 3 Abs. 1 BDSG).

Nicht alle Daten im „Internetrecht der Dinge“ sind personenbezogen. Z.B. Angaben zur Betriebstemperatur einer Maschine sind dies im Regelfall nicht. Allerdings lassen sich im Zeitalter von Big Data viele Daten durch Korrelation mit anderen Daten personenbezogen machen – bei unterschiedlich viel Aufwand. Ob dies zur Einbeziehung solcher Daten in den Schutzbereich des Datenschutzrechts führt, ist Gegenstand eines juristischen Meinungsstreits. Mit dessen Lösung befasst sich u.a. gerade auch der EuGH.[18]

Das Recht am personenbezogenen Datum ist kein Vermögensrecht im engeren Sinne. Es gehört zum allgemeinen Persönlichkeitsrecht und soll einzelne Personen („Betroffene”) davor schützen, dass ihre personenbezogenen Daten übermäßig bzw. ohne Rechtfertigung erhoben, verarbeitet, genutzt und weitergegeben werden. Das Datenschutzrecht nutzt für diesen Zweck aber zwei Methoden, die es sehr nah an die Systematik des klassischen Immaterialgüterrecht bringen: Einerseits das Verbot mit Erlaubnisvorbehalt (§ 4 BDSG), andererseits die Möglichkeit des Betroffenen, jenseits gesetzlicher Erlaubnisse auch eine Einwilligung in die Verwendung seiner personenbezogenen Daten zu erteilen (u.a. § 4a BDSG). Dieser (vielfach durchbrochene) Grundsatz des Datenschutzrechts ergibt sich aus dem Grundrecht auf informationelle Selbstbestimmung.[19]

In der Praxis führt die grundsätzliche Zuweisung des „Rechts am eigenen Datum“ dazu, dass häufig personenbezogene Daten als wirtschaftlich relevantes Vermögensgut eingesetzt werden. In vielen Situationen übergibt ein Betroffener „seine“ Daten absichtlich als Teil einer Transaktion, verbunden mit der

[18] Das Verfahren ist beim EuGH anhängig als Rs. C-582/14.
[19] BVerfGE 65, 1 (43) – *Volkszählung*; vgl. zum informationellen Selbstbestimmungsrecht als „Dateneigentum“ auch *Dorner*, CR 2014, 617 (624).

Einwilligung in deren wirtschaftliche Verwertung. Der Betroffene erteilt also seinem Geschäftspartner eine Art „Lizenz zum Datenverwenden" – als vermögenswertes Gut. Im Regelfall wird diese Lizenz aber nicht in Geld aufgewogen, sondern gegen Dienstleistungen eingetauscht.

Das Datenschutzrecht verleiht dem Betroffenen für den Fall, dass weder eine gesetzliche noch rechtsgeschäftliche Einwilligung zur Datenverwendung vorliegt, verschiedene Abwehrrechte. Der Betroffene hat das Recht, die Erhebung, Verarbeitung und Nutzung seiner personenbezogenen Daten zu gestatten (u.a. § 4, § 4a BDSG); er kann dies im Wege des Widerspruchs (u.a. § 28 Abs. 4, § 35 Abs. 5 BDSG) oder sogar Löschungsverlangens (§ 35 Abs. 2 BDSG) auch untersagen. Sowohl die Gestattungs-, als auch die Untersagungsansprüche sind jedoch vielfach durch gesetzliche Bestimmungen durchbrochen.

Ein absolutes Verfügungsrecht an Smart Devices und den von ihm erzeugten Daten ergibt sich aus dem Datenschutzrecht nicht. Aber das Datenschutzrecht vermittelt durchaus konkrete Ansprüche, die der Betroffene erheblichen Einfluss darauf vermittelt, was ein Device mit „seinen" Daten tut. Durch die Möglichkeit, die eigene Einwilligung auch an Bedingungen zu knüpfen, kann er diesen Einfluss auch in Form konkreter Rechtsgeschäfte umsetzen.

2.2.2 Urheberrecht

In vielerlei Hinsicht ergeben sich Rechte an Smart Devices auch aus dem UrhG, bzw. aus dem allgemeinen Immaterialgüterrecht. Denn auf Devices sind Informationen gespeichert, die immaterialgüterrechtlich geschützt sein können. Das betrifft vor allem den Schutz von Software (dazu 2.2.2.1), von Datenbanken (2.2.2.2), aber letztlich jede Information, die immaterialgüterrechtlichen Schutz genießt (allgemein dazu 2.2.2.3).

2.2.2.1 Software

Der immaterialgüterrechtliche Schutz von Software ist in Deutschland im Urheberrechtsgesetz geregelt, im Wesentlichen in den §§ 69a ff. UrhG. Der jeweilige Rechteinhaber an der Software – das ist meist der Programmierer oder dessen Arbeitgeber – hat die klassischen immaterialgüterrechtlichen Abwehrrechte, also insbesondere auf Unterlassung, Beseitigung und Schadensersatz.

Der Schutz des Softwareherstellers betrifft die „Ausdrucksform" eines Computerprogramms und verleiht – vorbehaltlich gewisser spezieller, vor allem in den §§ 69d und 69e UrhG geregelter Ausnahmen – den Schutz der § 97 ff. UrhG. Derjenige, dem ein ausschließliches Recht am Programmcode zusteht, kann u.a. die ungenehmigte Vervielfältigung, Bearbeitung oder Verbreitung der Software untersagen (§ 69c UrhG).

Die auf einem Smart Device aufgespielte Software ist also immaterialgüterrechtlich dem jeweiligen Rechteinhaber zugewiesen, der sie lizenziert. Eine Begrenzung dieser Rechte, die auch im „Internetrecht der Dinge" teils relevant wird, regelt der sog. Erschöpfungsgrundsatz: Untechnisch gesprochen das „Recht auf Weiterverkauf" des jeweiligen Werkträgers.

2.2.2.2 Datenbanken

Fast alle zum „Internet der Dinge" gehörenden Smart Devices sammeln und speichern in irgendeiner Weise Daten. Dies wird regelmäßig in geordneter Form erfolgen, also eine Datenbank erzeugen.

Wenn die Sammlung und Anordnung von Daten die Schutzvoraussetzungen der §§ 87a ff. UrhG erfüllt,[20] ergibt sich daraus ein Schutzrecht des Datenbankherstellers. Dieses schützt als Leistungsschutzrecht die Datenbank, also die systematisch angelegte Sammlung von Daten. Es schützt jedoch nicht die in der Datenbank enthaltenen Einzel- bzw. „Rohdaten".

Das Leistungsschutzrecht verleiht gem. § 87b UrhG dem Datenbankhersteller (dies ist derjenige, der die wirtschaftliche Aufwendung getätigt hat) ein ausschließliches Recht auf u.a. Vervielfältigung und öffentliche Zugänglichmachung der Datenbank. Damit einher gehen die Abwehrrechte nach § 97 UrhG. Der Datenbankhersteller kann seine Rechte also ebenfalls durch Unterlassungs-, Beseitigungs- und Schadensersatzansprüche verteidigen. Die Abwehransprüche greifen aber nur, wenn auch die Datenbank selbst (d.h. die *Ordnung* der Inhalte) in wesentlichen Teilen übernommen wird.

2.2.2.3 Sonstige immaterialgüterrechtlich geschützte Inhalte

Neben Software und Datenbanken können auf Smart Devices auch andere immaterialgüterrechtlich geschützte Inhalte abgelegt sein. Hier kommt im Prinzip die gesamte Palette des Immaterialgüterrechts in Frage; häufig dürften z.B. Lichtbilder oder Tonaufnahmen abgespeichert sein. Das kommt nicht nur in der Konsumentenelektronik vor: So kommt durchaus in Frage, dass auch die von den Kameras eines Smart Car angefertigten und ggf. gespeicherten Foto- bzw. Videobilder den leistungsschutzrechtlichen Lichtbildschutz beanspruchen können (§ 72 UrhG).

[20] *Zieger/Smirra*, MMR 2013, 418 (420). Die teils in diesem Zusammenhang zitierte Entscheidung des OLG Nürnberg (CR 2013, 212) übersieht, dass die §§ 87a ff. UrhG ein Leistungsschutzrecht darstellen, das gerade keine Schöpfungshöhe voraussetzt.

Je nach Fallkonstellation können auch die Inhaber der betreffenden Schutzrechte Abwehransprüche geltend machen – auch in Bezug darauf, was ein Smart Device mit „ihren“ Inhalten tut, d.h. welchen Funktionsumfang es hat.

2.2.3 Know How-Schutz

Jenseits des klassischen Immaterialgüterrechts hat sich ein Kanon an Schutzmechanismen herausgebildet, der – vom Gesetzgeber gewollt – lückenhaft ausgestaltet ist. Diese werden meist unter dem Begriff „Know-How-Schutz“ zusammengefasst. Es handelt sich im Prinzip um *faktische* Verhaltensweisen, die ein Unternehmen einsetzen kann, um „eigene“ Informationen vor dem Zugriff Dritter zu schützen. Gelingt die Geheimhaltung, knüpft die Rechtsordnung hieran ihrerseits einen gewissen Schutz an, indem sie den Verrat und die rechtswidrige Verwendung von Unternehmensgeheimnissen unter Strafe stellt (§§ 17 und 18 UWG, § 203 f. StGB).

Vorbedingung des Know How-Schutzes ist insbesondere die Geheimhaltung der betroffenen Informationen. Dies erfordert – neben faktischen Geheimhaltungsmechanismen – auch deren vertraglichen Schutz durch den Abschluss von Geheimhaltungsvereinbarungen.

2.2.4 Datenstrafrecht und „Dateneigentum“

Abschließend zu diesem Themenkomplex die Diskussion zum sog. „Dateneigentum”, auch wenn wir uns dieser Lehre nicht anschließen.

Die Lehre vom Dateneigentum knüpft primär an strafrechtliche Normen an, die einen unbefugten Zugriff auf Daten unter Strafe stellen. So wird insbesondere bestraft, wer sich „unbefugt“ zu Daten „Zugang verschaft“, wenn diese „nicht für ihn bestimmt“ sind und der Zugriff unter Überwindung einer Zugangssicherung erfolgt (§ 202a StGB). Ähnliches gilt auch für das Abfangen von Daten (§ 202b StGB) und deren Einkauf, durch den neuen Tatbestand der „Datenhehlerei“ (§

202d StGB).[21] Eine ähnliche Stoßrichtung hat § 303a StGB, der es unter Strafe stellt, wenn jemand „unbefugt“ Daten löscht, unterdrückt, unbrauchbar macht oder verändert.

Die Vorschriften sind größtenteils erst vor wenigen Jahren eingeführt worden, um echte oder vermeintliche Schutzlücken im Strafrecht zu schließen. In diesem Bemühen hat der Gesetzgeber aber die strafwürdigen Tatbestände so schlecht konturiert, dass dies die Strafrechtslehre nun vor Herausforderungen stellt. Insbesondere betrifft dies die vorgenannten Tatbestandsmerkmale („fremde” Daten, „unbefugter“ Zugriff auf bzw. Umgang mit Daten; die „Bestimmtheit“ von Daten für eine bestimmte Personengruppe).

Das Strafrecht definiert nicht selbst, wann ein Datum „fremd” ist, bzw. wann ein Zugriff auf die Daten „unbefugt“ erfolgt. Normalerweise wäre dies ein typischer Fall für die Akzessorietät des Strafrechts: Die Lücke wird geschlossen durch einen Rückgriff auf die allgemeinen Wertungen des Zivilrechts. Genau nach dieser Methode wird beispielsweise das Merkmal „fremd“ im Tatbestand des Diebstahls (§ 242 StGB) definiert: Eine „fremde” Sache nimmt weg, wer – festgestellt nach den Methoden des Zivilrechts – kein Eigentümer dieser Sache ist.

Eine vergleichbare Definition bezüglich eines unbefugten Umgangs mit *Daten* gibt es aber im Zivilrecht nicht. Nicht ohne Grund: Unsere Rechtsordnung hat das System der Ausschließlichkeitsrechte an Informationen ganz gezielt lückenhaft ausgestaltet.[22] Ausschließlichkeitsrechte an Informationen gibt es nur,

[21] Zur berechtigten Kritik an der „Datenhehlerei“ *Selz*, Tagungsband DSRI-Herbstakademie 2015, 915; *Golla/von zur Mühlen*, Telemedicus v. 20.05.2015, http://tlmd.in/a/2951; *dies*. JZ 2014, 668.

[22] Zum Datenschutzrecht *Hornung/Goeble* CR 2015, 265, 268 f.; abwägend der BGH mit Überlegungen zum ergänzenden wettbewerblichen Leistungsschutz, vgl. BGH v. 28.10.2010 – I ZR 60/09, Rn. 28 – *Hartplatzhelden*.

wenn bestimmte Bedingungen erfüllt sind.[23] Der Rest der Informationen soll frei und für jedermann nutzbar sein, er gehört zur Wissensallmende.

Die Zivilrechtsordnung enthält deshalb kein „Dateneigentum“ in einem allumfassenden Sinn. Die Strafrechtslehre hat dies zum Anlass genommen, sich von zivilrechtlichen Wertungen zu lösen und eine eigene Theorie zur rechtlichen Zuordnung von Daten zu entwickeln.[24] Die wohl h.M. sieht eine (strafrechtliche) Verfügungsbefugnis an Daten nun durch den sog. „Skripturakt“ begründet, d.h. den Vorgang des *Abspeicherns* der Daten. Verfügungsbefugt soll derjenige sein, der diesen Skripturakt durchführt, bzw. in dessen Auftrag er durchgeführt wurde. Dieser Theorie hat sich nun wiederum *Hoeren* angeschlossen, der auch im Zivilrecht ein „Dateneigentum“ erkennen will.[25]

Die zivilrechtliche „Dateneigentums“-Theorie ist abzulehnen.[26] Gleiches gilt für eine Auslegung strafrechtlicher Normen, die zivilrechtliche Schutzpositionen unterstellt, die von der Zivilrechtsordnung ganz absichtlich nicht zuerkannt werden.

Zum einen ist diese Theorie schon gar nicht für den Einzelfall operationalisierbar: Wenn diese Theorie den „Dateneigentümer“ über den sog. „Skripturakt” bestimmen will, muss sie bestimmen, *wer konkret* diesen Skripturakt durchgeführt hat. Aber wer soll denn der Skriptor sein, wenn ein Smart Device eben nicht nur in der Kontrolle einer einzelnen Person steht, sondern gleich mehrerer? Ein Smartphone, das beim Herumtragen WLAN-Daten mitschreibt, steht im sachenrechtlichen *Eigentum* der einen Person, vielleicht im *Besitz* einer anderen Person, und die *Software* darauf, die die Daten schreibt, „gehört” schon einem Dritten. Das Smartphone nutzt außerdem bereits vor-

---

[23] *Dorner* CR 2014, 617, 621 ff.
[24] OLG Nürnberg, Beschl. v. 23.01.2013 – 1 Ws 445/12, CR 2013, 212 m.w.N.
[25] *Hoeren* MMR 2013, 486, 486 f.
[26] Zutreffend kritisch *Zech* CR 2015, 137; *Dorner* CR 2014, 617; *Kraus*, Tagungsband DSRI-Herbstakademie 2015, 537, 544.

handene *Datenbanken*, um die neuen Daten einzutragen, und diese Daten sind u.U. *personenbezogene Daten*, betreffend eine oder mehrere Personen. Wer ist unter diesen Umständen der „Skriptor", der „Dateneigentümer"? Das Beispiel zeigt: Die Verwirrung wird durch das Anknüpfen an den Skripturakt nicht geringer. Im Gegenteil: Die Theorie vom Dateneigentum tritt *neben* das Urheberrecht, das Datenschutzrecht und das allgemeine Sachenrecht. Sie ergänzt lediglich einen *weiteren* Ansatz zur Zuweisung von Verfügungsrechten an Daten – und macht die komplizierte Rechtslage somit nur noch unübersichtlicher.

Zuletzt spricht gegen die Theorie vom „Dateneigentum" auch ein eher rechtsphilosophisches bzw. politisches Argument. Soll wirklich ausgerechnet über *Straftatbestände*, auf die Freiheitsstrafe von bis zu drei Jahren steht, ein neues Recht der Eigentumsordnung „erfunden" werden?[27] Es ist auch aus politischer Sicht bedenklich, die Fortbildung der Informationsrechtsordnung ausgerechnet im Strafrecht zu betreiben.

Die *Hoeren`sche*-Theorie vom „Dateneigentum" ist somit abzulehnen. Gleiches gilt auch für eine Auslegung von strafrechtlichen Tatbeständen, die im Ergebnis zu einer Aus- und Überdehnung des gezielt lückenhaft ausgestalteten zivilrechtlichen Informationsschutzes führen.

Stellt dies, wie es gelegentlich behauptet wird, Unternehmen die Daten als Wirtschaftsgut behandeln wollen, vor unlösbare Probleme? Wir denken nicht. Wer Daten als Wirtschaftsgut handeln will, der kann das mit den richtigen Methoden trotzdem tun – dazu braucht es kein „Dateneigentum", sondern dafür reichen die oben genannten Immaterialgüterrechte oder (wo Lücken gefüllt werden müssen) der Know How-Schutz. In der Praxis lassen sich Daten auf

[27] Zutreffend kritisch zur aktuellen Tendenz der Politik, das Strafrecht auf rechtlich schwer greifbare und vor allem nicht durchweg strafwürdige Verhaltensweisen auszudehnen, das Motto des 67. Anwaltstags im Juni 2016: „Wenn das Strafrecht alles richten soll – Ultima Ratio oder Aktionismus?"

diese Weise durchaus verkehrsfähig machen und in Datenkauf- oder Datenlizenzverträgen rechtlich erfassen.[28]

2.3 Die vertragliche Komponente

Neben dem Gesetzesrecht ist zu beachten, dass Gegenstände, die zum „Internet der Dinge" gehören, häufig auch Gegenstand von inhaltlich vielfältigen vertraglichen Absprachen sind. Denn anders als bei einfachen Gegenständen enden vertragliche Beziehungen betreffend Smart Devices meist nicht mit Übergabe und Übereignung des betreffenden Gegenstandes. Ab diesem Zeitpunkt beginnt vielmehr häufig erst ein Dauerschuldverhältnis über eine mit diesem Device erbrachte Dienstleistung.[29]

In der Praxis finden sich rund um „Smart Devices" eine Vielzahl unterschiedlicher Verträge, die auf die Besonderheiten des „Internetrechts der Dinge" nur teilweise ausgerichtet sind. Zu nennen wären insbesondere:

- **Kaufvertrag** mit anschließender Übereignung; im b2b-Bereich häufig auch komplexere Vertragsgestaltung wie z.B. Mietkauf-Verträge oder bedingte Übereignungen (Eigentumsvorbehalt). Aus derartigen Verträgen ergeben sich bezüglich des Funktionsumfangs u.U. auch nachlaufende Sorgfaltspflichten, z.B. aufgrund des Gewährleistungsrechts.
- Ein oder mehrere **Dienstverträge** über die mit diesem Device erbrachten Dienstleistungen. Denkbar wären z.B. ein Vertrag über Softwarepflege (Updates, Bugfixes) oder konkrete Services (z.B. die Ermöglichung einer Cloud-Speichermöglichkeit).

---

[28] Vgl. nur die einschlägigen Beiträge im Tagungsband der DSRI Herbstakademie 2015: *Kraus*, 537; *Schefzig*, 551; *Krätzschmar*, 753.

[29] *Chirro*, Tagungsband DSRI-Herbstakademie 2015, 519 (522); *Solmecke/Vondrlik,* MMR 2013, 755 (756).

- **Software-(endnutzer-) Lizenz**, d.h. die Einräumung des Rechtes, die auf dem Device aufgespielte Software in größerem Umfang zu nutzen, als dies nach den §§ 69a ff. UrhG zulässig ist.
- Auch auf Seiten der Nutzer sind dauerhafte Verpflichtungen häufig. So können Nutzer ihr **Device auch „vermieten"**[30], indem sie anderen das Recht einräumen, aus dem Device Daten zu entnehmen oder es anderweitig für eigene Zwecke zu verwenden.
- Häufig, aber keineswegs immer, ist Teil des Schuldverhältnisses auch eine **Einwilligung** des Nutzers in die Erhebung und Nutzung seiner **personenbezogenen Daten** und/oder ein Vertrag zur **Auftragsdatenverarbeitung**.

Derartige Verträge müssen nicht immer bilateral bestehen. So ist z.B. denkbar, dass ein Eigentümer bzw. Nutzer eines Device mit einer Vielzahl von anderen Rechtsträgern über dieses Device vertragliche Absprachen trifft:

- Mit dem **Verkäufer** des Device,
- mit dem **Anbieter der Betriebssoftware**,
- mit dem **Anbieter** einer mit dem Device verknüpften **Dienstleistung**,
- mit einem **Unternehmen**, das über das Device **Daten erhebt**.

Diese Zahl kann noch beliebig höher sein, denn auf einem Device kann Software von mehreren unterschiedlichen Anbietern installiert sein, bzw. es können darüber mehrere unterschiedliche Dienste erbracht werden.

Bei der Vertragsgestaltung sind viele Besonderheiten zu beachten. Zum einen, dass die Überlassung von Daten *urheberrechtliche* Spezifika beachten muss, wenn nicht nur die Rohdaten, sondern auch die nach den §§ 87a ff. UrhG ge-

[30] Tatsächlich dürfte es sich eher um einen Dienstvertrag handeln, da die physische Herrschaft am Gegenstand nicht im Vordergrund steht, sondern lediglich ein Recht auf Nutzungsziehung (dazu noch unten 4.2.1.4).

schützte Datenbank als solche übernommen wird. Dies betrifft z.B. den Zweckübertragungsgrundsatz (§ 31 Abs. 5 UrhG).[31] Wenn es um *personenbeziehbare Daten* geht (was bei Big Data häufig,[32] aber auch dort nicht zwangsläufig der Fall ist), sind außerdem die Besonderheiten des Datenschutzrechts zu beachten, insbesondere das häufig bestehende Erfordernis einer qualifizierten Einwilligung, die sich aus § 4a BDSG oder §§ 12, 13 TMG ergeben kann.[33] Soweit das TKG Anwendung findet, sind dem Diensteanbieter viele Arten der Datenverwendung von vornherein verboten oder nur eingeschränkt möglich, insbesondere soweit es sich um *Verkehrs- oder Standortdaten* handelt (§§ 95 ff. TKG). Und für standardmäßig eingesetzte Verträge gelten – insbesondere gegenüber Verbrauchern – die Erfordernisse des AGB-Rechts, u.a. das Erfordernis wirksamer Einbeziehung (§ 305 Abs. 2 BGB), das Verständlichkeitsgebot (§ 307 Abs. 1 Satz 2 BGB) und das Verbot überraschender Klauseln (§ 305c BGB). An diesen Kriterien gemessen dürfte wohl ein größerer Teil der im Umlauf befindlichen „Smart Device"-Endnutzerverträge unwirksam sein.[34]

---

[31] Mit ähnlicher Zielrichtung, aber datenschutzrechtlichem Ansatz *Schefzig*, Tagungsband DSRI-Herbstakademie 2015, 551 (561).
[32] *Schefzig,* K&R 2014, 772.
[33] *Hornung/Goeble*, CR 2015, 265 (270 ff.).
[34] Beispielsweise sind auf Englisch abgefasste AGB bei Kunden, bei denen die notwendigen Sprachkenntnisse nicht sicher vorhanden sind, wohl rechtsunwirksam, vgl. *Badesow* in MüKo, BGB, 7. Aufl. 2016, § 305 Rdn. 70; *Grüneberg* in Palandt, BGB, § 305 Rdn. 40; *Reich,* EuZW 1997, 581 (584); mit derselben Einschätzung *Solmecke/Vondrlik,* MMR 2013, 755 (756).

3 Zusätzliche Pflichten mit Bezug zu Konnektivität

Zu den Eigenschaften des „Internet der Dinge“ gehört auch, dass die hierüber verknüpften Gegenstände miteinander und mit der Außenwelt kommunizieren. Konnektivität ist also ein zentrales Merkmal von Smart Devices, wenn sie zum Internet der Dinge gehören.

Die Frage, ob mit dieser Konnektivität eine Regulierung als Telekommunikationsdienst verbunden ist, ist für die rechtliche Bewertung derartiger Sachverhalte zentral: An diese Weichenstellung knüpfen u.a. die Verpflichtung auf das Telekommunikationsgeheimnis (§ 88 TKG, § 206 StGB), Verpflichtungen zur Gewährleistung von Datensicherheit (§ 109 TKG) und Mitwirkungspflichten an der Telekommunikationsüberwachung an (u.a. § 110, § 113 TKG). Wenn weitere Kriterien erfüllt sind (z.B. wenn das Diensteangebot an die Öffentlichkeit oder an Endverbraucher gerichtet ist), kommen weitere, teils sehr umfangreiche telekommunikationsrechtliche Pflichten hinzu.[35]

Ob – und durch wen – im „Internet der Dinge“ ein Telekommunikationsdienst angeboten wird, hängt von der jeweiligen Einzelfallkonstellation ab. Die meisten Pflichten des TKG adressieren den *Anbieter eines Telekommunikationsdienstes*, d.h. denjenigen, der Telekommunikationsdienste erbringt oder an der Erbringung mitwirkt (§ 3 Nr. 6 TKG). Der Begriff „Telekommunikationsdienst“ ist in § 3 Nr. 24 TKG definiert als ein in der Regel gegen Entgelt erbrachter Dienst, der ganz oder überwiegend in der Übertragung von Signalen über Telekommunikationsnetze (§ 3 Nr. 27 TKG) besteht.

[35] Siehe dazu ausführlich *Heun,* CR 2008, 79 (84).

Nimmt man diese Anforderungen zusammen, ergibt sich eine Prüfung in drei Schritten.[36]

3.1 Dienstleistung an Dritte?

Zunächst ist zu fragen, ob die mit dem Device verknüpfte Konnektivität ein Feature darstellt, das als Dienstleistung an Dritte erbracht wird. Dies ist nicht der Fall, wenn das jeweilige Device zwar über das Internet kommunizieren kann, jedoch diese Kommunikationsfähigkeit gar nicht zum Angebot an den Nutzer gehört. Das wäre beispielsweise abzulehnen, wenn ein funkgestütztes Ablese- und Auswertungssystem von Verbrauchs- oder Telemetriedaten dem Anbieter dazu dient, seine Leistungspflicht etwa in Form der Erhebung und Auswertung der Daten in Berichtsform gegenüber dem Kunden (z.B. Vermieter, Fahrzeug- oder Maschinenbetreiber) zu erfüllen. Hier werden zwar auch Daten mittels Signalübertragung übertragen; allerdings ist die Übertragung ein reines Hilfsmittel, das der Anbieter für sich selbst einsetzt. Nicht dem Kunden wird Kommunikation in Form der Übertragung seiner Inhaltsdaten von A nach B angeboten, sondern der Anbieter erhebt die betreffenden Daten durch ein von ihm eingesetztes automatisches Übermittlungssystem.

Der Betreiber des Smart Device erbringt in einem solchen Fall keinen Dienst der „Signalübertragung" an Dritte. Dies wäre vielmehr nur dann der Fall, wenn der Endnutzer bzw. das Device mit Personen oder Geräten kommuniziert, die außerhalb der Sphäre des Diensteanbieters liegen.[37]

---

[36] Für eine ausführlichere Herleitung siehe ausführlich *Heun,* CR 2008, 79 (84); *Heun* in Auernhammer, BDSG, 4. Aufl. 2014, vor zu § 88 TKG Rn. 12 ff.; *Bernhard*, Tagungsband der DSRI Herbstakademie 2015, 985.

[37] Ähnlich *Bernhard*, Tagungsband der DSRI Herbstakademie 2015, 985 (991 f.).

3.2 Konnektivität als Einzeldienst abgrenzbar?

Ist das erste Kriterium erfüllt, kommt es darauf an, ob die mit dem Device verknüpfte Konnektivität einen abgrenzbaren Telekommunikationsdienst ausmacht. Für die Einordnung von gemischten Leistungen kommt es demnach darauf an, ob die einzelnen Leistungsteile separat betrachtet werden können. Ist dies der Fall, können die einzelnen Teile danach untersucht werden, ob sie ein Telekommunikationsdienst sind oder nicht.

Zum Internet der Dinge gehörende Gegenstände sind häufig in ein ganzes Dienstleistungspaket eingebunden, zu denen typischerweise auch Cloud- und Kommunikationsfunktionen gehören. Diese bauen notwendigerweise auf IP- oder Internet-Konnektivität auf.

Wenn der Konnektivitätsteil denklogisch getrennt oder durch einen Dritten angeboten werden könnte, handelt es sich bei diesem abtrennbaren Teil um einen Telekommunikationsdienst.[38] Dieser unterfällt dann der sektorspezifischen Regulierung nach dem TKG, während der übrige Teil des Serviceangebotes als einfache Dienstleistung oder als Telemediendienst einzustufen wäre.

3.3 Betrachtung nach dem Schwerpunkt

Lässt sich der Konnektivitätsteil des Angebots nicht abgrenzen, kommt es darauf an, ob die über das Smart Device angebotene Kommunikationsmöglichkeit den *Schwerpunkt* des Dienstes ausmacht. Dies ergibt sich aus der in § 3 Nr. 27 TKG enthaltenen Formulierung „ganz oder überwiegend". Ein Telekommunikationsdienst bleibt auch dann ein Telekommunikationsdienst, wenn er nur einen Teil eines ansonsten umfangreicheren, aber nicht aus Telekommunikati-

[38] *Bernhard*, Tagungsband der DSRI Herbstakademie 2015, 985 (987 f.).

onsdiensten bestehenden Leistungsbündels darstellt. Diese, auf die Einzelkomponenten bezogene Sichtweise legt auch Erwägungsgrund 10 der Rahmenrichtlinie zugrunde, wo ausdrücklich aufgeführt ist, dass derselbe Internet-Diensteanbieter „sowohl elektronische Kommunikationsdienste, wie den Zugang zum Internet, als auch nicht unter diese Richtlinie fallende Dienste, wie die Bereitstellung von Internet gestützten Inhalten, anbieten“ kann.

3.4 Wer ist Diensteanbieter?

Liegt ein Telekommunikationsdienst vor, kommt es auf die Frage an, wer Diensteanbieter ist. Dies ist keineswegs immer derjenige, der über das jeweilige Smart Device auch die anderweitigen Dienstleistungen erbringt. Es kommt darauf an, wer „technisch-operativ für die Leistungserbringung gegenüber dem Kunden verantwortlich ist.“[39]

Hierbei ist zu beachten, dass die Rolle der Anbieter in der Praxis verschieden sein kann und auch Grauzonen existieren.[40] So vermarkten beispielsweise Anbieter von Smart Cars diese gebündelt mit einer SIM-Karte, die entweder fest im Auto eingebaut ist oder zwar entnommen werden kann, aber für eine gewisse Zeitspanne vom Fahrzeughersteller vorfinanziert ist. Der Endkunde hat diese Dienstleistung beim Fahrzeugkauf also miterworben.[41] Und auch ob die Notruffunktion, die nach der eCall-Verordnung (2015/758/EU) von Fahrzeugherstellern anzubieten ist, diesen zum Telekommunikationsdiensteanbieter macht, ist zu diskutieren.[42]

---

[39] *Bernhard*, Tagungsband der DSRI Herbstakademie 2015, 985 (995).
[40] *Grünwald/Nüßing,* MMR 2015, 378 (380f.).
[41] Zu den unterschiedlichen denkbaren Konstellationen *Langer*, Tagungsband DSRI-Herbstakademie 2015, 973 (974 ff.); *Bernhard*, Tagungsband DSRI-Herbstakademie 2015, 985 (996).
[42] Das Problem wird angerissen bei *Lüdemann,* ZD 2015, 247 (251f.).

Telekommunikationsdiensteanbieter i.S.d. § 3 Nr. 6 TKG ist (mindestens) derjenige, der gegenüber dem Endkunden die rechtliche Verantwortung dafür übernimmt, dass die Informationen übertragen werden. Wenn der Diensteanbieter die Konnektivität, an den Kunden aus eigener Hand anbietet, kommt es deshalb nicht darauf an, ob er diese in Form eines Vorleistungsproduktes bei einem Dritten erworben hat; der Diensteanbieter ist dann Reseller einer Telekommunikationsdienstleistung.

Nur wenn es *ausschließlich* am Endnutzer liegt, die Kommunikationsfähigkeit des Device herzustellen, z.B. durch die Verbindung mit einem WLAN oder das Einschieben einer (eigenen) SIM-Karte, ist grundsätzlich derjenige, der über das Device Dienstleistungen anbietet, nicht gleichzeitig Telekommunikationsdiensteanbieter. Wenn allerdings (quasi *aufsattelnd* auf der IP-Anbindung des Kunden) ein logisch eigenständiger Kommunikationsdienst angeboten wird (z.B. Zustellung von E-Mail oder VoIP-Telefonie) kann es sich allerdings schon wieder um einen Telekommunikationsdienst handeln. Denn auch sog. OTT-Angebote sind – nach allerdings strittiger Ansicht – telekommunikationsrechtlich als TK-Diensteanbieter zu behandeln, wenn sie (trotz der Tatsache, dass sie auf die seitens des Kunden bereitgestellte Konnektivität zurückgreifen) funktional betrachtet eine eigenständige Funktion der Signalübermittlung übernehmen.[43] Dies ist z.B. der Fall, wenn der OTT-Anbieter die Kommunikationsdaten der Kunden über eigene zentrale Server weitervermittelt.[44]

---

[43] Vgl. *Kühling/Schall*, CR 2015, 641; VG Köln v. 11.11.2015 – 21 K 450/15; Wissenschaftlicher Arbeitskreis für Regulierungsfragen (WAR) bei der Bundesnetzagentur, Evolution der Regulierung in den Telekommunikations- und Mediensektoren angesichts der Relevanzzunahme von OTT-Anbietern vom 18. November 2015; abrufbar unter http://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Allgemeines/Bundesnetzagentur/WAR/WAR_OTT.pdf?__blob=publicationFile&v=1.

[44] *Kühling/Schall*, CR 2015, 641 (650 ff.).

Zusammengefasst lässt sich festhalten, dass Dienste, die im „Internet der Dinge“ erbracht werden, häufig, jedoch nicht zwangsläufig einen Telekommunikationsdienst darstellen.

4 Praxisfälle und Lösungsansätze

Die Grundfrage im Zusammenhang mit dem Aufkommen des „Internet der Dinge“ ist, in welchem Verhältnis zueinander die Rechte an den Daten und die Rechte an den Gegenständen stehen. Wenn die *Daten* der einen Person (oder sogar mehreren Personen) und der *Gegenstand* der anderen Person „gehören“, wessen Recht setzt sich durch?

Die Frage stellt sich in Form vieler Einzelfragen. Auch die Lösung ergibt sich nur auf Basis einer Betrachtung im Einzelfall. Einfache Lösungsansätze beispielsweise in die Richtung, dass beispielsweise ein „Recht am Datum“ immer das Recht am Gegenstand nach sich ziehe, oder umgekehrt, sind zurückzuweisen. Wir erörtern im Folgenden beispielhaft einige Fallkonstellationen.

4.1 Fallbeispiele

Fallkonstellation 1:

Hersteller G hat in sein Device eine Funktion integriert, bei der die betreffenden Geräte gleichzeitig GPS-Standortdaten und die jeweilige Urzeit erheben und live über das Internet übermitteln. Aus den gewonnenen Daten kann der Hersteller Straßenverkehrsdaten isolieren, z.B. wo gerade Stau ist und welche Routen schneller zum Ziel führen. Radiosender und Navigationsdiensteanbieter sind interessiert an diesen Daten.

1. Darf G diese Daten aus den Geräten ohne Zustimmung der Nutzer auslesen?

2. Darf er die aggregierten Daten an Dritte lizenzieren, ohne die eigentlichen "Hersteller" der Standort- und Bewegungsdaten an den Gewinnen zu beteiligen?

Fallkonstellation 2:

Hersteller G spielt auf sein Device "Over the Air" eine neue Softwareversion auf. Danach hat das Gerät einen gänzlich anderen Funktionsumfang. Eine (dem deutschen AGB-Recht entsprechende) Einwilligung der Eigentümer der Geräte liegt nicht vor. Einige Nutzer betrachten die neuen Funktionen als mangelhaft.

1. Haben die Nutzer ein Recht auf Beseitigung und Unterlassung solcher Updates?

2. Haben die Nutzer jetzt Mängelansprüche gegen G bzw. den jeweiligen Verkäufer?

3. Variante: Der Nutzer "rootet" das Device und spielt eigenmächtig andere Software auf. Ist dies zulässig?

4.2 Grundansätze für die Bearbeitung von Fällen im „Internetrecht der Dinge“

Die vorgenannten Fallfragen hier vollständig zu begutachten, würde den Rahmen dieser Erörterung sprengen. In den folgenden Absätzen sind einige Gedanken zu Lösungsansätzen festgehalten, die gleichermaßen für die Lösung der hiesigen Beispielsfälle wie auch für alle anderen Rechtsfragen im Zusammenhang mit dem „Internet der Dinge“ relevant sind.

4.2.1 Verhältnis von Sachenrecht und Informationsrecht

Informationsrechtliche und sachenrechtliche Rechtspositionen fallen nicht zwangläufig zusammen. Ein Recht am *Datenträger* ist nicht zwangsläufig identisch mit dem Recht an den darauf gespeicherten *Daten*. Hinzuweisen ist vor diesem Hintergrund insbesondere auf die jüngst veröffentlichte Entscheidung

des BGH i.S. *Kohl-Tagebücher*,[45] laut der die rechtliche Berechtigung an Daten nicht zwangsläufig mit der rechtlichen Berechtigung am Datenträger gleichzusetzen ist.[46] Es kann in der Diktion des BGH durchaus sein, dass das sachenrechtliche Eigentum am Datenträger bei der einen Person liegt, die Verfügungsbefugnis an den Daten aber bei einer anderen.[47]

Sachen- und informationsrechtliche Ansprüche beeinflussen sich aber gegenseitig. So kann es durchaus vorkommen, dass sich aus dem informationsrechtlichen Rechten auch Rechte am physischen Gegenstand ableiten. Aber auch umgekehrt können sich aus dem sachenrechtlichen Herrschaftsrecht (Eigentum, Besitzschutz, etc.) Rechte an Daten ergeben, die auf dem betreffenden Gegenstand gespeichert sind oder von diesem erzeugt werden.

4.2.1.1 Einwirkung von informationsrechtlichen Rechtspositionen auf das Sachenrecht

Je nachdem, wie eng Daten und Datenträger verknüpft sind, kann eine (an den Daten bestehende) informationsrechtliche Rechtsposition die (am Datenträger bestehende) sachenrechtliche Rechtsposition verdrängen. So hat der BGH in seiner Entscheidung i.S. *Kohl-Tagebücher* ausdrücklich betont, dass ein Herausgabeanspruch aus § 667 BGB, der sich im konkreten Fall eigentlich nur auf *Daten* bezog (in diesem Fall auf analog gespeicherte Audioaufzeichnungen), auch die Herausgabe des Daten*trägers* erfasst.[48] Ein „starkes" Recht an den gespeicherten Daten kann also durchaus auch die sachenrechtliche Eigentumsstellung einschränken oder sogar aufheben.

---

[45] BGH, Urt. v. 10.07.2015 – V ZR 206/14, Rn. 11ff. – *Kohl-Tagebücher.*
[46] *Assion*, Telemedicus v. 10.11.2015, http://tlmd.in/a/3012; zur Problematik auch *Dorner* CR 2014, 617, 618.
[47] So auch bereits BGH NJW 2007, 2394 m.w.N.
[48] Begründet in BGH, Urt. v. 10.07.2015 – V ZR 206/14, Rn. 36 – *Kohl-Tagebücher.*

In derselben Entscheidung hat der BGH auch festgestellt, dass das Aufspielen von Daten auf einen Datenträger als Verarbeitung (§ 950 BGB) zu einem Eigentumsübergang am Datenträger führen *kann*, wenn die Wesensnatur der Sache sich hierdurch grundlegend ändert.[49] Dies sei aber nicht der Fall, wenn der Datenträger seine eigentliche Funktion durch das Aufspielen von Daten nicht verliere.[50]

Auch soweit sich das Recht der Rechteinhaber an Informationen *nicht* unmittelbar auf das Sachenrecht überträgt, bleiben die immaterialgüter- und datenschutzrechtlichen Rechtspositionen bestehen. Denn ein informationsrechtlicher Rechtsanspruch besteht im Grundsatz auch dann weiter, wenn er mit einer sachenrechtlichen Rechtsposition konkurriert. Diejenigen, denen ein „Recht an den Daten" zugewiesen ist, stehen also Verfügungs- und Abwehrrechte zu – auch wenn „ihre" Daten auf dem Device eines anderen gespeichert sind. Sie können auf Basis dieser Rechtspositionen den Endnutzern (und Eigentümern) der Devices bestimmte Einwirkungen auf diese untersagen. Hier hängt vieles vom konkreten Fall und den jeweils einschlägigen Bestimmungen ab (vgl. nur §§ 69d, 69e UrhG, § 87c UrhG, § 108b UrhG, § 303a StGB).[51]

4.2.1.2 Einwirkung von sachenrechtlichen Rechtspositionen auf das Informationsrecht

Auch umgekehrt sind Fälle denkbar, in denen ein Recht am *Gegenstand* ein Recht am *Datum* nach sich zieht – das prominenteste Beispiel hierfür dürfte der im UrhG geregelte Erschöpfungsgrundsatz sein (§ 17 Abs. 2 UrhG): Der Eigentümer eines Datenträgers darf im Rahmen seiner Eigentümerbefugnisse diesen weiterveräußern, selbst wenn er dabei im urheberrechtlichen Sinn eine unli-

[49] BGH, Urt. v. 10.07.2015 – V ZR 206/14, Rn. 19 – *Kohl-Tagebücher.*
[50] BGH, Urt. v. 10.07.2015 – V ZR 206/14, Rn. 19 – *Kohl-Tagebücher.*
[51] Exemplarisch die Auseinandersetzung von *Kusnik* CR 2011, 718 mit dem Recht auf „Hacken" des eigenen Mobiltelefons. Das Ergebnis der Betrachtung dürfte allerdings anders ausfallen, wenn es um das Hacken des eigenen Autos und insbesondere von dessen sicherheitsrelevanten Funktionen geht.

zenzierte Verwertungshandlung vornimmt. Dies gilt im Grundsatz auch für die Weiterveräußerung von (datentragenden) Gegenständen des Internets der Dinge. Hier gibt es aber viele Details zu beachten, u.a. Spezialvorschriften und detaillierte Rechtsprechung für den Weiterverkauf von Gebrauchtsoftware.[52] Außerdem sollte beachtet werden, dass eine Transaktion über einen vernetzten Gegenstand und darauf aufgespielte Daten meist eine weitere rechtliche Ebene berührt: Denn häufig ist dieser Gegenstand mit einer *Dienstleistung* verknüpft, die ihrerseits vertraglich geregelt ist.[53]

Hinzu kommen klassische sachenrechtliche Rechtsansprüche, die auch Informationen betreffen können, die auf den zum „Internet der Dinge" gehörenden Devices gespeichert sind. Die Eigentümer und Besitzer der Devices können sich gegenüber informationellen Einwirkungen auf „ihre" Devices (z.B. Einspielen oder Entnahme von Daten) durch den Diensteanbieter regelmäßig auf ihre sachenrechtlichen Abwehrrechte berufen. Einwirkungen von außen auf ein Smart Device, die dessen bestimmungsgemäße Nutzbarkeit beeinflussen, dürften im Regelfall als „Störung" des Eigentums bzw. Besitzes i.S.d. § 1004 bzw. § 862 BGB zu qualifizieren sein.[54] Gleiches dürfte auch für das ungenehmigte Entnehmen von Daten gelten, jedenfalls dann, wenn der Eigentümer des Device ein berechtigtes Interesse an dessen informationstechnischer Integrität hat.

Es kommt dann darauf an, ob der Anspruch durch eine Duldungspflicht ausgeschlossen ist. Eine solche Duldungspflicht kann sich z.B. aus vertraglichen

---

[52] Vgl. nur EuGH, Urt. v. 3.7.2012 – C-128/11, CR 2012, 498 – *Usedsoft*; EuGH, Urt. 23.1.2014 – C-355/12, CR 2014, 224 – *Nintendo*; zusammenfassend *Apel,* ZUM 2015, 640.

[53] BGH, Urt. 11.2.2010 – I ZR 178/08, CR 2010, 565 – *Half Life 2*; zuletzt KG, Hinweisbeschluss v. 10.08.2015, Az. 23 U 42/14, http://tlmd.in/u/1638.

[54] So auch *Zech,* CR 2015, 137 (139, 142); OLG Karlsruhe, Urt. v. 7.11.1995 – 3 U 15/95, NJW 1996, 200 (201); OLG Oldenburg, Beschl. v. 24.11.2011 – 2 U 98/11, CR 2012, 77 (77).

Abreden, aber auch aus dem Gesetz ergeben.[55] So kann ein Anbieter z.B. gesetzlich *verpflichtet* sein, Softwareupdates einzuspielen, wenn dies der Gewährleistung von IT-Sicherheit dient (vgl. nur § 9 BDSG, § 13 Abs. 7 TMG, § 109 TKG).[56] Aus dieser Verpflichtung wäre wohl auch ein korrespondierender Duldungsanspruch des Nutzers herzuleiten.

Und auch *nach* der Entnahme von Daten aus einem Device weist die Rechtsordnung das Nutzungsrecht an diesen Daten im Grundsatz dem Eigentümer zu. Denn Daten, die von einem „Smart Device" erzeugt werden, sind *Nutzungen* dieser Sache i.S.d. § 100 BGB.[57] Nutzungen einer Sache sind, soweit keine spezielleren gesetzlichen oder vertraglichen Regelungen greifen,[58] vermögensrechtlich deren Eigentümer zugewiesen.[59] Die Nutzung von Daten, die von einem „Smart Device" erzeugt werden, steht somit im Zweifel dessen Eigentümer zu; er kann unberechtigte Datenentnahmen oder –änderungen als Eigentumsverletzung untersagen (§ 1004 BGB)[60] und unberechtigt entnommene Daten bzw. deren Wert als ungerechtfertigte Bereicherung herausverlangen (§ 818 Abs. 1 BGB).[61]

Die vermögensrechtliche Zuweisung von Daten ist indes nicht mit einem als Ausschließlichkeitsrecht geschützten „Dateneigentum" zu verwechseln.[62] Wer Daten, bzw. die in ihnen verkörperten Werte auch *nach* dem Wegfall ihrer unmittelbaren „Sachbindung" ausschließlich nutzen will, muss sich zum Schutz dieser Exklusivität der Instrumente des Know How-Schutzes bedienen.

---

[55] *Neuner,* JuS 2005, 487 (490 f.); *Rachlitz/Ringshandl,* JuS 2011, 970; *Lettl,* JuS 2005, 871.
[56] *Bräutigam/Klindt,* NJW 2015, 1137 (1141).
[57] *Heun/Assion,* CR 2015, 812, 818; vgl. auch *Zech*, CR 2015, 137, 142.
[58] Z.B. § 1030 Abs. 1 BGB (Nießbrauch).
[59] *Stresemann*, in: MüKo BGB, 7. Aufl. 2015, § 100 Rz. 8; vgl. auch § 903, § 446 Satz 2 und die § 987 ff. BGB.
[60] *Zech,* CR 2015, 137, 142.
[61] *Heun/Assion,* CR 2015, 812, 818.
[62] So auch *Zech,* CR 2015, 137, 142.

4.2.1.3 Konkurrenzen

In Situationen, in denen es zur Konkurrenz von Ansprüchen und Duldungspflichten unterschiedlicher Rechtsgebiete kommt, sind die herkömmlichen Konkurrenzregeln anzuwenden. Vielfach wird dabei *kreative Normauslegung* notwendig werden, denn das Aufeinandertreffen von z.B. IT-Sicherheitspflichten und § 1004 Abs. 2 BGB war vom Gesetzgeber sicherlich nicht vorgesehen.

Vielfach wird eine Lösung des Konkurrenzproblems eine Einzelfallbetrachtung erfordern, bei der letztlich anhand des *Sinns und Zwecks* der einschlägigen Normen zu ermitteln ist, in welchem Konkurrenzverhältnis diese zueinander stehen sollen. Dabei sind dann auch die Wertungen des höherrangigen Rechts zu beachten. Soweit es um die Frage geht, wie weit ein Dritter (z.B. der Gerätehersteller) auch nach Übereignung noch auf das Device einwirkt, ist dies insbesondere das sog. IT-Grundrecht. Das BVerfG hat demjenigen, der ein informationstechnisches System für Zwecke der Persönlichkeitsentfaltung verwendet, ein „grundrechtlich erhebliches Schutzbedürfnis" attestiert.[63] Dieser Gedanke kann (über die Ausstrahlungswirkung von Grundrechten auf das Privatrecht) auch für die Auflösung von Normenkonkurrenzen fruchtbar gemacht werden. Dies hilft im B2B-Verhältnis nicht weiter, gibt aber jedenfalls in Situationen, wo private Devices betroffen sind, eine Hilfestellung.

4.2.1.4 Vertragliche Regelungsmöglichkeiten

Gerade das dargestellte Geflecht von *gesetzlichen* im Gegenseitigkeitsverhältnis bestehenden Rechte und Pflichten können die Parteien nutzen, um das Rechtsverhältnis auch *vertraglich* zu gestalten. Eine solche Abrede wird typischerweise darin bestehen, dass die Rechte und Pflichten im Gegenseitigkeitsverhältnis geklärt werden. So kann z.B. geklärt werden, ob eine bestimmte Software gepflegt werden muss oder nicht, bzw. ob das Einspielen von Updates über-

[63] BVerfGE 120, 274 (306) – *Online-Durchsuchung*.

haupt zulässig ist. Auch die Befugnis zur Entnahme von Daten kann (und sollte) geklärt werden. Häufig tritt die Situation auf, dass der Hersteller eines Smart Device ein Interesse daran hat, auch *nachträglich* auf von diesem gespeicherte bzw. erhobene Daten zuzugreifen. Er sollte dies dann vertraglich lösen, indem er dieses Recht in einer Vereinbarung mit dem Eigentümer des Smart Device absichert.[64]

Die Folge eines solchen Vertrags wäre, dass der Eigentümer das Device an den Diensteanbieter (untechnisch gesprochen)[65] quasi teilweise „rückvermietet" und ihm auf diese Weise ermöglicht, dessen Funktionsumfang zu beeinflussen und Daten aufzuspielen und zu entnehmen. Soweit die Daten als „Nutzungen" des Smart Device zu betrachten sind, steht dieses Nutzungsrecht dann von vornherein dem vertraglich Nutzungsberechtigten zu.[66]

[64] Hierzu auch *Assion* CR 2016, 84 ff.
[65] Begrifflich dürfte dieser Vertragsteil wohl eher als Dienstvertrag zu charakterisieren sein, auch wenn gewisse Ähnlichkeiten zur Vermietung bestehen.
[66] OLG Naumburg CR 2016, 83 ff. m. Anm. *Assion*; *Stresemann*, in: MüKo BGB, 7. Aufl. 2015, § 100 Rz. 8.

5 Zusammenfassung und Schlussbemerkung

Das „Internetrecht der Dinge“ vereint mehrere Rechtsgebiete, die bisher wenig miteinander zu tun hatten. Das Aufeinandertreffen von sachenrechtlichen und informations-, bzw. kommunikationsrechtlichen Rechtsbestimmungen wirft vielfältige Fragen auf, die sich in dieser Form noch nie gestellt haben – aber dennoch enorme praktische Relevanz aufweisen.

Für die Rechtswissenschaft und -praxis stellt sich nun die Aufgabe, die verschiedenen Fallkonstellationen zu bearbeiten und Rechtssicherheit zu schaffen. Auch wenn Datenbestände sich rechtlich durchaus als verkehrsfähiger Vermögensgegenstand behandeln lassen, gibt es diesbezüglich noch viele Einzelfragen zu klären. Die „Erfindung“ eines neuartigen „Dateneigentums“ ist hierzu nicht notwendig, aber doch eine (Weiter-) Entwicklung der Praxis der Vertragsgestaltung über Datenkauf-, Datenleih- oder Datenlizenzverträge.

Die Gerichte werden voraussichtlich mittelfristig Sachverhalte zu entscheiden haben, in denen derartige Verträge fehlten bzw. nicht eingehalten wurden und ein Kläger deshalb die Herausgabe der Daten (bzw. der daraus erlangten Vermögensvorteile) verlangt. Hier wird es dann um die Frage gehen, ob Daten Nutzungen oder Früchte einer Sache sind und, falls die gesamte Datenbank als solche übernommen wurde, wer im urheberrechtlichen Sinn „Hersteller“ einer Datenbank ist.[67]

[67] Die Frage wurde hier nicht weiter thematisiert; vgl. zum Herstellerbegriff des § 87f Abs. 2 UrhG statt vieler *Krätzschmar*, Tagungsband DSRI-Herbstakademie 2015, 753 (757); *Arkenau/Wübbelmann*, Tagungsband DSRI-Herbstakademie 2015, 95 (105); *Wiebe* in: Spindler/Schuster, 3. Aufl. 2015, § 87a UrhG Rn. 18ff.

Es handelt sich also keineswegs um eine Aufgabe, die reflexartig nur dem Gesetzgeber zuzuweisen ist. Aktuell besteht eher ein *zu viel* als ein *zu wenig* an einschlägigem Recht. Jede Einzelfrage spezifisch zu regeln, wäre nur begrenzt hilfreich, zumal es hier um Grundfragen geht, die auch grundlegend (und nicht durch spezielle Einzelfallregelungen) geklärt werden sollten. In der eCall-Verordnung (betreffend Smart Cars)[68] und in dem kürzlich vorgelegten Entwurf des „Gesetzes zur Digitalisierung der Energiewende" (betreffend Smart Grids) versucht der Gesetzgeber, sehr feingranular jede (datenschutzrechtliche) Einzelfrage einzeln zu adressieren. Diesen Ansatz auf alle betroffenen Industriebereiche zu übertragen, wäre sicherlich nicht sinnvoll.

[68] Verordnung 2015/758/EU des Europäischen Parlaments und des Rates v. 29.04.2015 über Anforderungen für die Typgenehmigung zur Einführung des auf dem 112-Notruf basierenden bordeigenen eCall-Systems in Fahrzeugen und zur Änderung der Richtlinie 2007/46/EG.

Ist es Zeit für ein eigentumsähnliches immaterielles Recht an personenbezogenen Daten?

Ein Gedankenspiel

Tina Krügel

Der Beitrag befasst sich mit der Diskrepanz zwischen dem Marktwert von personenbezogenen Daten einerseits und andererseits dem Umstand, dass es eine anerkannte vermögensrechtliche Zuordnung personenbezogener Daten (bisher) nicht gibt. Dabei wird, jenseits eingefahrener datenschutzrechtlicher Dogmatik, dem über die Jahrzehnte immer wieder erneuerten Ruf nach einer vermögensrechtlichen Verfügungsbefugnis zugunsten des Betroffenen nachgegangen und hinterfragt, ob eine solche geeignet sein könnte, in Zeiten von intelligenten Haushaltsgeräten, Smartphones und vernetzten Autos den Datenschutz für die Betroffenen zu verbessern.

1 Personenbezogene Daten sind eine Ware

Unsere Daten sind eine Währung. Dass wir bei vermeintlich kostenlosen Internetdiensten mit der Preisgabe unsere personenbezogenen Daten bezahlen, überrascht heute kaum noch jemanden. Eine – jedenfalls aus datenschutzrechtlicher Sicht - bittere Erkenntnis ist es aber, dass es die Mehrheit insbesondere der jüngeren Generation auch gar nicht stört. Das Datenschutzrecht, zu Zeiten des Volkszählungsurteils noch (weitgehend allein) mit dem Staat als einem greifbaren Gegner konfrontiert, der zudem trefflich als Bösewicht taugte, sieht sich im Zeitalter von facebook, Alphabet (der Google Mutterkonzern), twitter und Co. ganz anderen, kaum bedrohlich wirkenden und doch omnipotenten Akteuren gegenüber, die sich bestens darauf verstehen, ihren unstillbaren Datenhunger nicht allzu offensichtlich zur Schau zu stellen.

Dies alles ist nicht neu. Im Gegenteil, es ist seit Jahren Realität: personenbezogene Daten sind ein Wirtschaftsgut und werden als solches weltweit gehandelt. Neu ist auch nicht, dass in diesem Wirtschaftszweig sehr viel Geld steckt. Einen Augenblick des Innehaltens hat es dann aber doch verdient, wenn man sich die Entwicklung des Börsenwertes etwa von facebook anschaut, der sich seit dem Börsenstart im Mai 2012 knapp verdreifachte und im November 2015 erstmals die 300 Milliarden US-Dollar Marke übersprang.[1]

Was aber heißt das für das Datenschutzrecht? Das Datenschutzrecht ist die einfachgesetzliche Ausformung des Grundrechts auf informationelle Selbstbestimmung, das seinerseits Teil des allgemeinen Persönlichkeitsrechts aus Art. 2

[1] http://deutsche-wirtschafts-nachrichten.de/2015/11/06/boersenwert-von-facebook-springt-ueber-300-milliarden-dollar/

Abs. 1 i.V.m. Art. 1 Abs. 1 GG ist[2]. Ursprünglich als Abwehrrecht ausgestaltet, verbietet es jede Art der Erhebung oder Verarbeitung personenbezogener Daten es sei denn, diese erfolgt aufgrund einer Rechtsvorschrift oder aufgrund einer Einwilligung des Betroffenen (§ 4 Abs. 1 BDSG). Unabhängig davon, dass dieses Verbot mit Erlaubnisvorbehalt insbesondere bei den hier behandelten vermeintlich kostenlosen Internetdiensten der Privatwirtschaft praktisch kaum noch einschränkende Wirkung entfaltet. Denn letztlich bleibt auch den datenschutzrechtlich sensibilisierten Nutzern nur eine Alles–oder-Nichts-Entscheidung: Wollen sie die Dienste nutzen, müssen sie in die Datenverarbeitung einwilligen und erlauben damit je nach Ausgestaltung der vorgefertigten Einwilligungserklärung eine umfassende Verarbeitung und Weitergabe ihrer personenbezogenen Daten. Einziger Ausweg dies zu vermeiden, ist es, die Dienste gar nicht zu nutzen mit der unmittelbaren und – in Zeiten, in denen die klassische Telefonkette wegen Unterrichtsausfall durch facebook-Gruppen ersetzt wird – weitreichenden Konsequenz, von dem jeweiligen Kommunikationsweg ausgeschlossen zu sein.

Dies wird sich auch nicht merklich ändern, wenn die nunmehr verabschiedete europäische Datenschutzgrundverordnung[3] am 25. Mai 2018 in Kraft tritt. Zwar ist diese Reform zweifellos eine Zäsur, die das Datenschutzrecht in der europäischen Union nicht nur zu vereinheitlichen sucht, sondern es auch für die Herausforderungen der digitalen Welt wappnen möchte – etwa über die Ausdehnung des Anwendungsbereichs auf Unternehmen außerhalb der europäischen Union, die Produkte oder Dienstleistungen in der EU anbieten und in diesem Rahmen personenbezogene Daten von EU Bürgern verarbeiten[4]. In ihren Grundsätzen hält die Datenschutzgrundverordnung jedoch an den Prinzipen der noch geltenden Datenschutzrichtlinie aus dem Jahre 1995 fest, so dass

[2] BVerfGE 65,1.
[3] http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016R0679&from=DE.
[4] Vgl. Art. 3 Abs. Abs. 2.

viele bekannte Eckpfeiler, etwa die grundsätzliche Unterscheidung zwischen personenbezogenen und nicht personenbezogenen Daten, das Verbot mit Erlaubnisvorbehalt und die Einwilligung als Legitimationsmöglichkeit auch der Datenschutzgrundverordnung immanent sind und dem Nutzer in oben beschriebenem Szenario nicht helfen.[5]

[5] Nicht umsonst fanden sich schon vor ihrer Verabschiedung Stimmen, die sie als veraltet bezeichnen, siehe etwa Forgó, http://www.heise.de/newsticker/meldung/Datenschutz-in-der-EU-Nach-dem-Spiel-ist-vor-dem-Spiel-3045740.html.

2 Gibt es Eigentum an personenbezogenen Daten?

Bemerkenswert ist zudem ein weiterer Aspekt: Trotz des erheblichen wirtschaftlichen Wertes, den personenbezogene Daten offensichtlich aufweisen, ist die Frage, „Wem gehören personenbezogenen Daten?“ weder geklärt noch scheint man ihr große Bedeutung, geschweige denn Lösungspotenzial beizumessen und so findet sich – wenig verwunderlich - auch in der kommenden Datenschutzgrundverordnung hierauf keine Antwort.

Ist man mit dem Datenschutzrecht weniger vertraut, mag man wohl davon ausgehen, dass die eigenen personenbezogenen Daten selbstverständlich dem jeweils Betroffenen „gehören“. Rechtlich verankern lässt sich diese Annahme jedoch keinesfalls. Im Gegenteil: Mit der deutschen Ausgestaltung als Ausfluss des allgemeinen Persönlichkeitsrechts wurde und wird das Grundrecht auf informationelle Selbstbestimmung als unübertragbar angesehen. Begriffe wie „Eigentum“ oder „Verfügungsbefugnis“ sind dem Datenschutzrecht in seiner jetzigen Form fremd. Historisch war dies auch unschädlich. In den frühen 80iger Jahren war der Fokus des noch sehr jungen Datenschutzrechts auf die Übermacht des Staates gerichtet. Dies war ebenso folgerichtig wie zielführend. Vor dem Hintergrund der seit Jahren durch wenige (US-amerikanische) Großunternehmen bestimmten Internetökonomie scheint diese rein persönlichkeitsrechtliche Ausgestaltung aber nicht erst heute zu kurz zu greifen. Personenbezogene Daten weisen im digitalen Zeitalter einen erheblichen wirtschaftlichen Wert auf. Sie werden nicht nur als Gegenleistung für „kostenlose“ Internetservices erhoben, sondern etwa durch Smartphones generiert, beim mobilen Bezahlen oder in immer neuen Geschäftsfeldern, etwa in der Automobilbranche, der von PWC mit dem „vernetzten Auto“ ein enormes Wachstumspotential bescheinigt wird. Die Massen an personenbezogenen Daten die über

„smarte“ Technologie gesammelt und ausgewertet werden, erreichen neue Dimensionen. Auswertung und Verkauf dieser Daten etwa zu Produktoptimierung oder zu Werbezwecken nähren nicht nur einen Wirtschaftzweig. Ein Markt, von dem die Betroffenen, deren Daten ausgewertet und vermarktet werden, (rein rechtlich) ausgeschlossen sind und sich nach deutscher Auffassung mangels vermögensrechtlicher Position an den eigenen Daten auch nicht integrieren lassen.

So sehr diese Unübertragbarkeit grundrechtsdogmatisch einleuchten mag, so irritierend ist gleichzeitig die Erkenntnis, dass eben diese personenbezogenen Daten, einmal durch Einwilligung des Betroffenen in den Verkehr gebracht, plötzlich Marktwert erlangen und (weiter-) veräußert werden. Dies impliziert eine Verfügungsbefugnis über die überlassenen Daten. Aber gibt es eine solche Befugnis über personenbezogene Daten überhaupt und wenn ja, wer kann ein solches Recht beanspruchen? Tatsache ist jedenfalls, dass die (rein faktische) Entwicklung zu einer Verkehrsfähigkeit eines ursprünglich dem Persönlichkeitsrecht entstammenden Gutes allein nicht zu einer Rechtsänderung führt. Eine solche ist vielmehr dem Gesetzgeber, bzw. im Rahmen von unbestimmten Rechtsbegriffen und Werturteilen, den Gerichten vorbehalten, die freilich gehalten sind, gesellschaftliche Entwicklungen aufzunehmen und ihnen in den Grenzen höherrangiger rechtlicher oder ethischer Prinzipien einen Rechtsrahmen zu geben.

Die Frage nach einer Verfügungsbefugnis über die eigenen Daten indes ist nicht neu. Im Gegenteil, immer wieder gab und gibt es Überlegungen, ob und wie man die stetig voranschreitende Kommerzialisierung personenbezogener Daten auch juristisch abbilden könnte und müsste. Eine anerkannte rechtliche Theorie über die vermögensrechtliche Zuordnung personenbezogener Daten gibt es bisher jedoch nicht. Kernproblem ist dabei, dass sich personenbezogene Daten wegen ihrer fehlenden Verkörperung einerseits und ihrer Ubiquität andererseits nicht dem zivilrechtlichen Eigentumsbegriff i.S.d. §§ 903 ff. BGB unterord-

nen lassen. Dies muss freilich nicht unmittelbar zu einer Verneinung eines vermögensrechtlichen absoluten Rechts an personenbezogenen Daten führen, denn selbstverständlich gibt es auch unkörperliche Gegenstände, die – über das Immaterialgüterrecht – einer solchen vermögensrechtlichen Zuordnung zugänglich sind. So sind etwa Werke bei entsprechender Schöpfungshöhe, trotz ihres immateriellen Charakters, dem Schutz des Urheberrechts unterstellt und damit eigentumsfähig. Dem Urheberrecht lassen sich personenbezogene Daten aber nur in Ausnahmefällen, möglich etwa im Falle einer Selbstfotografie, unterwerfen, denn die erforderliche Schöpfungshöhe wird im Normalfall nicht erreicht werden. Auch das Leistungsschutzrecht des Datenbankherstellers aus §§ 87a ff. UrhG wird vereinzelt für personenbezogene Daten eingreifen, vorausgesetzt, sie sind systematisch angeordnet und eine wesentliche Investition wurde getätigt. Grundsätzlich kommt ein Urheberrecht an den eigenen personenbezogenen Daten aber nicht in Betracht und gleiches gilt für das Markenrecht. Dem Urheberrecht vergleichbare Verwertungsrechte an personenbezogenen Daten fehlen aber bisher und auch das Bundesdatenschutzgesetz, so wird vielfach vorgetragen, gewähre dem Betroffenen keine vermögenswerte Position. *Kilian* ist der Frage nach einem Anknüpfungspunkt für eine vermögensrechtliche Position an personenbezogenen Daten in den datenschutzrechtlichen Vorschriften intensiver nachgegangen und sieht in einer Gesamtschau in dem Einwilligungserfordernis des Betroffenen in die Datenverarbeitung, in seinem Recht auf Widerruf, Berichtigung, Sperrung und Löschung und der Möglichkeit nach §§ 7 und 8 BDSG Vermögensschäden bei Verletzung geltend zu machen, bereits ein „Bündel an datenschutzrechtlichen Teilrechten“ einer Person, das sich zu einer vermögenswerten Position an den eigenen marktfähigen personenbezogenen Daten verfestigt habe und als eine eigentumsähnliche Stellung zu bewerten sei. Dass zudem die §§ 28 und insbesondere 29 BDSG sogar Dritten in bestimmten Bereichen die kommerzielle Nutzung personenbezogener Daten erlauben, lässt eine Verwehrung solcher Dispositionen durch die Betroffenen selber durchaus unsachgemäß erscheinen. Aber

selbst wenn man mit guten Gründen für eine bereits im Datenschutzrecht verankerte Dispositionsbefugnis plädiert, bleibt die Frage, wie diese zur Anerkennung eines eigentumsähnlichen Rechts führen sollten, denn einziger Anknüpfungspunkt wäre das Immaterialgüterrecht, das aber personenbezogene Daten, wie oben gezeigt, grund-sätzlich nicht schützt. Ein eigentumsähnliches immaterielles Recht an den eigenen personenbezogenen Daten muss de lege lata mithin verneint werden.

3 Brauchen wir ein eigentumsähnliches immaterielles Recht an personenbezogenen Daten?

Das Gedankenspiel an diesem Punkt abzuschließen, wäre jedoch verfrüht: Tatsache ist, dass die momentane und mit der beschlossenen Datenschutzgrundverordnung auch die zukünftige deutsche und europäische Gesetzeslage den aufgezeigten Widerspruch zwischen dem internationalen Handel mit und dem erheblichen Marktwert von personenbezogene Daten auf der einen Seite und einer fehlenden vermögensrechtlichen Zuordnung zum Betroffenen auf der anderen Seite nicht zu lösen vermag. Das Hauptargument gegen die Schaffung einer vermögenswerten Position ist die fehlende Übertragbarkeit des Rechtes auf informationelles Selbstbestimmung als Teil des allgemeinen Persönlichkeitsrechts. Indes scheint diese schwarz-weiße Betrachtungsweise insbesondere vor dem Hintergrund ihrer anerkannten Durchbrechung bei der Berichterstattung über Prominente[6] zu kurz zu greifen. Der Schritt zu einer differenzierten Betrachtung hingegen ist nicht weit:

Dem Urheber werden Verwertungsrechte an seinem Werk zuerkannt und er kann (auch ausschließliche) Nutzungsrechte an seinem Werk einräumen, behält aber zugleich einen abtrennbaren, nicht übertragbaren Teil seines Urheberrechts, die Urheberpersönlichkeitsrechte, die dem persönlichkeitsrechtlichen Charakter der geistigen Schöpfung Rechnung tragen. Wollte man diesen Grundgedanken auf personenbezogene Daten übertragen, käme man zu einer Aufspaltung personenbezogener Daten in wirtschaftlich verwertbare Bestandteile und solchen, die - etwa der Intimsphäre zugehörig - nicht

[6] BGH, GRUR 1987, 127 (128) – Nena; BGH, GRUR 2000, 709 - Marlene Dietrich.

kommerzialisierbar sind. Eine Grenzziehung wäre vergleichbar der Grenze der Einwilligungsfähigkeit dort erforderlich, wo der Würdekern des Einzelnen betroffen ist, wo also eine Verwertung des personenbezogenen Datums einem Grundrechtsverzicht gleichkäme[7] und Fremdbestimmung drohte.[8] Sieht man sich die heute so populären Realityshows an, wird man allerdings schnell einsehen müssen, dass die Grenzziehung sehr von der gesellschaftlichen Entwicklung abhängt. Was vor 30 Jahren undenkbar in die Öffentlichkeit getragen worden wäre, ist heute häufig nicht einmal eine Schlagzeile wert. Das ist freilich auch gut so, denn die Rechtsordnung bildet kein starres System, an dem sich die Wirklichkeit orientieren muss, sondern vielmehr umgekehrt, ihr kommt eine „dienende Funktion" zu, die auf die gesellschaftliche Entwicklung zu reagieren hat.[9]

[7] BVerwG, Urteil vom 15.12.1981, NJW 1982, 664 (665); Hillgruber, Der Schutz des Menschen vor sich selbst (1991) S. 138.
[8] Unseld, wie vor Fn 19.
[9] GRUR 2000, 709 (713) - Marlene Dietrich.

4 Verbesserung des Datenschutzniveaus?

Aus datenschutzrechtlicher Sicht macht die Forderung nach der Schaffung eines eigentumsähnlichen immateriellen Rechts an personenbezogenen Daten aber nur Sinn, wenn ein solches Recht das Potenzial hätte, dem Datenschutz zu mehr Geltung zu verhelfen. Man mag mit dieser Forderung gerade das Gegenteil verwirklicht sehen: das Schreckensszenario eine „Zwangskommerzialisierung" personenbezogener Daten, die jene, die ihre Daten auch bisher schon leichtfertig preisgegeben haben, in ihrem Handeln noch bestärkt und andere überhaupt erst auf die Idee bringt, mit ihren personenbezogenen Daten „Geld zu verdienen".[10] Solche Befürchtungen mögen auf den ersten Blick einleuchten. Man muss und kann ihnen aber begegnen, denn bei entsprechender rechtlicher Ausgestaltung wäre gerade das Gegenteil der Fall. Ein eigentumsähnliches immaterielles Recht an personenbezogenen Daten zuzulassen, könnte dazu führen, dass die Betroffenen (endlich) wieder mehr Übersicht bekämen und ihr Grundrecht auf informationelle Selbstbestimmung effektiver ausüben können.

[10] Selbstverständlich gibt es auch Kritik von ganz anderer Seite: ein wie auch immer geartetes eigentumsähnliches Recht des Betroffenen an seinen Daten würde der Informations- und Meinungsfreiheit zuwiderlaufen (so wohl Härting, „Kommunikationsfreiheit und Datentransparenz", AnwBl 4/2011, S. 246 (248)). Dies ist zwar richtig, wie immer bei kollidierenden Grundrechten, ließe sich dieser Konflikt aber über Schrankenbestimmungen lösen, die sich etwa im Urheberrecht in der Sozialbindung des Urheberrechts niederschlagen. Sehr interessant in diesem Zusammenhang war der Vortrag von v. Lewinski, der mit seiner Matrix des Datenschutzrechts aufzeigte, dass sich die hier vorgestellten Ansichten keineswegs ausschlössen, sie vielmehr (lediglich) in unterschiedlichen Sphären des Datenschutzrechts angesiedelt seien (vgl. v. Lewinski in diesem Band und zusammenfassend Jakob, Telemedicus SoKo 2015, ZD-Aktuell 2016, 04170).

5 Verwertung ausschließlich über Verwertungsgesellschaft

Die Möglichkeit, die eigenen personenbezogenen Daten vermögensrechtlich verwerten zu können, wird den Betroffenen allein aber noch nicht weiterbringen. Wobei die mit dem dann einschlägigen Vertragsrecht einhergehende Anwendbarkeit des Verbraucherrechts[11] auf der einen Seite und der §§ 104 ff. BGB für Minderjährige auf der anderen Seite nicht zu unterschätzende Nebeneffekte wären. Nach wie vor sähen sich die Betroffenen aber großen international agierenden Unternehmen gegenüber, deren Dienste sie nutzen möchten und die im Gegenzug deren Daten erwerben. Im Vergleich würde sich die Situation kaum verbessern, denn selbstverständlich würde auch hier mangels Marktmacht keine (ernsthafte) Verhandlung über Lizenzbedingungen stattfinden.

Helfen könnte aber eine spezielle Verwertungsgesellschaft-Daten[12]. Schon lange wird datenschutzrechtlich diskutiert, dass der Einzelne gar nicht mehr in der Lage und Willens ist, datenschutzrechtliche Einwilligungen zu lesen und in ihrer Konsequenz zu erfassen, geschweige denn, einen Überblick über erteilte Einwilligungen zu behalten und seine Rechte effizient zu verfolgen. Eine Verwertungsgesellschaft ausgeformt als eine Art Datentreuhänder[13] könnte hier Abhilfe schaffen. Der Datentreuhänder übernimmt für die Betroffenen aufgrund von deren zuvor freigewählten Voreinstellungen, die Vermarktung ihrer Daten und setzt ihre Rechte durch. Gleichzeitig ließe sich die Vermarktung in Anlehnung an § 54h UrhG nur über den Datentreuhänder vornehmen. Die so gewon-

[11] Siehe auch Kilian, wie vor, S. 215.
[12] So auch bereits von Kilian, ebenda und Unseld, „Die Übertragbarkeit von Persönlichkeitsrechten“, GRUR 2011, 982 (983) angedacht.
[13] Unseld, ebenda, S. 988 mit Verweis auf Buchner, Informationelle Selbstbestimmung im Privatrecht (2006), S. 283ff.

nene Marktmacht auf Seiten der Verwertungsgesellschaft würde das Ungleichgewicht gegenüber den Internetkonzernen schmälern und bestenfalls echte Vertragsverhandlung ermöglichen.

Die Vorteile für die Betroffenen liegen auf der Hand: Sie müssten sich nicht in jedem Einzelfall durch überlange kaum verständliche Vertragsbedingungen quälen, sondern entscheiden abstrakt in den Voreinstellungen, welche Daten für welche Art von Leistungen vermarktet werden sollen oder eben nicht. Freilich müssten sie die Möglichkeit haben, diese Voreinstellungen im Bedarfsfall anzupassen. Eine solche Anpassung allein könnte dadurch, dass eine Änderung der Voreinstellungen beim Datentreuhänder erforderlich würde, geeignet sein, die Betroffenen über ihre Entscheidung (datenschutzrechtlich) nochmals nachdenken zu lassen. Gleichzeitig könnten die Betroffenen hierdurch stets einen aktuellen Überblick darüber haben, wem sie welche Daten zur Verfügung gestellt haben und auch die Rechtsdurchsetzung könnte über die Verwertungsgesellschaft erfolgen. Und letztlich hätte auch die Wirtschaft Vorteile: durch mehr Rechtssicherheit einerseits und einer vereinfachten Abwicklung andererseits, da statt vieler Betroffener nur die Verwertungsgesellschaft als Ansprechpartner in Betracht käme, wenn es um den Erwerb von personenbezogenen Daten geht.

Die Schaffung eines eigentumsähnlichen immateriellen Rechtes an personenbezogenen Daten könnte mithin den Datenschutz effektiver machen. Die überfällige Einbindung der Betroffenen in den Handel mit ihren Daten ist dabei nur ein Faktor. Mindestens ebenso wichtig ist, dass die Einräumung eines solchen Rechts und deren Ausübung über Verwertungsgesellschaften das Potenzial hätte, den Betroffenen die verlorene Übersicht zurück zu geben und gleichzeitig geeignet wäre, ihnen die Marktmacht zu geben, datenschutzfreundlicher Bedingungen durchzusetzen.

6 Fazit

Es ist nicht verwunderlich, dass der Ruf nach einer vermögensrechtlichen Zuordnung personenbezogener Daten immer wieder zu hören ist. In der Realität ist der (internationalen) Handel mit personenbezogenen Daten längst angekommen, freilich ohne dass er sich rechtlich zufriedenstellend abbilden ließe. Es ist daher erforderlich über diese Diskrepanz jenseits von scheinbar unumstößlichen Dogmen weiter nachzudenken. Ein eigentumsähnliche immaterielles Recht an personenbezogenen Daten würde die Betroffenen (endlich) an diesem Markt teilhaben lassen und die Abwicklung über eine Verwertungsgesellschaft bietet Potential, den Datenschutz und seine Durchsetzbarkeit effektiver zu machen. Dabei soll nicht der Eindruck erweckt werden, dass es eine einfache Lösung gibt - im Gegenteil. Um den Datenschutz zukunftsfähig zu machen, braucht es grundlegende und vor allem internationale Lösungen. Die nun verabschiedete Datenschutzgrundverordnung wird diesem Anspruch nicht gerecht und es ist kaum zu erwarten, dass wir in naher Zukunft weitere grundlegende Reformen des Datenschutzrechts in Europa sehen werden. Das sollte aber nicht davon abhalten, trotzdem über neue Wege nachzudenken, denn letztlich ist nach der Reform auch vor der Reform und Zeit haben wir ja jetzt.

Medienbruch und Sphärentheorie: Rückbesinnung auf Altbewährtes?

Kai v. Lewinski[1]

Kann die gute alte Sphärentheorie die Rettung des Datenschutzes sein? Dies klingt wie ein nun entferntes Donnergrollen aus der Vorzeit des Datenschutzrechts und damit fast wie eine reaktionäre These. Ein Blick zurück, ein Schritt zurück kann aber neue Perspektiven schaffen. Und von dort kann man dann neue alte Konzepte erkennen. So mögen Medienbrüche, v.a. der Idee gestufter und gradueller Öffentlichkeiten und ein rollenbasierter Datenschutz, das Datenschutzrecht der Zukunft bereichern.

[1] Überarbeitete und um Eisenbahn- und Dampfmaschinenmetaphern verschlankte Vortragsfassung von der Sommerkonferenz 2015.

1 Grenze der konzeptionellen Leistungsfähigkeit des bisherigen Datenschutzrechts

Das Datenschutzrecht ist seit der Verbreitung des Internets, also der weltumspannenden Vernetzung von (allen) Rechnern und (allen) Telefonen, spätestens jedenfalls seit der aktiven Beteiligung der Nutzer („Web 2.0“) nicht mehr zeitgemäß, da konzeptionell überholt.[2] Dies zeigt sich an der Begrifflichkeit (1.1), der faktischen Undurchführbarkeit der gesetzlichen geforderten Subsumtionsgeschwindigkeit im Computerzeitalter (1.2) und der Überdehnung des Anwendungsbereichs (1.3).

1.1 Kritik an den Begrifflichkeiten

Schon an den Begrifflichkeiten des Datenschutzrechts kann viel Kritik geübt werden.[3] Datenverarbeiter seien als „verantwortliche Stellen“ nicht mehr verantwortlich, natürliche Personen nicht mehr nur „Betroffene“, sondern Nutzer. Überhaupt ist allgemein der Begriff „Datenschutz“ unglücklich gewählt. So ist bei genauerer Betrachtung „informationelle Selbstbestimmung“ zwar das Ziel von Datenschutz, das heutige Mittel hierzu ist aber „informationelle

[2] Zusammenfassende Kritik schon bei *v. Lewinski*, Überwachung, Datenschutz und die Zukunft des Informationsrechts, in: Telemedicus e.V. (Hrsg.), Überwachung und Recht, 2014, S. 1, 10–17.

[3] *Simitis*, in: Simitis, BDSG, 8. Aufl. 2014, Einleitung, Rn. 2: „Wortwahl […] nicht gerade glücklich“; *ders.*, NJW 1971, S. 673, 676; *Druey*, Information als Gegenstand des Rechts, 1995, S. 387; *Cornelius*, NJW 2013, S. 3340, 3341; *v. Lewinski*, Die Matrix des Datenschutzes, 2014, S. 3; s.a. SPD-Entwurf für ein Bundes-Informationsschutzgesetz v. 13.12.1988 (BT-Drucks. 11/3730).

Fremdbestimmung“,[4] nämlich die rechtliche Möglichkeit des Betroffenen, dem Verarbeiter (teilweise) das Ob und Wie der ihn betreffenden personenbezogenen Datenverarbeitung vorzuschreiben.

Es handelt es sich hierbei nicht nur um einen Streit um Worte, sondern es illustriert zugleich konzeptionelle Schwächen des Datenschutzes. Der Begriff „Datenschutz“ bezeichnet ebenso wie der der „informationellen Selbstbestimmung“ das rechtliche Schutzgut nur in unscharfer Weise. Denn es verbergen sich hinter diesen Begriffen eine Mehrzahl von Schutzgütern, was sich in der einseitig auf den Begriff „Datenschutz“ fokussierten Dogmatik aber nicht abbildet.

1.2 Übergroßer rechtlicher Header

Das deutsche Datenschutzrecht beruht sehr weitgehend auf Abwägungen (s. nur § 28 Abs. 1 S. 1 Nr. 2 BDSG als Generalklausel für den nicht-öffentlichen Bereich). Mit der zunehmenden Automatisierung und Beschleunigung der Datenverarbeitung, die ja ganz ursprünglich der Anlass für das BDSG waren, ist das einzelfallbezogene Normprogramm des BDSG allerdings immer weniger kodierbar. Eigentlich soll ja bei jedem personenbezogenen Verarbeitungsschritt das gesamte Abwägungsprogramm des Datenschutzrechts durchlaufen werden. Der Overhead bei personenbezogener Datenverarbeitung (informatisch: Verwaltungsdaten) ist nach den Buchstaben des Gesetzes so enorm, dass er nicht realistisch ist. Das Gesetz fordert nämlich genaugenommen einzelfallbezogene Subsumtion im Tera-FLOP/s-Bereich, was kaum kodierbar scheint, auch konterkarierte sie den Zweck der Datensparsamkeit (§ 3a BDSG).[5] Denn jeden

[4] Zu dieser Unterscheidung *v. Lewinski*, Die Matrix des Datenschutzes, 2014, S. 40 f. et pass.

[5] Dies übersieht natürlich nicht, dass die Datensparsamkeit nach § 3a BDSG nicht auf den Umfang der Datenverarbeitung und -speicherung als solche

Verarbeitungsschritt mit der konkreten (und damit personenbezogenen) Situation des Betroffenen abgleichen zu müssen, ist, da sie dann selbst wieder personenbezogene Datenverarbeitung wäre, vom Gesetz offensichtlich nicht gewollt.

1.3 Verformung des Anwendungsbereichs

Aber nicht genug damit, dass das Datenschutzrecht die persönlichkeitsrechtsschutzrechtlichen Probleme der Zeit nicht adäquat mehr adressiert. Zusätzlich weitet sich sein Anwendungsbereich immer mehr aus, auch in Bereiche, für die es ursprünglich gerade nicht gedacht war und für das es deshalb auch konzeptionell ungeeignet ist, während ganz sensible andere Bereich ausdrücklich ungeregelt geblieben sind.

So war die heute bezeichnenderweise nur noch so genannte „Haushaltsausnahme" (§ 1 Abs. 2 Nr. 3 a.E. BDSG) ursprünglich dafür gedacht, alle nicht staatlichen und nicht gewerblichen Datenverarbeitungen umfänglich aus dem Anwendungsbereich des BDSG herauszunehmen. Das im Großrechnerzeitalter für Rechenzentren geschriebene BDSG sollte nicht das gesamte Leben erfassen, sondern eine spezifische Gefahrenlage. Dieses Regel/Ausnahme-Verhältnis hat sich über die verschiedenen Novellierungen des BDSG immer mehr umgekehrt,[6] und seit der Lindqvist-Entscheidung des EuGH[7] wissen wir, dass man nicht einmal mehr eine Kirchgemeindegruppe mit modernen Medien organisieren kann, ohne das volle Programm und die volle Härte des Datenschutzrechts zu spüren zu bekommen.

---

gerichtet ist, wohl aber auf die Minimierung der personenbezogenen Verarbeitung.

[6] Nachzeichnung bei *v. Lewinski*, Die Matrix des Datenschutzes, 2014, S. 10 f.

[7] EuGH, Urt. v. 6.11.2003, Rs C-101/01 – Bodil Lindqvist.

Ferner und weil eine funktionierende Kontrolle durch die Vierte Gewalt nicht von der Einwilligung der Kontrollierten abhängen kann, müssen die Medien datenschutzrechtlich eine Sonderrolle spielen. Bezeichnenderweise ist deshalb für den vielleicht persönlichkeitsrechtssensibelsten Bereich der Informationsgesellschaft, nämlich die personenbezogene Veröffentlichung, das Datenschutzrecht gerade nicht anwendbar. Das „datenschutzrechtliche Medienprivileg" (§ 41 Abs. 1 BDSG)[8] illustriert, dass das überkommene Datenschutzrecht für die spezifischen Gefahren der Veröffentlichung von Daten nicht gemacht ist. Im Auge eines persönlichkeitsrechtlichen Sturms bleibt das Datenschutzrecht ruhig und stumm.

Und andersherum zeigt sich in der Diskussion[9] und auch in der Gesetzgebung (insb. § 6a, § 28b BDSG) dann aber wieder eine Tendenz zur Ausweitung des Datenschutzrechts, etwa wenn es um die Einhegung der Gefahren geht, die mit Big Data verbunden sind.[10] Nun sind die gesellschaftlichen und individuellen Gefahren durch Scoring und Algorithmen keineswegs geringzuachten. Aber diese Bereiche gehören systematisch zum Statistikrecht, das – wie der datenschutzrechtliche Grundbegriff des „personenbezogenen Datums" zeigt – das Komplementärgebiet zum Datenschutzrecht darstellt.

---

[8] Aufgrund der etwas verwickelten Gesetzgebungskompetenzverteilung in Deutschland regelt § 41 Abs. 1 BDSG genaugenommen nur das datenschutzrechtliche *Presse*privileg. Die hier gemachte Grundaussage gilt aber für die übrigen Mediensektoren ebenso.

[9] Vgl. für den herkömmlichen datenschutzzentrierten Ansatz etwa *Jandt*, Beihefter 2 zu K&R 6/2015, S. 6 ff.

[10] *v. Lewinski*, Überwachung, Datenschutz und die Zukunft des Informationsrechts, in: Telemedicus e.V. (Hrsg.), Überwachung und Recht, 2014, S. 1, 13.

1.4 Zwischenbefund: „Datenschutzrecht ist kaputt."

Das Datenschutzrecht greift also in Gebiete aus, für die es dezidiert nicht konzipiert worden ist, klammert aber zugleich die Bereiche, in denen die schwersten Persönlichkeitsrechtsgefährdungen stattfinden (Medienbereich), aus. Auch der persönliche Nähebereich ist nur unvollkommen erfasst. Zudem kann erkennbar das einzelfall- und verarbeitungsschrittbezogene Regelungskonzept heute gar nicht mehr durchgeführt werden. Dass dann die Nomenklatur und Begrifflichkeit des Datenschutzrechts schief ist, rundet die Zustandsbeschreibung des Datenschutzrechts nur noch ab. – In Abwandlung von Sascha Lobo kann man sagen: „Datenschutzrecht ist kaputt."[11]

[11] Vgl. *Lobo*, Die digitale Kränkung der Menschheit, in: F.A.S. v. 12.1.2014, S. 37: „Das Internet ist nicht das, wofür ich es gehalten habe".

2 Rückbesinnung auf alte Konzepte

Das Datenschutzrecht hat sich von einem Querschnittsrechtsgebiet zu einem Über-Rechtsgebiet entwickelt, das alles und jedes Problem der Informationsgesellschaft lösen können soll. Dieser „One Law Fits All"-Anspruch würde jedes Rechtsgebiet überfordern. Bevor man aber alles „irgendwie zu Datenschutz" erklärt, sollten vielmehr die unterschiedlichen Konzepte aufgefächert werden, die heute unter dem Begriff „Datenschutz" zusammengepackt werden. Sie reichen von dem grundrechtlichen Kernbereichsschutz bis zum Kartellrecht und der Gewaltenteilung. Dies alles sollte gründlich auseinandergenommen – de-konstruiert[12] – werden. So kann man dann erkennen, welche Bauelemente sich in welchen Verwendungen bewährt haben, was ausgetauscht werden muss und was vielleicht noch fehlt.

2.1 Schutz des Eigenwerts des Menschen

Wie schon bei der terminologischen Polemik (1.1) angemerkt und wie es natürlich unter Datenschützern Allgemeingut ist, geht es beim Datenschutz nicht um den Schutz von Daten, sondern um den Schutz von Menschen. Klar bringt dies § 1 Abs. 1 BDSG zum Ausdruck, der vom „Schutz des Persönlichkeitsrechts" spricht. Das eigentliche Schutzgut des Datenschutzrechts – sein Schatz und Kern – sind also nicht Daten oder ein amorphes Schutzgut „Datenschutz", sondern das Individuum, seine Autonomie und – ins Rechtliche übersetzt – die Menschenwürde und das (Allgemeines) Persönlichkeitsrecht.

Offensichtlich sind die Würde und die Persönlichkeit des Menschen ein sehr fragiles Gut, und Verletzungen sind oft nicht gutzumachen und können lebens-

[12] Ausführlich hierzu *v. Lewinski*, Die Matrix des Datenschutzes, 2014.

lang spürbar bleiben. Deshalb ist es eine sinnvolle Entscheidung, den Schutz des Eigenwerts des Menschen vorzuverlagern.

2.2 Raum- und sphärenbezogene Schutzkonzepte

Die älteste Vorverlagerung des Schutzes des Eigenwerts des Menschen – Abstraktion der normativ-tatbestandlichen Anknüpfungen am Risiko statt an der Verletzung – sind raumbezogene Schutzkonzepte.[13] Die Höhle des Steinzeitmenschen, die Klotür, der Vorhang am Fenster – das Abschirmen eines „privaten" Raums ist eine kulturelle Grundtechnik, die durch das Recht (Hausfriedensbruch) seit jeher geschützt wird. Und was uns früher die Höhle und dem Engländer seit jeher seine Burg, ist heute das „informationstechnische Systeme", diese programm-logisch bestimmte Sphäre, deren Vertraulichkeit und Integrität nun verfassungshoch geschützt sind.[14]

Letztlich beschreiben diese Ansätze, bezogen auf den Schutz des Eigenwerts des Menschen, einen typisierten und abstrahierten Schutzraum,[15] mit anderen Worten: eine Sphäre. Nun wird die informationelle Sphärendogmatik im überkommenen Datenschutzschrifttum teilweise grundsätzlich abgelehnt.[16] Das Festhalten an diesem ablehnenden Dogma der Kontextabhängigkeit ist aber weder mit der (europarechtlich eingeführten) Kategorie der sensitiven Daten (vgl. § 3 Abs. 9 BDSG) noch mit der Kernbereichsrechtsprechung des BVerfG[17]

[13] Vgl. zum Schutzraum-Konzept *Wolff*, in: Wolff/Brink, Datenschutzrecht in Bund und Ländern, 2013, Syst. A, Rn. 2 ff.; ähnlich zum Umfeldschutz *v. Lewinski*, Die Matrix des Datenschutzes, 2014, S. 29.
[14] BVerfGE 120, S. 274, 302 ff. – Online-Durchsuchung.
[15] *v. Lewinski*, Die Matrix des Datenschutzes, 2014, S. 39.
[16] Statt vieler *Simitis*, in: Simitis, BDSG, 8. Aufl. 2014, § 1 BDSG, Rn. 65–68.
[17] Umfassend *I. Dammann*, Der Kernbereich der privaten Lebensgestaltung, 2011.

zu vereinbaren, hat also seinerseits die dogmatische Anschlussfähigkeit verloren.

2.3 Gesamtgesellschaftliches Informationsgleichgewicht

Gegenüber der Frühzeit des Datenschutzrechts findet die gesamtgesellschaftliche Dimension von Datenverarbeitung jedenfalls in der praxisorientierten juristischen Diskussion kaum noch Widerhall. Das Datenschutzrecht ist ganz auf das individualistische Verhältnis von Verarbeiter (= verantwortliche Stelle) und Individuum (= Betroffener) fixiert. Soweit ersichtlich ist es in der deutschen Gesetzeslandschaft allein § 1 Abs. 1 Nr. 2 des hessischen Landesdatenschutzgesetzes, wo der Aspekt des Informationsgleichgewichts überhaupt aufgegriffen wird.

Dabei ist etwa das Problem der vielen netzbasierten Dienste (Soziale Netzwerke, Suchmaschinen, Cloud, SaaS) nicht so sehr, dass sie uns jeweils über die Schulter auf die Tastatur (und sonst wohin) schauen, um die angebotenen Dienste individueller zuzuschneiden und zu verbessern. Das Problem ist, dass die Anbieter dies bei einem so großen Teil der (Welt-)Bevölkerung tun und wir informationelle Unverschämtheiten von Monopolisten nicht ohne weiteres durch einen Anbieterwechsel ausweichen können.

Es scheint naheliegend, das Datenschutzrecht (wieder) um diesen überindividueller Aspekt zu ergänzen.[18] Hierfür kann man sich etwa vom Kartellrecht inspirieren lassen, um Datenmacht zu beschränken; auch das Steuerrecht mag

[18] *Bull*, Sinn und Unsinn des Datenschutzes, 2015, S. 116 f.; *Pohle*, DANA 1/2016, S. 14 ff.; *v. Lewinski*, Die Matrix des Datenschutzes, 2014, S. 55 et pass.; *ders.*, Überwachung, Datenschutz und die Zukunft des Informationsrechts, in: Telemedicus e.V. (Hrsg.), Überwachung und Recht, 2014, S. 1, 21 f.

dazu genutzt werden, Datenmacht zu bepreisen. Überhaupt könnte das Wirtschaftsrecht an vielen Stellen in Richtung einer Datensparsamkeit steuern.

2.4 Zwischenstand: Rückbesinnung, nicht Rückbau

Das gegenwärtige Datenschutzrecht krankt daran, dass sehr stark auf das eine Konzept der Regelung der einzelnen Schritte der Verarbeitung personenbezogener Daten fokussiert wird. Dabei sind frühere oder andere „Datenschutz"-Konzepte nicht falsch und auch nicht allein deshalb überholt, weil sie vielleicht schon etwas betagt sind.

3 Matrix des Datenschutzes

Allerdings ist ein Blick zurück und eine Rückbesinnung auf alte Konzepte allein kein Modell für einen zukunftsfesten Datenschutz. – „Back to the Roots" ist keine Lösung, „Old School" kein Konzept. Allerdings kann man die älteren Ansätze des Persönlichkeitsschutzes mit dem heutigen Stand des Datenschutzes durchaus im Zusammenhang betrachten, um hierdurch die Richtung der künftigen Entwicklung des Datenschutzrechts vorherzusagen oder jedenfalls einzuschätzen.[19]

Dabei ergeben sich – jedenfalls für den Verfasser dieser Zeilen – fünf Ebenen des Privatheits- bzw. Datenschutzes.[20] Der eben schon erwähnte (2.1) Eigenwert des Menschen ist das eigentliche und grundlegende Schutzgut, dessen ebenfalls schon angesprochene (2.2) sphärenhafte Vertypung eine erste Schicht des Vorfeldschutzes[21] als zweite Ebene. Das gegenwärtige Datenschutzrecht kann auf einer dritten Ebene als informationelle Fremdbestimmung oder Fremdbeschränkung verstanden werden (Fn. 3). Als nächste, vierte Stufe, die wir gegenwärtig schon in Umrissen erahnen,[22] ist die informationelle Verfügung und Gestaltung, also „Market Privacy" oder informationelle Selbstbestimmung auch im rechtstechnischen Sinne einer Selbstverfügungsmöglichkeit.

---

[19] Zu Zufall und Notwendigkeit bei der Datenschutzentwicklung *v. Lewinski*, in: Pohle/Knaut, Geschichte und Theorie des Datenschutzes (Fundationes I), 2014, S. 9 ff.

[20] *v. Lewinski*, Die Matrix des Datenschutzes, 2014, S. 17–63, s.a. S. 88.

[21] Zum Konzept des Vorfeldschutzes im Bereich des Umweltschutzes *Smeddinck/Willmann*, UPR 2015, S. 285 ff.

[22] Dazu in diesem Tagungsband *Krügel*, Ist es Zeit für ein eigentumsähnliches immaterielles Recht an personenbezogenen Daten?, S. 49 ff.

Schließlich und als fünfte Ebene ist an die gesamtgesellschaftliche Informationsordnung zu denken (vgl. 2.3), die dann allerdings auch wieder Rückwirkungen auf die informationelle Stellung des Individuums und dessen Eigenwert hat.

Dieses Modell dient nun nicht der chronologischen Illustration geschichtlicher Entwicklungsphasen des Datenschutzes, sondern will als Kaskadenmodell[23] unterschiedliche Ebenen des aktuellen und künftigen Datenschutzes auseinanderzuhalten helfen. Verschränkt mit verschiedenen Schutzkonzepten ergibt sich eine „Matrix des Datenschutzes". Diese Matrix nun kann dazu genutzt werden, um neue und vielleicht kommende Arten des Datenschutzes vorherzusagen.[24]

[23] Näher dazu *v. Lewinski*, Die Matrix des Datenschutzes, 2014, S. 82 f.
[24] Zu diesem Nutzen der „Matrix" *v. Lewinski*, Die Matrix des Datenschutzes, 2014, S. 89 f.

4 Konzept von Öffentlichkeit*en*

Insbesondere die fünfte Stufe der Datenschutz-Schutzgüter – das informationelle gesellschaftliche Gleichgewicht – wird bislang noch (zu) wenig betrachtet. Dabei können hier zwei neue oder jedenfalls weitere Konzepte von Datenschutz verortet werden: künstliche Medienbrüche und damit verbunden das Konzept sozialer Rollen. Sie können in jeweils als Ausprägung von „Öffentlichkeit*en*" begriffen werden.

4.1 Scheinbare Binarität von Öffentlichkeit und Privatsphäre

Das Datenschutzrecht geht – wie weite Teile des Informationsrechts insgesamt – von einer Entgegensetzung von „öffentlich" und „privat" aus. Haus und Heim haben eine Drinnen und ein Draußen;[25] ein Geheimnis kann nur solange bestehen, wie es geheim ist. Auch die grundrechtliche Informationsfreiheit (Art. 5 Abs. 1 S. 1 GG) kennt die „allgemein zugängliche Quelle" als Kategorie des Öffentlichen. Das Datenschutzrecht unterscheidet ebenfalls danach, ob etwas öffentlich (vgl. § 13 Abs. 2 Nr. 4, § 14 Abs. 2 Nr. 5, § 28 Abs. 1 S. 1 Nr. 3, § 29 Abs. 1 S. 1 Nr. 2 BDSG) ist oder nicht; entsprechendes gilt für das Informationszugangsrecht (§ 9 Abs. 3 Var. 2 IFG).

Allerdings verschwimmt die Grenze zwischen „öffentlich" und „privat" im Maße und Wege der Digitalität und Vernetzung. Alles, was digitalisiert und vernetzt ist, ist potentiell ubiquitär verfügbar und nur durch mehr oder minder starke

[25] Auch die Haut wird v.a. im Anschluss an *Vilém Flusser* als Grenze zwischen dem Innen und Außen verstanden (zu *Flussers* Haut- und Körperbild z.B. *Guldin*, Ineinandergreifen grauer Zonen, in: Kleinschmidt/Hewel, Topographien und Grenzen, 2011, S. 39 ff. mit vielen Nachw.; allgemein zu diesem Aspekt *Benthien*, Haut. Literaturgeschichte – Körperbilder, Grenzdiskurse, 2001).

Verschlüsselungen und Passworte geschützt. Die Digitalität als umfassende Verarbeitbarkeit überwindet überkommene Schranken, Grenzen und Entfernungen. So scheint es sinnvoll, rechtlich, technisch und sozial künstliche Brüche in die vernetzte Welt einzubauen.

4.2 Teilöffentlichkeiten

Eine Möglichkeit hierzu ist das künstliche Schaffen und Erhalten von Teilöffentlichkeiten. Teilöffentlichkeiten werden in vielen Fällen durch einen Medienbruch konstituiert. So ist etwa die Gerichtsöffentlichkeit zwar umfänglich gewährleistet, zugleich aber durch ein Verbot von Ton- und Filmaufnahmen flankiert; die Allgemeinheit soll die richterliche Tätigkeit kontrollieren können, ohne aber zugleich Eindrücke von Tätern und Opfern medienbruchlos aus dem Gerichtssaal herauskommunizieren können (§ 169 GVG). Auch das Google Spain-Urteil des EuGH[26] kann als die Anordnung eines künstlichen Medienbruchs gelesen werden; so wird zwar der – medienfreiheitsrechtlich geschützte – eigentliche Inhalt nicht gelöscht, wohl aber dessen Auffindbarkeit mittels Beschränkung der personenbezogenen Suchmöglichkeit erschwert; die (globale) Suchmaschinenöffentlichkeit ist also beschränkter als die (lokale) Zeitungsleseröffentlichkeit. Aus dem Medienrecht kennen wir ferner Sendezeitbeschränkungen zu Zwecken des Jugendschutzes, die ein Medienbruch in zeitlicher Hinsicht sind. Auch proprietäre Datenformate können als logische Zweckbindung und Vorkehrung gegen eine unbegrenzte Verbreitung interpretiert werden.

[26] EuGH, 13.05.2014, C-131/12 – Google Spain.

4.3 Rollenbasierung

Ähnlich, aber stärker vom Betroffenen her konstruiert wäre ein datenschutzrechtliches Denken von der sozialen Rolle her,[27] einem Konzept, das der Informatik und Psychologie gleichermaßen geläufig ist. Wenn der Mensch, die ja im Ausgangspunkt zu schützende Persönlichkeit, gar nicht in den Blick genommen wird, sondern nur der jeweils relevante Ausschnitt, kann dies in vielen Konstellationen die Gesamtheit der Persönlichkeit schützen. Das im deutschen Datenschutzrecht verbreitete (technisches bzw. logische) Konzept des Pseudonyms fällt hierunter, ebenso die Erschwerung einer Indexierbarkeit durch das Verbot von Personenkennziffern.

[27] Aus dem älteren juristischen Schrifttum *Müller*, ÖVD 1973, S. 61 ff.; *ders.*, in: Dammann/Karhausen/ders./Steinmüller, Datenbanken und Datenschutz, 1974, S. 63, 65 ff.; *ders.*, Soziale Kontrolle durch Datenbanken, in: Krauch, Erfassungsschutz, 1975, S. 141 ff.; ausführlich auch darauf aufbauend *Meister*, Datenschutz im Zivilrecht, 1977, S. 98–109; vgl. auch *Simon*, JA 1985, S. 450, 572, 575; aktuell zuletzt *v. Lewinski*, Die Matrix des Datenschutzes, 2014, S. 38 f.

5 Ein Schritt zurück, um Anlauf zu holen

Das Datenschutzrecht, wie wir es seit den Siebziger Jahren kennen und das sich auch durch die EU-Datenschutz-Grundverordnung konzeptionell nicht weiterentwickeln wird, ist keine universelle Antwort auf die Herausforderungen der Informationsgesellschaft. Grund ist eine einseitige Betonung und Fokussierung auf das individuelle (und einzelverarbeitungsschrittbezogene) Verhältnis zwischen (nur) Verarbeiter und Betroffenem. Datenschützer und Protagonisten eines hohen informationellen Schutzniveaus sollten sich nicht in dieser hohlen Gasse des überkommenen Datenschutzrechts verkämpfen, sondern einen Schritt zurückgehen, um weitere Wege für besseren oder anderen Datenschutz erblicken zu können. Der Schritt zurück führt nicht zu weniger Datenschutz, weil man ja dort nicht stehenbleiben soll, sondern von dort nach neuen Pfaden schauen kann, die dann mit frischem Anlauf beschritten werden können.

Brave New World: Grundrechtsschutz durch Technik

Agata Królikowski

1 „Digitale“ Grundrechte

Die Rede von „digitalen“ Grundrechten ist spätestens mit der Forderung nach einer Internet-Charta Ende 2015 als Schlagwort auch in die Mainstream-Medien vorgedrungen.[1] Im Gegensatz zum klassischen Kommunikationsmedium wie dem Telefon vereint das Internet Funktionen verschiedener Medien und erweitert diese.[2] Es bildet eine neue Sphäre öffentlicher Kommunikation, in der Meinungsfreiheit, Kunstfreiheit, Berufsfreiheit, ja sogar Versammlungsfreiheit wahrgenommen werden können. Auch der Staat nutzt diese Möglichkeiten im Rahmen von eGovernment. So ist es in allen gesellschaftlichen Bereichen relevant, seien es wirtschaftliche, staatliche oder private.[3]

Dass das Digitale Herausforderungen an das Recht formuliert, ist keine neue Erkenntnis und zeigt sich immer wieder in den verschiedenen Forderungen nach Grundrechten, die der digitalen Welt gerecht werden.[4] Ob nun das Digitale eigenständige Grundrechte begründet oder nicht, so eröffnet es doch zumindest eine weitere Dimension, die jedem einzelnen Grundrecht innewohnt.[5] Darüber hinaus gibt es aber auch eine technische Dimension, nämlich dann, wenn nicht rechtliche Verfahren, sondern wenn die Technik quasi Voraussetzung ist und den Schutz eines Grundrechts (z. B. Anonymisierung, Verschlüsselung) oder eine Grundrechtsausübung (z. B. Ausübung der Meinungsfreiheit im Internet) gewährleistet.

---

[1] Vgl. *Maas*, Unsere digitalen Grundrechte, ZEIT online vom 10.12.2015, URL: http://www.zeit.de/2015/50/internet-charta-grundrechte-datensicherheit [26.2.2016].
[2] Vgl. *Królikowski*, Packet Inspection in Zeiten von Big Data, in: Überwachung und Recht, 2014, S. 161.
[3] Vgl. *Hoffmann/Luch/Schulz/Borchers*, Die digitale Dimension der Grundrechte, 2015, S. 21.
[4] Vgl. Fn. 1 oder auch *EDRi*, Die Charta, URL: https://www.wepromise.eu/de/page/charta [26.2.2016].
[5] Vgl. *Hoffmann* et al., Die digitale Dimension der Grundrechte, 2015, S. 25.

Unsachgemäß oder bösartig eingesetzt, schafft die Technik eine Bedrohungslage für Bürger, aus der sie ohne neue rechtliche Rahmenbedingungen, technische Weiterentwicklungen und neue Kompetenzen nicht so leicht entkommen.

Dabei haben gewisse technische Designentscheidungen erheblich zu der heutigen Situation beigetragen. Ein zentrales Beispiel ist dabei die paktetbasierte Informationsübertragung im Internet. Wird die Kommunikation nicht verschlüsselt, können mit Hilfe der sogenannten *Deep Packet Inspection* alle Metadaten und Inhalte gelesen und analysiert werden. Sowohl bei der unverschlüsselten als auch bei der verschlüsselten Datenübertragung können darüber hinaus statistische Verfahren angewendet werden, die Muster in der Kommunikation aufdecken und letztendlich auch über die Inhalte der Kommunikation Aufschluss geben können. Das Verhalten der Bürger im Internet ist daher sehr gut großflächig und in Echtzeit überwachbar.[6] Die Technik schafft hier die Fakten, die Bürger und das Recht haben das Nachsehen.

Zudem tritt neben die staatlichen Eingriffe in Grundrechte immer stärker auch die Bedrohung der Grundrechte durch Private.[7] In der Diskussion stehen Eingriffe in die Meinungsfreiheit, Datenlecks oder Allgemeine Geschäftsbedingungen, die Bürger dazu bringen, Daten herzugeben, die nicht immer notwendig sind. Daneben geht es inzwischen ebenso nicht mehr nur darum, Eingriffe zu vermeiden, sondern auch darum, technische und rechtliche Rahmenbedingungen zu schaffen, die es den Bürgern erlauben, ihre Grundrechte wahrzunehmen. So verlieren Grundrechte als Abwehrrechte im Digitalen zunehmend an Bedeutung.[8]

---

[6] Vgl. *Królikowski*, S. 148.
[7] Vgl. *Hoffmann* et al., S. 17.
[8] Vgl. *Hoffmann* et al., S. 68.

Auch die Diskussion um das Urteil des EuGH zum Recht auf Vergessen[9] zeigt, dass sich die Rechtssetzung, Rechtsanwendung und Rechtsprechung zur Zeit in einer Übergangsphase befinden. Dennoch können die Schwächen der Technik regulatorisch noch eine ganze Weile nicht abgemildert werden.[10] Doch die Diskussion zeigt ebenfalls, dass Grundrechte neu gedacht und neu beleuchtet werden müssen. Digitale Technik erweitert den Schutzbereich der Grundrechte, der in der rechtlichen und technischen Diskussion bisher ein blinder Fleck war. Aber brauchen wir gänzlich neue Grundrechte etwa in Form von digitalen Grundrechten oder Grundrechten, die auf die Technik hin maßgeschneidert werden?[11] Oder erweitert das Digitale unsere Grundrechte nur um eine Dimension, die wir mitdenken müssen?[12] Wie auch immer die Antwort lauten mag, in jedem Fall zeichnet sich ein Paradigmenwechsel der Grundrechte ab.

Und während die Grundrechte neu diskutiert und neue rechtliche Lösungen gesucht werden, bleibt die Frage, wie die Grundrechte der Bürger in der Zwischenzeit geschützt bleiben.

[9] EuGH vom 13.5.2014, Az. C-131/12.
[10] Vgl. *Hoffmann* et al., S. 50.
[11] Vgl. z. B. *Lewinski*, Überwachung, Datenschutz und die Zukunft des Informationsrechts, in: Überwachung und Recht, S. 27.
[12] Vgl. *Hoffmann* et al., S. 25.

2 Brave New World: Grundrechtsschutz durch Technik

Eine mögliche und zur Zeit einzige praktikable Lösung ist der Selbstschutz der Bürger durch Technik. Technik wird dabei zur Vermittlerin zwischen Grundrechten und den Bürgern. Zudem verschieben sich Machtgefüge und Verantwortlichkeiten, denn durch die Technik spielen neue Akteure eine Rolle für den Grundrechtsschutz: Informatiker und Technikanbieter. Plötzlich übernehmen sie im Zuge von Technikentwicklung, die beispielsweise der Verschlüsselung dient, Verantwortung nicht nur für ihr Produkt, sondern weitergehend auch für die Funktion von Grundrechten. Die Perspektive wechselt vom Bürger auf den technischen Nutzer und aus dem Zweier-Verhältnis Bürger/Nutzer – Grundrechtsgefährder wird eine Dreiecksbeziehung Softwareentwickler/-anbieter – Bürger/Nutzer – Grundrechtsgefährder. Die verwendete Technik wirkt zurück auf die Softwareentwickler und ihr Produkt. Software bekommt dadurch eine grundrechtliche Dimension, wodurch der Softwareentwicklungsprozess (ähnlich wie bei sicherheitsrelevanten Systemen) und die Softwarequalität eine besondere Betonung erhalten.

Eine weitere Rückkopplung zwischen Technik und Grundrechten findet sich auch in den rechtlichen Anforderungen an die Technik wie beispielsweise in der Datenschutzgrundverordnung bei dem Begriff *Privacy by Design* bzw. *Privacy by Default* oder auch in dem 2015 in Kraft getretenen IT-Sicherheitsgesetz.[13] So hat beispielsweise das Konzept Privacy by Design direkte Auswirkungen auf den Technikentwicklungsprozess. Als Paradigma muss es von Anfang an und zu jeder Zeit berücksichtigt werden. Das von Ann Cavoukian in den 1990er Jahren geprägte Konzept umfasst dabei sieben Prinzipien: Es

[13] Z. B. bei der Änderung des § 13 TMG.

dient der Vorbeugung und nicht als Abhilfe; Datenschutz ist die Standardeinstellung (Privacy by Default); der Datenschutz ist in das Design eingebettet; keine Kompromisse, das heißt, es sollen alle Interessen berücksichtigt und keine gegeneinander ausgespielt werden; der Schutz der Privatsphäre soll während des gesamten Lebenszyklus der erhobenen Daten gewährleistet sein; Sichtbarkeit sowie Transparenz der Komponenten und Operationen sollen für Vertrauenswürdigkeit sorgen.[14] Weitere rechtliche Forderungen an die Technik, die sich aus Privacy by Design entwickelt haben lauten, *Privacy by Assistance*[15] (Nutzer sollen nicht mit der Technik allein gelassen werden), *Privacy by Adjustment* (Anpassung an den eigenen Bedarf der IT-Nutzung), *Privacy by Trust* (vertrauensbildende Maßnahmen für die Vereinbarkeit von Unternehmens- und Verbraucherinteressen), *Privacy by Transparancy* (Eingriffe in die Privatsphäre werden offen gelegt). All diesen Konzepten ist gemein, dass sie schon während des Entwicklungsprozesses der Software mitgedacht werden müssen. Dies wiederum setzt aber voraus, dass sowohl die Entwickler oder die Auftraggeber der Software diese Konzepte kennen und in den Anforderungskatalog aufnehmen.

Dabei ist Transparenz eine immer wieder auftauchende Anforderung an Software und ihre Entwicklung. Man findet sie in Forderungen nach nachvollziehbaren Standardisierungsprozessen, nach offenen Standards sowie nach einsehbarem Code (bzw. in der weitergehenden Form sogar Open Source) wieder.[16] Diese Anforderungen können je nach Sichtweise als allgemeine Designparadigmen für Software betrachtet werden. Doch bei Software, die grundrechtsrelevant ist, gelten diese Anforderungen in besonderer Weise. Beispielsweise

---

[14] Vgl. *Cavoukian*, Privacy by Design, The 7 Foundational Principles, August 2009, URL: https://www.ipc.on.ca/images/Resources/7foundationalprinciples.pdf [26.2.2016].
[15] Vgl. *Hoffmann* et al., S. 49.
[16] Vgl. *Schneier*, Secrecy, Security, and Obscurity, vom 15.5.2002, URL: http://www.schneier.com/crypto-gram-0205.html#1 (26.2.2016).

erfüllt Transparenz bei Verschlüsselungssoftware eine wichtige Sicherheitsfunktion. Es ist möglich, die Software danach zu beurteilen, ob sie Fehler enthält oder gar sogenannte Hintertüren eingebaut sind, bei denen die Schlüssel der Nutzer an unberechtigte Dritte ohne Wissen der Nutzer weitergegeben werden.

Grundrechtsschutz im Digitalen ist maßgeblich von der Software abhängig. Daher müssen von rechtlicher Seite aus Rahmenbedingungen geschaffen werden, um die Softwareentwicklung optimal zu gewährleisten. Erst so erfahren Sicherheitsaspekte, Lizenzfragen und Bedienbarkeit eine adäquate zeitliche und monetäre Würdigung.

3 Die Seite der Nutzer

Allerdings darf in dieser Diskussion die Seite der Nutzer nicht fehlen. Schließlich sollen sie selbst die Verantwortung für die Durchsetzung und die Abwehr ihrer Grundrechte im digitalen Raum übernehmen.

Wohlgemerkt muss die Abwälzung des Grundrechtsschutzes auf die Nutzer im großen Umfang eine Übergangslösung bleiben. Alles andere wäre eine Bankrotterklärung des Rechtsstaates. Aber die Alternative, nämlich die digitale Dimension nicht zu betreten, das Internet nicht zu nutzen, kann nicht die Lösung sein. Zwar ist Datensparsamkeit ist ein sinnvoller Ansatz, jedoch sollte auch beachtet werden, dass die Nutzung des Internets selbst unter die Ausübung von Grundrechten fällt und die verschiedenen Grundrechte nicht gegeneinander ausgespielt werden dürfen.

Die Frage der selbstverantworteten Schutzmaßnahmen reicht über die Bedienbarkeit der Software weit hinaus. Vielmehr spielen die Motivation und Kompetenzen der Nutzer eine zentrale Rolle, die wiederum seitens der Informatiker bei der Entwicklung der Technik berücksichtigt werden müssten. Gleichzeitig muss (neben der grundrechtlichen Debatte) das Recht Rahmenbedingungen schaffen, um technische Paradigmen wie beispielsweise Sicherheitsanforderungen, Privacy by Design, Privacy bei Assistance oder gut benutzbare Oberflächen auch um- und durchsetzen zu können.

Technik wird immer komplexer und gleichzeitig nimmt die Herrschaft der Nutzer über ihre eigenen Daten immer mehr ab.[17] Um Selbstschutzmaßnahmen wie E-Mailverschlüsselung, Smart Privacy Management, Antivirusprogramme, Anonymisierungstools, Firewalls ergreifen zu können, müssten Nutzer die

[17] Vgl. *Hoffmann* et al., S. 48.

Technik in Gänze verstehen. Das Abwälzen der Verantwortung für Grundrechte auf die Nutzer setzt implizit voraus, dass zum einen Nutzer dieser Verantwortung nachkommen können und zum anderen auch wollen.

Ein Hindernis hierbei ist, dass Datensicherheit und der daraus resultierende Schutz der Privatsphäre für viele Nutzer eine untergeordnete Rolle in der Nutzung ihres Computers spielen.[18] Ist die Verschlüsselungssoftware dann auch noch schwierig zu bedienen, kann von den meisten Nutzern nicht erwartet werden, dass sie sich mit den oben erwähnten Sicherheitsaspekten und Gefahren für ihre Internetkommunikation beschäftigen. An dieser Stelle tritt häufig Überforderung auf, gepaart mit dem Unverständnis, warum man überhaupt etwas tun sollte.[19] Man sei doch nicht wichtig genug, private E-Mails seien unkritisch, oder der Glaube, jemand anders kümmere sich schon um die Sicherheit, sind Gründe, die Nutzer immer wieder anführen, warum sie beispielsweise nicht ihre E-Mails verschlüsselten. [20] Oder wie es ein Teilnehmer in einem Workshop formulierte: „Warum sollte ich meine E-Mails verschlüsseln? Das macht doch GMX für mich." [21]

In der Regel haben Nutzer also ein sehr geringes Verständnis davon, wie das Internet, E-Mail und Verschlüsselung funktionieren.[22] Und: Sie haben kaum ein Bewusstsein für die eigenen Grundrechte und kaum Motivation, sich der Thematik anzunehmen. Auch eine Umfrage des Digitalverbandes Bitkom vom Januar 2016 zeigt, dass sich das Selbstschutzverhalten der Nutzer in den letzten Jahren kaum verändert hat. Verschlüsselten im Vorjahr 14 Prozent der Nutzer

---

[18] Vgl. *Whitten/Tygar,* in: Proceedings of the 8th Usenix Security Symposium, 1999, S. 172.
[19] Vgl. *Hoffmann* et al., S. 76.
[20] So auch in Untersuchungen mit Nutzern immer wieder zu finden, vgl. *Renaud* et al., Why Doesn't Jane Protect Her Privacy?, in: PETS 2014, S. 12.
[21] Zitat eines Nutzers aus dem Workshop „Selbstverteidigung Digitaler Grundrechte" auf der Schweriner Wissenschaftswoche, „Die digitale Gesellschaft" am 7.10.2014.
[22] Vgl. *Renaud* et al., S. 15.

ihre E-Mails, sind es aktuell 15 Prozent.[23] Ein häufig genannter Grund hierfür ist, dass der Aufwand zu hoch sei. Immer wieder wird auch darauf hingewiesen, dass Software, die sogenannten Selbstschutzmaßnahmen dient, einfach schlecht bedienbar wäre.

Dabei trifft schlechte Bedienbarkeit das Problem nicht im Kern. Vielmehr müssen Nutzer nicht nur wissen, an welcher Stelle welche Knöpfe geklickt werden müssen, sondern auch, welche Grundrechte in Gefahr sind und grundlegende informatische Konzepte kennen. Damit ist also explizit nicht die Nutzung von Software gemeint, sondern unter Umständen das Wissen um mathematische Verfahren, Infrastruktur oder Sicherheitsaspekte. Dieses Wissen geht daher weit über Medienkompetenz hinaus.

3.1 Konzepte und Kompetenzen: Beispiel E-Mailverschlüsselung[24]

Und so überrascht es nicht, dass Untersuchungen mit Nutzern gezeigt haben, dass die Bereitschaft zur Nutzung von E-Mailverschlüsselungssoftware nicht nur mit der Gestaltung der Oberfläche zusammenhängt, sondern auch damit, inwieweit die Software die Nutzer mit technischen Konzepten regelrecht belästigt.

Wenn man sich die typischen Schritte anschaut, die Nutzer gehen müssen, wenn sie Verschlüsselungssoftware benutzen möchten, steht zunächst einmal die Frage im Raum, auf welcher Ebene die Verschlüsselung stattfinden soll: Soll die Nachricht Ende-zu-Ende-verschlüsselt werden, sollen nur die Server mitei-

[23] Vgl. *Bitkom*, Verschlüsselung von E-Mails kommt nur langsam voran, Pressemeldung vom 21.1.2015, URL: https://www.bitkom.org/Presse/Presseinformation/Verschluesselung-von-E-Mails-kommt-nur-langsam-voran.html (26.2.2016).

[24] Das Signieren soll an dieser Stelle nicht weiter vertieft werden, die Probleme stellen sich aber in einer ähnlichen Weise.

nander verschlüsselt kommunizieren, geht es vielleicht auch nur um die Sicherstellung der Identität der Kommunikationspartner? Allein um diese Fragen einigermaßen sicher beantworten zu können, müssen Nutzer zumindest in Ansätzen die Funktionsweise des Internets kennen und verstehen. Die E-Mailanbieter können den Nutzern zwar Teile der Verantwortung für den Schutz der eigenen Daten abnehmen, indem sie für verschlüsselte Serverkommunikation sorgen[25] oder sicherstellen, dass bestimmte E-Mailadressen nur mit bestimmten IP-Adressen benutzt werden können.[26] Zudem gibt es Verfahren wie beispielsweise De-Mail,[27] mit deren Hilfe die Mails abschnittsweise verschlüsselt werden[28] und somit die Vertraulichkeit und Integrität sichergestellt werden soll. Doch sollen Nachrichten auf der gesamten Strecke vom Sender zum Empfänger Ende-zu-Ende-verschlüsselt werden, müssen die Nutzer sich mit der Technik auseinandersetzen und selbst dafür sorgen.

Da in Netzwerken die asymmetrische Verschlüsselung eine wichtige Rolle spielt, wird der Nutzer auch mit dem Konzept des privaten und öffentlichen Schlüssels bzw. Zertifikats konfrontiert.

Um einen öffentlichen Schlüssel auch an bestimmte Identität zu binden, d. h. sicherzustellen, dass der Empfänger der Nachricht auch Inhaber des öffentlichen Schlüssels ist, werden Zertifikate ausgestellt. Wie das geschieht, hängt

---

[25] Z. B. mit Hilfe des Protokolls DNS-based Authentication of Named Entities DANE, das die verschlüsselte Kommunikation mit einem anderen Server erzwingt, vgl. *Hoffman et al.*, RFC 6698, URL: https://tools.ietf.org/html/rfc6698 [26.2.2016].

[26] Z. B. mit Hilfe des Protokolls Sender Policy Framework (SPF), vgl. *Kitterman*, RFC 7208, URL: https://tools.ietf.org/html/rfc7208 (26.2.2016) oder Domain Key Identified Mail (DKIM), vgl. Allman et al., RFC 4871, URL: https://tools.ietf.org/html/rfc4871 (26.2.2016).

[27] Vgl. *BMI*, De-Mail – einfach verschlüsselt und jederzeit nachweisbar, URL: http://www.cio.bund.de/Web/DE/Innovative-Vorhaben/De-Mail/de_mail_node.html (26.2.2016).

[28] Die Ende-zu-Ende-Verschlüsselung ist optional, worum sich der Absender aber selbst kümmern muss.

vom Vertrauensmodell ab, für das sich wieder die Nutzer entscheiden müssen: Entweder der Nutzer vertraut einer zentralen Instanz (*Certification Authority*, CA), die öffentliche Schlüssel mit Hilfe von Zertifikaten beglaubigt (z. B. bei S/MIME)[29] oder die Nutzer überprüfen die Echtheit der Schlüssel selbst und schaffen damit das sogenannte *Web of Trust* (PGP). Die Wahl eines dieser Modelle verlangt dem Nutzer eine technische, aber auch ideologische Entscheidung ab, nämlich die Frage, welche Art der *Public-Key-Infrastruktur* (PKI) er für vertrauenswürdiger erachtet. Wofür auch immer er sich entscheidet, beide Seiten der Kommunikation müssen sich auf dasselbe Modell einigen. Bedienbarkeit richtet sich auch danach, ob solche Entscheidungen den Nutzern weitestgehend abgenommen werden. Darüber hinaus sollten alle Funktionen sollten mit griffigen Metaphern oder Piktogrammen so umschrieben sein, dass Nutzer sich intuitiv zurechtfinden.

Ein weiterer und immer wieder diskussionswürdiger Punkt ist auch, ob Nutzer in der Lage sind, richtig einzuschätzen, ob ein System sicher und damit vertrauenswürdig ist. Diese Frage wird bei konkreten Systemen selbst in der technischen Literatur und Praxis immer wieder heftig diskutiert.[30] Vertrauenswürdige Systeme zu bauen hat Implikationen, die selbst Informatiker schwer, d. h. erst nach sorgfältigen Evaluationen durch Codereview und Tests, beurteilen können. Daher ist dieses Kriterium in Bezug auf Laien noch um einiges problematischer umzusetzen bzw. auf einer anderen Ebene anzusetzen. Beispielsweise ist es einem Laien schwer zumutbar, dass er öffentliche Schlüssel selbst überprüft, wohingegen eine zentrale CA, die die Beglaubigung von Schlüsseln

[29] Secure / Multipurpose Internet Mail Extensions.
[30] Z. B. die immer wieder aufflammende Debatte um die Sicherheit von SSL, vgl. z. B. *Schneier*, FREAK: Security Rollback Attack Against SSL vom 6.3.2015, URL: https://www.schneier.com/blog/archives/2015/03/freak_security_.html [26.2.2016].

übernimmt, eine große Erleichterung im Sinne der Bedienbarkeit ist.[31] Vertrauen auf eine sichere Software bedeutet daher, dass Nutzer wissen können müssen, ob sie getestet wurde, ob der Anbieter einen guten Ruf hat usw. Diese Evaluation hingegen liegt in der Verantwortung der Softwareentwickler und -anbieter.

Die heutigen Anforderungen an das Know How der Nutzer gestalten sich zusammenfassend also wie folgt: Nutzer müssen wissen oder zumindest ein mentales Konzept davon haben, wie das Internet und wie E-Mail funktionieren sowie den Zusammenhang zwischen Privatsphäre und Verschlüsselung kennen. Sie müssen die unterschiedlichen Vertrauensmodelle und den Begriff der PKI kennen. Sie müssen wissen, was ein Zertifikat und ein Schlüsselpaar ist und wie man es erzeugt (und unter Umständen wissen, dass Schlüsselpaare bei asymmetrischer Verschlüsselung Verwendung finden). Sie müssen den öffentlichen Schlüssel propagieren, darauf achten, den privaten Schlüssel nicht zu propagieren, an den öffentlichen Schlüssel des Kommunikationspartners kommen, den Unterschied zwischen Verschlüsseln und Signieren kennen und schließlich auch ihre E-Mails verschlüsseln bzw. entschlüsseln oder signieren.

---

[31] Über die Vor- und Nachteile der verschiedenen Vertrauensmodelle vgl. z. B. *Perlman*, An overview of PKI trust models, Network, IEEE 13.6 (1999): 38-43, URL:
http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.362.7257&rep=rep1&type=pdf (26.2.2016) oder *Ellison*/*Schneier*, Ten Risks of PKI: What You're not Being Told about Public Key Infrastructure, in: Computer Security Journal, Volume XVI, Number 1, 2000,
URL: https://www.schneier.com/cryptography/paperfiles/paper-pki.pdf [26.2.2016].

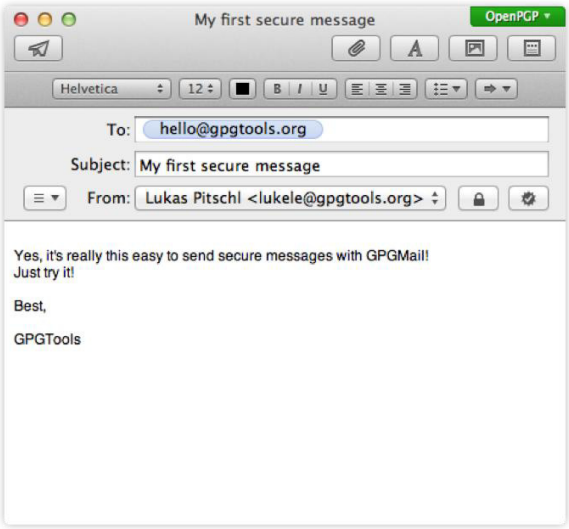

Abb. 1: E-Mailoberfläche mit installierter Verschlüsselungs- und Signierungssoftware PGPTools

Da diese Kompetenzen kaum von nicht Informatik-affinen Nutzern zu erwarten sind, stellt sich die Frage, wie man solche Systeme nutzerfreundlicher gestalten kann. Dabei gibt es nur wenige Kriterien zu erfüllen, die es jedoch dann konkret zu implementieren gilt: E-Mailverschlüsselungssoftware sollte Sicherheitsstandards erfüllen und es Nutzern erlauben, sicher und einfach zu kommunizieren. Zu den Sicherheitsstandards gehören neben der Vertraulichkeit und Integrität einer Nachricht, also dass sie weder durch Unberechtigte gelesen noch manipuliert werden kann, auch, dass der Empfänger die Authentizität des Senders nachvollziehen und überprüfen kann. Doch die bisherigen Ansätze in den verschiedenen Spielarten wie beispielsweise GPGTools[32] lassen Einfachheit vermissen. Insgesamt gibt es kein E-Mailsystem oder –anbieter, die es Nutzern erlauben, einfach und sicher zu kommunizieren.[33] Auch aktuelle Projekte wie

[32] https://gpgtools.org [26.2.2016].
[33] *Moecke/Volkamer*, Usable secure email communications: criteria and evaluation of existing approaches, in: Information Management & Computer Security, Volume 21 Issue 1, 2013, S. 41.

die sogenannte Volksverschlüsselung bleiben die Einlösung dieser Versprechen noch schuldig.[34]

3.2 Konzepte und Kompetenzen: Tor[35]

Als ein weiteres Beispiel zur Illustration, wie tiefgehend Nutzerkenntnisse sein müssen, soll Tor dienen. Tor ist ein Netzwerk, über das man Verbindungsdaten im Internet anonymisieren kann. Mit Hilfsprogrammen wie dem Tor-Browser ist es möglich, Zugang ins Internet über das Tor-Netzwerk zu erhalten. Der Tor-Browser ist einfach herunterzuladen und zu bedienen, denn mit der oberflächlichen Funktionsweise von Browsern sind Internetnutzer weitestgehend vertraut. Allerdings täuscht diese Einfachheit hier über die Konzepte, die Nutzer kennen müssen, um sich wirklich anonym im Netz bewegen zu können. Auf der Tor-Webseite findet man zusätzliche Hinweise dafür, was es zu beachten gilt, wenn man möchte, dass Tor funktioniert (und man tatsächlich anonym surft). Dazu gehören das Konzept der *Anonymität* selbst, auch hier wieder das Wissen um die Funktionsweise des Internets, IP-Adressen, das Konzept von *Paket-* und *Verkehrsanalyse* sowie *Browser Fingerprinting*.[36] Also obwohl die Entwickler von Tor mit der Verwendung eines Browsers den Nutzern entgegenkommen, bleiben die Nutzer auch hier nicht davon verschont, informatische Konzepte kennen zu müssen.

Sowohl die Konzepte bei Tor als auch die oben genannten notwendigen Fähigkeiten bei GPGTools gehen weit über das Alltagswissen der Durchschnittsnutzer hinaus. Teilweise handelt es sich um Wissen und Fähigkeiten, die Informatikstudierende in ihrem Studium lernen (sollen).

---

[34] *Fraunhofer SIT*, Volksverschlüsselung, Offene Initiative für Ende-zu-Ende-Sicherheit, URL: https://volksverschluesselung.sit.fraunhofer.de/index.php [26.2.2016].
[35] https://www.torproject.org
[36] https://www.torproject.org/download/download-easy.html.en [26.2.2015].

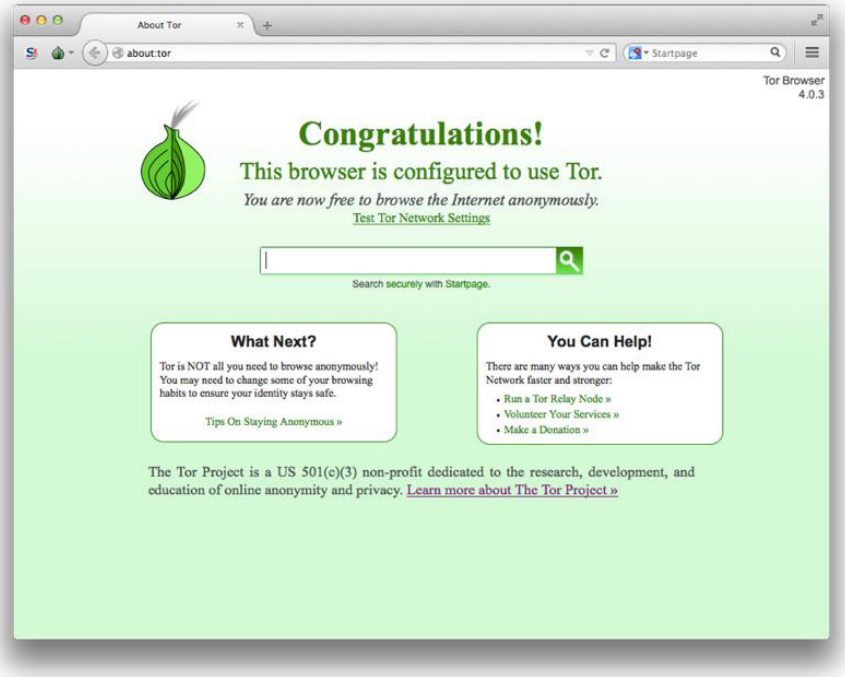

Abb. 2: Oberfläche des Tor-Browers

Werden aber informatische Kompetenzen von Nutzern implizit verlangt, ist es kaum verwunderlich, dass Selbstschutzmaßnahmen ins Leere laufen.

Insgesamt bleibt also festzuhalten, dass der Grundrechtsschutz durch Technik eine ganze Palette an Kompetenzen, Wissen um Konzepte und Motivation beim Nutzer voraussetzt. Neben den informatischen Aspekten sind zudem politische Kompetenz, juristische Kompetenz und auch Medienkompetenz ein Faktor in der Nutzung grundrechtsrelevanter Software.

Diesem Umstand kann man auf zwei Wegen begegnen. So ist die Aufklärung der Nutzer zum einen aber auch die Entwicklung entsprechender einfach zu bedienender Werkzeuge unabdingbar.[37] Dabei sind Informatiker gefragt, die nicht

[37] Vgl. *Hoffmann* et al., S. 50.

nur ihren Berufsethos ernst nehmen, sondern auch über den Tellerrand hinaus die gesellschaftlichen und rechtlichen Aspekte der Informatik einordnen können sollten. Auf Seiten der Nutzer sollte der Fokus auf die Stärkung der Mündigkeit der Nutzer gelegt werden, da sich sonst ein gewisser Paternalismus einschleicht und man versucht ist, die Nutzer vor sich selbst zu schützen.

4 Fazit

Die digitale Dimension der Grundrechte und der damit einhergehende Paradigmenwechsel kann nicht bestritten werden. Ob und inwieweit Grundrechte eigens für den digitalen Raum geschaffen werden, wird sich in der Diskussion in den kommenden Jahren zeigen. Zur Zeit jedoch ist die digitale Dimension ein Einfallstor für Grundrechtseingriffe von staatlicher, aber auch privater Seite. Technik schafft Fakten, und so ist das Internet ein grundrechtsdurchsetzungsfreier Raum. Damit bleibt der Schutz den Nutzern selbst überlassen. Doch die Nutzung von Software, die solche Selbstschutzmaßnahmen erlaubt, erfordert politisches Interesse, Motivation, juristische und informatische sowie Medienkompetenz. Und so bleibt: Nur, wer sich auskennt, kann seine Grundrechte im Internet ausüben und schützen. Soll sich das ändern, brauchen wir nicht nur neue rechtliche Rahmenbedingungen. Vielmehr müssen zum einen die Nutzer ihre Fähigkeiten erweitern zum anderen aber muss die Technik grundrechts- und nutzerfreundlich gestaltet werden.

Rechtsfragen der Robotik

Rechtlich gesehen: Der Roboter als softwaregesteuerte, bewegliche und zum Teil autonome Maschine

Thomas Söbbing

Das Thema Robotik ist in Deutschland kein Thema, welches in der rechtlichen Literatur große Präsenz genießt. Dies erscheint doch sehr unverständlich, da heute keine Fabrikation ohne Robtortechnik mehr vorstellbar und Robotik viel alltäglicher geworden ist, als noch vor einigen Jahren.

Wenn es um die rechtliche Betrachtung der Robotik geht, finden sich in der Literatur sehr viele Hinweise auf moralische oder philosophische Fragen. Dabei beschäftigen sich diese Betrachtungen häufig mit (rechtlichen) Fragen, die sich vielleicht in einer fernen Zukunft ergeben könnten, aber wenig mit den heutigen alltäglichen rechtlichen Fragen der Robotik zu tun haben.

Doch betrachtet man Roboter als das, was sie sind, nämlich softwaregesteuerte Maschinen, tauchen viele bekannte IT/IP-rechtliche Fragen auf, die sicherlich nichts mit dem Bereich alter Legenden oder Science Fiction zu tun haben. Ausgehend von der These, dass Roboter heute lediglich softwaregesteuerte Maschinen (ggf. mit dem Bestreben im begrenzten Bereich autonom zu handeln) sind, lassen sich daher trotz mangelnder rechtlicher Literatur zum Thema Robotik, einige rechtliche Antworten geben.

1 Einleitung und Definition

Im Jahre 2004 waren ca. zwei Millionen Roboter[1] im Einsatz.[2] Die deutsche Roboterbranche steigerte 2007 den Umatz um 13 Prozent.[3] Nach Schätzungen des Robotikverbandes International Federation of Robotics haben sich im Jahr 2010 die Verkäufe von Industrierobotern auf 120.000 Stück verdoppelt[4] und der Automobilkonzern General Motors plant den Test für erste unbemannte Pkw ab 2015 und die Serienproduktion ab 2018.[5] Aber bis zum vielseitig einsetzbaren Serviceroboter ist es noch ein weiter Weg,[6] dennoch zeigen viele Entwicklungen gerade in den USA und Japan,[7] wie eine Zukunft mit Robotern aussehen könnte. Dabei sind viele Entwicklungen real und keine Irritationen mehr aus der Welt alter Legenden[8] oder moderner Science Fiction Geschich-

---

[1] Der Ursprung des Wortes „Roboter" liegt im slawischen bzw. tschechischen Wort robota, das mit „Arbeit", „Frondienst" oder „Zwangsarbeit" übersetzt werden kann. Der Begriff robot wurde 1920 von Josef Čapek, einem bedeutenden Künstler geprägt, dessen Bruder Karel Čapek ursprünglich den Begriff labori verwendet hatte, als er 1921 in seinem Theaterstück R.U.R. in Tanks gezüchtete menschenähnliche künstliche Arbeiter beschrieb, die dafür geschaffen wurden, menschliche Arbeit zu übernehmen und dagegen revoltieren. *Tomáš Sedláček* Die Ökonomie von Gut und Böse, 1. Auflage 2012 S. 36.

[2] *Bill Gates*: Ein Roboter in jedem Haushalt bis 2013 - Elektronische Helfer werden immer kleiner und billiger, www.golem.de/0612/49631.html abgerufen am 18.09.2012.

[3] *Heise.de* Roboterbranche boomt: Deutsche Firmen rechnen mit starkem Wachstum vom 01.06.2008 11:25.

[4] *Produktion.de* Roboterbranche verdoppelt Verkäufe vom 14.02.2011 | Maschinenbau.

[5] *Spiegel online* Pläne des GM-Chefs: Autofahrer ab 2018 überflüssig vom 07.01.2008.

[6] *Marsiske* "Der lange Marsch" CT Magazin für Computertechnik Nr. 20 vom 10.9.2012, S. 96.

[7] Z. B. ASIMO, ein von Honda hergestellter Roboter der zurzeit als der fortschrittlichste Roboter der Erde gilt, siehe www.world.honda.com/ASIMO.

[8] Gemeint ist die Geschichte vom Golem**,** eine Figur der jüdischen Legende, die in Böhmen und in Mitteleuropa verbreitet war. Dabei handelt es sich um ein in menschenähnlicher Gestalt aus Lehm gebildetes Wesen, das durch Magie zum

ten.[9] Heute finden sich Roboter in vielen Bereichen des Wirtschafts-, Militär-Medizin- und Privatleben wieder. Der Begriff „Roboter" beschreibt sehr unterschiedliche Maschinen, weshalb man Roboter in viele Kategorien einordnet. Einige davon sind:[10]

- autonomer mobile Roboter
- Beam
- Erkundungsroboter
- humanoider Roboter
- Industrieroboter
- Laufroboter
- Personal Robot
- Portalroboter
- Serviceroboter
- Spielzeugroboter
- Transportroboter

Bei der Definition von Robotern finden sich neben der Sciene Fiction geprägten Literatur auch seriöse Quellen. Eine seriöse Definition von Robotern findet so z. B. in der VDI Richtlinie 2860. Danach sind Industrieroboter: universell einsetzbare Bewegungsautomaten mit mehreren Achsen, deren Bewegungen hinsichtlich Bewegungsfolge und Wegen bzw. Winkeln programmierbar und gegebenenfalls sensorgeführt sind. Legt man die Definition des Robot Institute of America (RIA) zugrunde, ist *ein Roboter ein programmierbares Mehrzweck-Handhabungsgerät für das Bewegen von Material, Werkstücken oder Spezialgeräten*.[11] Weiter ist Definition der Japan Robot Association: Sie umfasst Maschinen von Handlungsgeräten, die kein Programm haben, sondern direkt vom

---

Leben erweckt wurde. Der Golem besitzt besondere Kräfte, kann Befehlen folgen, aber nicht sprechen, siehe z. B. *Holitscher,* Der Golem 1. Auflage 1908.

[9] Z. B. in populären Filmen wie Star Wars (R2D2) von George Lucas, I, Robot (NS 5 – Sonny) von Alex Proyas, Star Trek Next Generation (Mr. Data) von Gene Roddenberry, Terminator (T-800 Modell 101) von James Cameron, etc. siehe *Ruge, Marotzki, Fromme,* Roboter im Film, 1., Aufl. 2012. S. 1 – 3.

[10] Online-Enzyklopädie Wikipedia (*http://de.wikipedia.org*) Stichwort "Roboter" Zugriff 25.10.2012 – 21.27h.

[11] Siehe auch *Beck*, Grundlegende Fragen zum rechtlichen Umgang mit der Robotik, JR 2009, 225, 230 (226).

Bediener geführt werden bis zu "Intelligent Robots", Geräten die über verschiedene Sensoren verfügen und damit in der Lage sind, den Programmablauf selbsttätig den Veränderungen der Umwelt anzupassen.[12] Zusammenfassend haben diese Definitionen gemeinsam, dass ein Programm (Software) eine bewegliche Maschine steuert. Neigt man zur Simplifizierung, so könnte man zur der einfachen Definition kommen, dass Roboter lediglich "*bewegliche, von Software gesteuerte, Maschinen*" sind.

Ein Unterschied zwischen Robotern und konventionellen Maschinen, die heute alle grundsätzlich von Software gesteuert sind (sog. Embedded Software[13]), besteht darin, dass Roboter möglichst autonom in einem begrenzten Bereich handeln sollen. Inwieweit die Technik heute schon bereit da-zu ist, kann sehr unterschiedlich eingeschätzt werden. Erkennbar ist aber sicherlich, dass das Autonomiebestreben in der Robotik zu nehmen wird. Dabei ist aber sicherlich nicht dran gedacht, menschenähnliche Lebewesen zu erschaffen, sondern viel mehr auch komplexe Prozesse von Menschen auf Roboter zu verlagern. Ein Beispiel hierfür sind die Bestrebungen, Fahrzeuge völlig selbständig fahren zu lassen (sog. autonomes Fahrzeug). Als autonomes Fahrzeug bezeichnet man dabei ein Fahrzeug, das frei (also ohne menschliche Unterstützung) navigiert.[14] Hierbei entscheidet das Auto (als Roboter) autonom, wie es sein Fahrverhalten (Lenkung, Geschwindigkeit, etc.) an die Umgebung anpasst.[15] Roboter nehmen dabei sensorisch ihre Umwelt war und reagieren entsprechend ihrer Programmierung. Eine gewisse Lernfähigkeit, die zu einer Erweiterungen der Möglichkeiten führt, ist sicherlich dabei nicht ausgeschlossen, sondern wünschenswert. Hierbei kann sicherlich schon von Ansätzen einer künstlichen Intelligenz (KI)

---

[12] *Christaller / Vollmer,* Autonome Maschinen 1. Auflage 2003 S. 46 ff.
[13] *Marly:* Praxishandbuch Softwarerecht 5. Auflage 2009, Rn. 80.
[14] *Hägele/Schäfer*: Definitionen. In: Hans-Jürgen Gevatter, Ulrich Grünhaupz (Hrsg.): Handbuch der Mess- und Automatisierungstechnik in der Produktion. 1. Auflage 2006.
[15] *Kirsch:* "Fahrerloses Auto bewältigt Berliner Innenstadt", CT Magazin für Computertechnik Nr. 22, 2011, S. 43.

und mehr gesprochen werden. Die Robotik beschäftigt sich dabei mit einer sog. manipulativen Intelligenz: Mit Hilfe von Robotern können gefährliche Tätigkeiten oder auch immer gleiche Manipulationen, wie das Entschärfen von Bomben auf Roboter verlagert werden. Der Grundgedanke ist es, Systeme (Roboter) zu schaffen, die intelligente Verhaltensweisen von Lebewesen nachvollziehen können. Daher muss die oben aufgestellte Definition um einem "Autonomen Ansatz" erweitert werden. Danach wären Roboter "*bewegliche, von Software gesteuerte, Maschinen mit dem Bestreben, in einem begrenzten Bereich autonom zu handeln.*"

Sucht man nach speziell zur Robotik geschriebener Rechtsliteratur, so wird man nur wenig finden.[16] Dies mag vielleicht an der Mystifizierung des Themas liegen, aber auch an der schwer zufassenden Definition. Entscheidet man sich dafür, dass ein Roboter eine Maschine ist, die von einer Software gesteuert wird (ggf. mit Autonomiebestreben), führt dies im Ergebnis zu bekannten IT-rechtlichen Fragen, wie Produkt-haftungsgesetz, Patentierung / Embedded Software und Nutzungsrechten.

[16] Eine der wenigen Ausnahmen: Beck, Grundlegende Fragen zum rechtlichen Umgang mit der Robotik JR 2009, 225, 230 (226).

2 Embedded System

Ein eingebettetes System (engl. *Embedded System*) ist ein binärwertiges digitales System (Computersystem), das in ein umgebendes technisches System eingebettet ist und mit diesem in Wechselwirkung steht.[17] Dabei hat das Computersystem die Aufgabe, das System, in das es eingebettet ist, zu steuern, zu regeln oder zu überwachen.[18] Zweifelsohne lassen sich die meisten in Abschnitt 1 definierten Robotersysteme unter diese Definition subsumieren.

Ein Embedded System besteht immer auch aus sog. Embedded Software. Ohne diese Embedded Software wäre ein Roboter sicherlich nicht zu verwenden, was aber natürlich auch für die meisten (intelligenten) Maschinen von der Waschmaschine bis hin zu komplexen Fertigungsstraßen oder Großflugzeugen gilt. Bereits vor der EuGH Entscheidung[19] zur Weiteräußerung von Gebrauchtsoftware wurde im TRIPS[20] Abkommen und WIPO Urheberrechtsvertrag (WCT)[21] festgelegt, dass Hardware mit Embedded Software frei gehandelt werden darf.[22] Es besteht zudem auch Einigkeit darüber, dass Embedded Software auch nicht als wesentliche Elemente einer Vermietung zu zählen und somit für Vermietung von Hardware (z.B. Roboter), die von einer Embedded Software

---

[17] Online-Enzyklopädie Wikipedia (*http://de.wikipedia.org*) Stichwort "Eingebettetes System" Zugriff 21.10.2012 – 18.21h.

[18] *Balzert*: Lehrbuch der Software-Technik. Band 1: *Software-Entwicklung.* Spektrum Akademischer Verlag, Heidelberg 1996, 1998, 2001

[19] EuGH, 03.07.2012 - C-128/11 = NJW 2012, 2565; ZIP 2012, 1610; GRUR 2012, 904; EuZW 2012, 658; MMR 2012, 586.

[20] Agreement on Trade-Related Aspects of intellectual Property Rights ("TRIPs"), ABl. EG Nr. L 336 v. 23.12.1994. TRIPs ist selbst keine eigenständiger völkerrechtlicher Vertrag, sondern integraler Bestandteil des WTO, Art. II 2 Übereinkommen zur Errichtung der Welthandelsorganisation (WTO), ABl. EG Nr. L336 v. 23.12.1994, 3.

[21] WIPO Copyright Treaty (WCT"), Beschluss des Rates vom 16.03.2000, ABl. EG Nr. L 89 v. 11.4.2000, 6.

[22] *Vander,* CR 2011, 77 (78-79): Gilt auch für das Recht zur Vermietung.

gesteuert wird, kein Vermietrecht in Sinne von § 69 c Abs. 3 UrhG explizit übertragen werden muss,[23] auch wenn einige Autoren auf eine Einzelfallbetrachtung verweisen.[24] Im Ergebnis bleibt daher festzuhalten, dass Roboter veräußert und vermietet werden dürfen, ohne dass es zusätzlicher Rechte bedarf.

[23] *Gervais*, The Trips Agreement, Art. 11 Rn. 2.65; *Klopmeier* in Busche/Stoll, TRIPs Agreement, 1. Auflage 2007, Art. 11 Rn. 11; *Duggal*, Trips-Übereinkommen und Internationalen Urheberrecht, 2001 S. 73; *Rehbinder/Staehelin*, UFITA 127 (1995), 5 (20); *Senfleben* in Dreier/Hugenholtz Concise European Copyright Law, 2006, Art. 7 WCT, S. 101; *Hoeren* in Möhring/Nicolini, UrhG, 2. Auflage 2000, § 69c Rn. 20; *Grützmacher* in Wandtke/Bullinger, UrhR, 3. Auflage 2009, § 69 c Rn. 48; *Katzenberger* in Beier/Schricker, From GATT to TRIPS, 1996, S. 59, 88.

[24] *Klopmeiner* in Busche/Stoll, TRIPs, 1. Auflage 2007, Art. 11 Rn. 11; *Grützmacher* in Wandtke/Bullinger, UrhR, 3. Auflage 2009, § 69 c Rn. 48;

3 Patentierung

Bereits im Jahre 1954 ließen sich die beiden US-Amerikaner George Devol und Joe Engelberger den ersten industriell einsetzbaren Roboter patentieren. Der tonnenschwere „Unimate“, der hauptsächlich aus einem beweglichen, stählernen Arm bestand, konnte Objekte von einem Ort zum anderen bewegen und schweißen.[25]

Die technische Erfindung eines Roboters oder Teile eines Roboters lassen sich durch eine Patentierung schützen, wenn man unterstellt, dass es sich bei Robotern um *bewegliche, von Software gesteuerte, Maschinen* handelt.[26]

In Deutschland lassen sich Patente durch das Patentgesetz (PatG) schützen, in der EU schützt das Europäische Patentübereinkommen (EPÜ) Patente. Das PatG definiert im ersten Abschnitt (§§ 1 – 25 PatG) ein Patent. Gem. § 1 Abs. 1 PatG werden Patente für Erfindungen auf allen Gebieten der Technik erteilt, sofern sie neu sind, auf einer erfinderischen Tätigkeit beruhen und gewerblich anwendbar sind.

Nach § 3 Abs. 1 PatG und Art. 54 EPÜ gilt eine Erfindung als neu, wenn sie nicht zum Stand der Technik gehört. Der Stand der Technik umfasst alle Kenntnisse, die vor dem für den Zeitrang der Anmeldung maßgeblichen Tag durch schriftliche oder mündliche Beschreibung, durch Benutzung oder in sonstiger Weise der Öffentlichkeit zugänglich gemacht worden sind; vgl. § 3 Abs. 1 S. 2 PatG. Bei Robotern muss also der Patentanmelder darlegen, dass sein Roboter neue

---

[25] *Dorf/Kusiak* Handbook of Design, Manufacturing and Automation 1994 S. 260.

[26] Z. B. Prof. Dr. Wolfgang Echelmeyer Erfindung: Roboter und Vorrichtung zum Be- und/oder Entladen von Stückgütern und Vorrichtung zum Ein- und Auslagern von Stückgütern mit denselben (Portalroboter D 10463); Anmeldung als deutsches Patent 102005047644.9-15 am 23.09.05; Patent erteilt.

Funktionen hat, welche nicht zum Stand der Technik gehören (z.B. zur Lauffähigkeit von Robotern).

Des Weiteren muss es sich um eine Erfindung handeln. Patentierbare Erfindungen sind technische Lehren zum planmäßigen Handeln, die einen kausal übersehbaren Erfolg unter Einsatz beherrschbarer Naturkräfte ohne Zwischenschaltung verstandesmäßiger Tätigkeiten reproduzierbar herbeiführen.[27] Eine technische Weiterentwicklung eines Roboters ist nur dann eine patentierbare Erfindung, wenn sie sich für „den durchschnittlichen Fachmann, der den gesamten Stand der Technik kennt" (eine Rechtsfiktion, keine reale Person), nicht in naheliegender Weise aus dem Stand der Technik ergibt, vgl. § 4 S. 1 PatG, Art. 56 S. 1 EPÜ. D. h., es fehlt an Erfindungshöhe, wenn man von diesem Fachmann erwarten kann, dass er, ausgehend vom Stand der Technik auf diese Lösung alsbald und mit einem zumutbaren Aufwand gekommen wäre, ohne erfinderisch tätig zu werden.[28] Im Bereich der Robotik sind somit nur Erfindungen patentierbar, die einen deutlichen Fortschritt in der Entwicklung von Robotertechnologien darstellen. Dies muss sich aber nicht auf den Roboter als Ganzes beziehen, sondern kann sich auch auf einzelne Komponenten, wie ein Roboterarm oder eine Funktionsweise zur Fortbewegung beziehen.

Zudem muss die Erfindung gem. § 5 Abs. 1 PatG, Art. 57 EPÜ auf irgendeinem gewerblichen Gebiet anwendbar sein. Dabei wird der Begriff der gewerblichen Anwendbarkeit vom Europäischen Patentamt weit ausgelegt und ist in der Praxis von untergeordneter Bedeutung. Ausreichend ist es, dass die Erfindung in einem technischen Gewerbebetrieb hergestellt oder sonst verwendet werden

[27] BGH, 27.03.1969 - X ZB 15/67 = BGHZ 52, 74; NJW 1969, 1713; GRUR 1969, 672.

[28] Dieses Kriterium ist nach der Rechtsprechung des Bundespatentgerichts, des BGH und der technischen Beschwerdekammern des Europäischen Patentamts rein objektiv zu verstehen. Es spielt keine Rolle, wie die zu beurteilende Erfindung tatsächlich gemacht worden ist und ob sie subjektiv für den Erfinder eine besondere Leistung bedeutet hat; *Osterrieth* Patentrecht 4. Auflage 2010, Rn. 421.

kann. Es kommt auch nicht darauf an, ob man mit der Vorrichtung oder dem Verfahren „Geld machen“ kann, maßgebend ist allein, dass der beanspruchte Gegenstand außerhalb der Privatsphäre verwendet werden kann. Die meisten Erfindungen im Bereich der Robotik sind auf einem kommerziellen Erfolg ausgerichtet, sei es z. B. bei der Erschaffung von Haushaltshilfen oder Roboter für Operationen. Dies liegt schon in der Natur der Sache, da die Erfindung von Robotertechnologien ernorme Investitionen verlangen und diese von den Investitionsgebern mit Gewinn zurückgefordert werden.

Die maximale Laufzeit eines Patents beträgt gem. § 16 PatG und Art. 63 Abs. 1 EPÜ 20 Jahre ab dem Tag nach der Anmeldung. Gemäß § 16a PatG, Art. 63 Abs. 2 b) EPÜ i. V. m. VO (EWG) Nr. 1768/92 kann allerdings für Erfindungen, die erst nach aufwändigen Zulassungsverfahren wirtschaftlich verwertet werden können, ein ergänzendes Schutzzertifikat erteilt werden, das die Patentlaufzeit dann um maximal fünf Jahre verlängert. Durch die langen Entwicklungszyklen in der Robotik sollte dies regelmäßig Anwendung finden.

Nach § 1 Abs. 2 und 3 PatG und Art. 52 Abs. 2 und 3 EPÜ können wissenschaftliche Theorien und mathematische Methoden, wie Baupläne für einen Roboter nicht als Patent geschützt werden. Das gleiche gilt für Design und Erscheinungsbild eines Roboters, da ästhetische Formschöpfungen nicht patentrechtlich geschützt werden können.

4 Haftungsfragen

Ein Fehlverhalten eines Roboters, stammt es nun dem Autonomiebestreben oder aus einem sonstigen Grund, zieht immer eine Reihe von Haftungsfragen nach sich. Diese können sich zum einem aus einer vertraglichen Pflichtverletzung gem. § 280 Abs. 1 BGB, zu, anderem dem Deliktsrecht nach § 823 BGB gegenüber fremden Dritten oder auch aus dem Produkthaftungsgesetz ergeben.

4.1 Pflichtverletzungen

Wird ein Roboter im Rahmen eines Vertragsverhältnis (z. B. Miete) bei einer anderen Vertragspartei tätig und erzeugt der Roboter dabei Schäden bei dieser Partei, so stellt dies sicherlich eine Pflichtverletzung i.S.v. § 280 BGB dar. Ein durch die Medien bekannt gewordener Fall ist die Verwendung des ROBODOC von Integrated Surgical System, welches zu zahlreichen Schadensersatzforderungen geführt hat.[29]

Gem. § 249 S.1 BGB hat der Schuldner, der zum Schadensersatz verpflichtet ist, den Zustand herzustellen, der bestehen würde, wenn der zum Ersatz verpflichtende Umstand nicht eingetreten wäre. Dabei soll der Schädiger allen Schaden ersetzen, der durch das zum Ersatz verpflichtende Ergebnis eingetreten ist (sog. Totalreparation).[30] Außer der Regel der Totalreparation wird in § 249 S. 1 BGB noch ein weiterer Grundsatz des Schadensrechts ausgedrückt, nämlich das Prinzip Herstellung oder des Naturalersatzes (sog. Natural-restitution). Hierbei soll der Schädiger den Zustand in Geld herstellen, der ohne das Schadensereignis bestünde.

[29] BGH, 13.06.2006 - VI ZR 323/04 = BGHZ 168, 103; NJW 2006, 2477; MDR 2007, 153; VersR 2006, 1073; JR 2007, 191.
[30] Brox Schuldrecht AT Rn. 585.

4.2 Abgrenzungsfragen

Eine in der Zukunft sicherlich immer wichtigere Frage wird sein, wer für die von einem Roboter auf Basis Künstlicher Intelligenz (KI) gefällte Entscheidung haftet. So ist sicherlich zu vertreten, dass derjenige haften muss, der die Roboter verwendet, da er für die Verkehrssicherheit des eingesetzten Roboters haftet und für entsprechende Sicherungsmaßnahmen sorgen muss. In einem vertraglichen Verhältnis ergeben sich diese sicherlich aus dem allgemeinen Sorgfaltspflichten des Schuldverhältnis, vgl. § 280 Abs. 1 BGB, gegenüber Dritten sicherlich aus dem Deliktsrecht, §§ 823 ff BGB.

Grundsätzlich könnte der Hersteller nach dem Produkthaftungsgesetz (ProdHaftG)[31] haften. Voraussetzung der Produkthaftung ist gemäß § 1 Abs. 1 S. 1. ProdHaftG ist u.a., dass ein Fehler der schadensursächlichen Sache vorlag (sprich im Roboter). Ein solcher Fehler könnte ggf. vorliegen, wenn der Hersteller keine geeigneten Sicherheitsmaßnahmen in der Programmierung der Steuerungssoftware des Roboters eingebaut hat. Der Hersteller haftet jedenfalls nicht, wenn der Roboter den schadenursächlichen Fehler zum Zeitpunkt des In-Verkehr-Bringens noch nicht aufwies[32] und wenn der Fehler nach dem Stand der Wissenschaft und Technik in dem Zeitpunkt, in dem der Hersteller das Produkt in den Verkehr brachte, nicht erkannt werden konnte, vgl. § 1 Abs. 2 Nr. 5 ProdHaftG. Dennoch muss der Hersteller von Robotern Sicherungsmaßnahmen in einen Roboter (und vor allem in der Software) einbauen, so dass keine Schäden, selbst nach einem KI-Lernprozess erfolgen können. In der Science Fiction Literatur wurden z. B. hierzu von Isaac Asimov die drei Gesetze der Robotik entwickelt (siehe Fazit).[33] Ob solche eher philosophischen Gesetze ausreichend sind, lässt sich heute noch nicht beurteilen, sicher ist aber, dass

---

[31] ProdHaftG vom 15. Dezember 1989, siehe BGBl. I S. 2198.
[32] Palandt *Sprau* Kommentar zum BGB 69. Auflage 2009 § 1 ProdHaftG Rn. 17.
[33] *Asimov* Alle Roboter-Geschichten 3. Auflage 2011, Kurzgeschichte Herumtreiber (engl. Runaround) S. 276 – 295 (S. 291).

dem Hersteller und Entwickler von Robotern eine entsprechende Pflicht zur Verkehrssicherheit trifft. Die Aufrechterhaltung dieser Verkehrssicherungspflichten trifft dann aber nicht mehr den Hersteller, sondern den Halter bzw. Eigentümer des Roboters. Hier finden die Grundsätze zum Umgang mit gefährlichen Sachen Anwendung. Als eine gefährliche Sache wird z. B. ein KFZ gesehen, von dem eine gewisse Betriebsgefahr ausgeht. Der Hersteller produziert ein Auto, welches die entsprechenden Anforderungen zur Zulassung eines KFZ erfüllt, während der Halter dafür sorgen muss, dass sich das Fahrzeug ständig in verkehrssicherem Zustand befindet.[34] Insbesondere gilt dies bei einer Garantenstellung gegenüber Dritten.[35] Gleiches sollte auch für die Herstellung und Verwendung von Roboter Anwendung finden.

Der Hersteller haftet auch für Entwicklungsfehler. Ein Entwicklungsfehler liegt aber nur dann vor, wenn er zum Zeitpunkt, in dem der Hersteller den Roboter in Verkehr brachte, nach dem Stand der Wissenschaft und Technik noch nicht erkannt werden konnte.[36] Der Haftungssausschluss betrifft aber nur Konstruktions- nicht aber Fabrikationsfehler.[37] Der Fehler ist nicht erkennbar, wenn die potenzielle Gefährlichkeit des Roboters nach der Summe an Wissen und Technik, die allgemein nur in der betroffenen Branche und national, anerkannt ist und zur Verfügung steht und von niemandem erkannt werden konnte, weil diese Erkennungsmöglichkeiten noch nicht vorhanden war.[38]

Die Haftung für die Beschädigung von Sachen ist im Pro-dukthaftungsgesetz begrenzt auf andere Sachen als das fehlerhafte Produkt, welche zum privaten Ge- oder Verbrauch bestimmt waren und hierzu vom Geschädigten hauptsäch-

[34] BGH, 14.10.1997 - VI ZR 404/96 = NJW 1998, 311; MDR 1998, 41; NZV 1998, 23; VersR 1998, 120.
[35] BGH, 24.04.1979 - VI ZR 73/78 = NJW 1979, 2309; VersR 1979, 766.
[36] Palandt *Sprau* Kommentar zum BGB 69. Auflage 2009 § 1 ProdHaftG Rn. 21.
[37] BGH, 09.05.1995 - VI ZR 158/94 = BGHZ 129, 353; NJW 1995, 2162; NJW 1995, 2161; ZIP 1995, 1094; MDR 1995, 1124; VersR 1995, 924; WM 1995, 1317; BB 1995, 1431; DB 1995, 1504.
[38] Palandt *Sprau* Kommentar zum BGB 69. Auflage 2009 § 1 ProdHaftG Rn. 21.

lich verwendet wurden.[39] Diese Formulierung schließt u.a. Schäden an Erzeugnissen im Rahmen einer geschäftlichen Tätigkeit aus.[40]

Eine wichtige Haftungsvoraussetzung ist in § 1 Abs. 2 Nr. 1 ProdHaftG geregelt. Danach ist die Haftung des Produzenten für den Fall ausgeschlossen, dass er das Produkt nicht in den Verkehr gebracht hat. Der Hersteller und auch der Quasihersteller, bringen ein Produkt in Verkehr, sobald er sich willentlich der tatsächlichen Herrschaftsgewalt über das Produkt begibt, z. B. dadurch dass er es ausliefert, in den Vertrieb, in die Verteilerkette oder in den Wirtschaftskreislauf gibt.[41]

Schwierig wird sicherlich die Frage der Abgrenzung der Haftung zwischen dem Hersteller eines Roboters und dem Verwenders eines Roboters, insbesondere dann, wenn sich der Roboter und seine Embedded Software durch KI-Prozesse autonom weiterentwickelt haben. Zur Absicherung des Geschädigten könnte man dann auf den Gedanken, dass Hersteller und Verwender des Roboters als Gesamtschuldner haften.

---

[39] Palandt *Sprau* Kommentar zum BGB 69. Auflage 2009 § 1 ProdHaftG Rn. 7.
[40] Eisenberg/Gildeggen/Reuter/Willburger: Produkthaftung. 1. Auflage. München 2008, § 1 Rn. 5.
[41] EuGH, 09.02.2006 - C-127/04 = Slg. 2006, I-1313; NJW 2006, 825; EuZW 2006, 184; NZV 2006, 243.

5 Fazit

Ausgehend von der Definition, dass Roboter softwaregesteuerte Maschinen (ggf. mit dem Bestreben weitgehend autonom zu handeln) sind, lassen sich viele rechtliche Antworten aus bekannten anderen Rechtsbereichen (Patentrecht, Haftungsrecht, etc.) ableiten. Mit dieser einfachen, aber stimmigen Definition werden Roboter zwar das mystische abgesprochen, aber es ermöglicht eine sachliche Umgangsweise mit der rechtlichen Seite der Robotik.

Wagt man dennoch einen Blick in die Zukunft und in eine Welt, in der Roboter mit einer künstlichen Intelligent ausstanden sind, kommt man natürlich nicht ohne den Hinweis auf die drei (philosophischen) Gesetze von Isaac Asimov aus. Dabei besagen die drei Gesetze:[42]

1. Ein Roboter darf keinen Menschen verletzen oder durch Untätigkeit zu Schaden kommen lassen.

2. Ein Roboter muss den Befehlen eines Menschen gehorchen, es sei denn, solche Befehle stehen im Widerspruch zum ersten Gesetz.

3. Ein Roboter muss seine eigene Existenz schützen, solange dieser Schutz nicht dem Ersten oder Zweiten Gesetz widerspricht.

In der Literatur[43] und im Film[44] führte die Anwendung dieser Gesetze zu irrationalen Handlungen und zu Katastrophen, da sie ohne Auslegung oder Ermessenspielraum umgesetzt wurden. Dies erscheint doch für uns Juristen doch sehr

[42] *Asimov* Alle Roboter-Geschichten 3. Auflage 2011, Kurzgeschichte Herumtreiber (engl. Runaround) S. 276 – 295 (S. 291).
[43] *Asimov* Alle Roboter-Geschichten 3. Auflage 2011, Kurzgeschichte Herumtreiber (engl. Runaround) S. 276 – 295.
[44] Z.B. im Film "I, Robot" von Alex Proyas aus dem Jahre 2004.

erfreulich zu klingen, da es zeigt, dass die berufliche Tätigkeit des Juristen nicht durch Roboter oder Maschinen ersetzt werden kann.

Hinweis: Dieser Beitrag erschien zuerst in InTeR 2013, 13 ff. und wird hier mit freundlicher Genehmigung des dfv Deutscher Fachverlag GmbH genutzt.

Autorenhinweise

Dr. Till Kreutzer (geb. 1971) ist Rechtsanwalt, Publizist und Rechtswissenschaftler. Er ist Gründungsmitglied und Redaktionsleiter von iRights.info. Er ist Partner des Think Tanks iRights.Lab und der Rechtsanwaltskanzlei iRights.Law. Till Kreutzer ist „ad personam" Mitglied der Deutschen UNESCO-Kommission und assoziiertes Mitglied des Forschungsbereichs Medien- und Telekommunikationsrecht am Hans-Bredow-Institut für Medienforschung an der Universität Hamburg sowie Mitglied des "Instituts für Rechtsfragen der Freien und Open Source Software"(ifrOSS). Seine Promotion hat er über das Thema: „Das deutsche Urheberrecht und Regelungsalternativen" verfasst.

Dr. Simon Assion ist Rechtsanwalt bei Bird&Bird LLP in Frankfurt a.M und Lehrbeauftragter für Europäisches Medienrecht an der FH St. Pölten. Er berät IT-, Medien- und Telekommunikationsunternehmen, oft in Zusammenhang mit der Entwicklung und Markteinführung von neu entwickelten Produkten. Simon Assion ist außerdem einer der Gründer und Herausgeber von Telemedicus. Vor seiner Tätigkeit als Rechtsanwalt war er Juristischer Referent beim Mitteldeutschen Rundfunk, wo er u.a. für die Kabelverbreitung der ARD-Rundfunkprogramme zuständig war. Studium in Augsburg, Münster und Speyer, Promotion am Hans Bredow-Institut in Hamburg.

Sven-Erik Heun ist Rechtsanwalt und Partner bei Bird&Bird LLP. Seit 2015 koordiniert er als Head of Country die Geschäfte in Deutschland und ist Mitglied in den internationalen Führungsgremien der Kanzlei. Sein Tätigkeitsspektrum beinhaltet die rechtliche, regulatorische und strategische Beratung in Projekten und Transaktionen, das Strukturieren und Verhandeln von Verträgen, Verfahren vor nationalen und europäischen Regulierungs- und Kartellbehörden sowie

kartell-, verwaltungs- und zivilgerichtliche Prozesse und Schiedsverfahren. Er ist Herausgeber und Mitautor des „Handbuch Telekommunikationsrecht“.

Prof. Dr. Kai von Lewinski ist seit Beginn des Sommersemesters 2014 Professor an der Juristischen Fakultät der Universität Passau. Zuvor war er Wissenschaftlicher Leiter der Stiftung Datenschutz und Lehrstuhlvertreter an verschiedenen Universitäten, darunter an der HU Berlin und am Karlsruhe Institut für Technologie (KIT); davor Rechtanwalt in einer internationalen Wirtschaftskanzlei mit Arbeitsschwerpunkten im Datenschutz- und Softwarelizenzrecht. Kai von Lewinski arbeitet u.a. zum Datenschutzrecht und zu Big Data.

RA Prof. Dr. Tina Krügel, LL.M. ist Rechtsanwältin für IT-Recht, Gesellschafterin der Firma lexICT UG, die sich auf die Stellung des externen Datenschutzbeauftragten spezialisiert hat, und seit April 2014 Juniorprofessorin für Informationsrecht, insbesondere Datenschutzrecht am Institut für Rechtsinformatik der Leibniz Universität Hannover. Sie hat den letzten Jahren an zahlreichen europäischen Forschungsprojekten im Bereich des Datenschutzes und der IT-Sicherheit mitgewirkt und viele Fachbeiträge insbesondere im Bereich des (europäischen) Datenschutzrechts veröffentlicht.

Dipl.-Inf. Dipl.-Jur. Agata Królikowski hat an der Humboldt-Universität zu Berlin Jura und Informatik studiert. Zur Zeit ist sie wissenschaftliche Mitarbeiterin am Innovations-Inkubator der Leuphana Universität Lüneburg und arbeitet dort in den Projekten Hybrid Publishing und Grundversorgung 2.0. Daneben ist sie Präsidiumsmitglied und Mitglied des erweiterten Vorstands der Gesellschaft für Informatik e.V. sowie Sprecherin der Fachgruppe Internet und Gesellschaft.

Dr. Thomas Söbbing ist seit 2011 als Chief Legal Specialist/Fachleiter Recht beim Markführer Deutsche Leasing tätig. Zuvor war er in leitenden und beratenden Positionen bei IBM, KPMG und Siemens, betreute u.a. den größten

Vertrag der Siemens AG und wurde 2014 von Legal 500 zu einem der Top 100 Corporate Counsel normiert. Daneben ist er Dozent an der German Graduate School, lehrte in Oxford/Cambridge und hat 6 Bücher sowie mehrere hundert internationale Publikationen veröffentlicht. Dr. Söbbing studierte Jura in Münster, war Mitarbeiter von Prof. Hoeren und hat den LLM der HHU mit einem Studienaufenthalt an der Univ. of Washington abgeschlossen. Ferner absolvierte er Programme in Harvard, Oxford, Shanghai und St. Gallen.

Wir danken den Sponsoren der Telemedicus Sommerkonferenz 2015: