ITeG | Interdisciplinary Research on Information System Design | 4

Alexander Roßnagel | Christian Geminn |
Silke Jandt | Philipp Richter

Datenschutzrecht 2016
„Smart“ genug für die Zukunft?
Ubiquitous Computing und Big Data als Herausforderungen des Datenschutzrechts

ITeG Research Center for Information System Design

kassel university press

ITeG – Interdisciplinary Research on Information System Design

Band 4 / Vol. 4

Herausgegeben von / Edited by
ITeG Wissenschaftliches Zentrum für Informationstechnik-Gestaltung
an der Universität Kassel

Universität Kassel
ITeG Wissenschaftliches Zentrum
für Informationstechnik-Gestaltung
Pfannkuchstraße 1
D-34121 Kassel

Alexander Roßnagel, Christian Geminn,
Silke Jandt, Philipp Richter

Datenschutzrecht 2016
„Smart“ genug für die Zukunft?

Ubiquitous Computing und Big Data als
Herausforderungen des Datenschutzrechts

kassel university press

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

ISBN 978-3-7376-0154-2 (print)
ISBN 978-3-7376-0155-9 (e-book)
DOI: http://dx.medra.org/10.19211/KUP9783737601559
URN: http://nbn-resolving.de/urn:nbn:de:0002-401558

www.upress.uni-kassel.de/

Printed in Germany

VORWORT

Das nationale und das europäische Datenschutzrecht stammen in ihren Grundzügen aus der Vor-Internetzeit. Das Bundesdatenschutzgesetz von 1977 und die Europäische Datenschutzrichtlinie von 1995 sind zu einer Zeit entstanden, als die wichtigsten Techniken und Geschäftsmodelle, die heute personenbezogene Daten erzeugen oder verarbeiten, noch nicht bekannt oder verbreitet waren. Seitdem wurde im Internet ein virtueller Raum geschaffen, der alle gesellschaftlichen Bereiche erfasst und in dem jede Lebensregung eine Spur hinterlässt. Diese Spuren auszuwerten und zu Profilen der Internetnutzer zusammenzuführen sowie diese für wirtschaftliche Zwecke zu nutzen, hat sich als hochattraktiv erwiesen und bildet die Grundlage dafür, dass viele Internetangebote ohne Geldzahlungen genutzt werden können. Bezahlt werden diese Angeboten mit den Daten der Nutzer.

Trotz der bereits erfolgten massiven Realitätsveränderungen und der in naher Zukunft zu erwartenden Umwälzungen im Umgang mit personenbezogenen Daten durch die genannten technischen und wirtschaftlichen Entwicklungen wurden das nationale und das europäische Datenschutzrecht seit ihrer Entstehung lediglich punktuell geändert und angepasst.

Vor diesem Hintergrund drängen sich die folgenden rechtlichen Fragestellungen auf:

Ist das aktuelle Datenschutzrecht und sind insbesondere die Datenschutzprinzipien geeignet, die Risiken für die informationelle Selbstbestimmung durch moderne Informationstechnologie angemessen zu reduzieren und das Datenschutzniveau zu erhalten? Besteht insbesondere ein ausreichender rechtlicher Schutz vor dem Risiko der umfassenden Erstellung von Nutzerprofilen?

Bestehen konkrete Regelungsdefizite im Hinblick auf die sich immer weiter verbreitenden „smarten" Alltagsprodukte, den Umgang mit

personenbezogenen Daten durch private Unternehmen und die neuen technischen Auswertungsmöglichkeiten?

Welche Anpassungen im nationalen und europäischen Datenschutzrecht sind erforderlich, um der informationellen Selbstbestimmung jedes Einzelnen größtmögliche Geltung zu verleihen? Welche konkreten Regelungen sollten getroffen werden, um das Erstellen von umfassenden Nutzerprofilen auf Basis der durch die smarten Informationstechniken erlangten Daten zu verhindern?

Wie sind die europäischen Rechtssetzungsaktivitäten für eine Datenschutz-Grundverordnung (DSGVO) in Bezug auf die beschriebenen Risiken und „smarte" Alltagsprodukte zu bewerten?

Diese Fragestellungen werden in dem vorliegenden Buch untersucht und beantwortet. Es ist folgendermaßen aufgebaut: Ausgehend von einer funktionalen Beschreibung der beispielhaft zu untersuchenden „smarten" Alltagstechniken und der Möglichkeiten von Big Data-Auswertungen mit und ohne Personenbezug werden die spezifischen Risiken für die informationelle Selbstbestimmung in Kapitel 1 herausgearbeitet. Dabei werden nicht nur technische Potentiale beschrieben, sondern auch die Motive und Handlungslogiken für die Verarbeitung personenbezogener Daten analysiert, die sich aus den praktizierten oder zukünftig möglichen Geschäftsmodellen ergeben.

Im zweiten Kapitel wird die erste Frage beantwortet, ob das geltende Datenschutzrecht geeignet ist, die Risiken für die informationelle Selbstbestimmung durch moderne Informationstechniken angemessen zu reduzieren und das Datenschutzniveau zu erhalten. Da bisher keine datenschutzrechtlichen Spezialvorschriften für Ubiquitous Computing-Anwendungen und Big Data-Analysen bestehen, werden vor allem die allgemeinen Erlaubnistatbestände für den Umgang mit personenbezogenen Daten durch Unternehmen sowie die tragenden Datenschutzprinzipien daraufhin untersucht, gegen welche Risiken sie Schutz gewähren und für welche Risiken sie überfordert sind. Dabei wird ein Schwerpunkt auf die Untersuchung gelegt, ob ein ausrei-

chender rechtlicher Schutz vor dem Risiko der umfassenden Erstellung von Nutzerprofilen besteht. Diese Untersuchungen beziehen sich im ersten Schritt auf allgemeine Merkmale von Ubiquitous Computing-Anwendungen und Big Data-Analysen. In einem zweiten Schritt erfolgt eine rechtsgutachterliche Bewertung der drei beispielhaften „smarten“ Informationstechniken für den Alltag und der beiden Big-Data-Anwendungen.

Im dritten Kapitel geht es um die zweite Frage, ob es konkrete Regelungsdefizite im Hinblick auf die sich immer weiter verbreitenden „smarten" Alltagsprodukte, den Umgang mit personenbezogenen Daten durch private Unternehmen und die neuen technischen Auswertungsmöglichkeiten gibt. Diese Frage wird auf der Grundlage der Erkenntnisse des Kapitels 2 zum einen dadurch beantwortet, dass die Regelungsdefizite für die allgemeinen Regelungen zu Zulassungstatbeständen und Datenschutzprinzipien zusammengestellt werden sowie danach gefragt wird, ob bereichsspezifische Regelungen fehlen. Zum anderen wird sie dadurch beantwortet, dass für die Beispiele Smart Car, Smart Home und Smart Health sowie für Big Data-Analysen konkrete Regelungsdefizite festgestellt werden.

Im vierten Kapitel wird untersucht, welche Anpassungen im nationalen und europäischen Datenschutzrecht erforderlich sind, um der informationellen Selbstbestimmung jedes Einzelnen größtmögliche Geltung zu verleihen. Hierzu wird für jedes der erkannten Regelungsdefizite ein konzeptioneller Regelungsvorschlag ausgearbeitet, der die Zielsetzung der informationellen Selbstbestimmung gewährleistet oder zumindest ihre Erreichung verbessert. Diese Untersuchung bezieht sich im ersten Schritt auf die Anpassung oder Ergänzung der Erlaubnistatbestände und der Datenschutzprinzipien. In einem zweiten Schritt werden konkrete Regelungskonzeptionen für die Beispiele Smart Car, Smart Home und E-Heath sowie für die Big Data-Anwendungen Profilbildung aus heterogenen Quellen und personenbezogene Verhaltensprognosen erarbeitet. Dabei wird ein Schwerpunkt auf der Kombination der Erzeugung von personenbezogenen Daten in

„smarten“ Alltagsprodukten und neuen Auswertungsmethoden liegen. Dadurch wird insbesondere die dritte Frage beantwortet, welche konkreten Regelungen getroffen werden sollten, um das Erstellen von umfassenden Nutzerprofilen auf Basis der durch die smarten Technologien erlangten Daten zu verhindern.

Schließlich befasst sich das fünfte Kapitel mit der neu erlassenen Datenschutz-Grundverordnung und bewertet diese daraufhin, ob und wie sie Schutz vor den erkannten Risiken „smarter“ Alltagsprodukte und neuer Auswertungsmethoden bietet. Da sie keine spezifischen Regelungen für diese Risiken enthält, bezieht sich die Untersuchung auf die Schutzwirkungen allgemeiner Vorschriften wie zu Zweckbindung und Erforderlichkeit, Transparenz und Betroffenenrechten, Profiling, Recht auf Vergessenwerden und sonstige Regelungen wie zu „Privacy by Design“ und zu „Privacy by Default“. Für die Datenschutz-Grundverordnung werden Regelungsdefizite untersucht und für erkannte Regelungsdefizite konzeptionelle Verbesserungsvorschläge entworfen. Schließlich wird der Ansatz der Verordnung, nur technikneutrale allgemeine Regelungen zu treffen und auf spezifische Problemregelungen zu verzichten, kritisch hinterfragt.

Im abschließenden sechsten Kapitel werden die wesentlichen Ergebnisse der gesamten Studie zusammengefasst.

Die Studie befasst sich im Schwerpunkt mit den Grundrechtsgefährdungen durch private Anbieter und Anwender modernster und künftiger Informationstechnik und sucht für diese Gefährdungen nach Lösungen. Die Handlungsmöglichkeiten von staatlichen Stellen und die Grundrechtsgefährdungen durch diese stehen ebenso wenig im Mittelpunkt der Untersuchung wie mögliche datenschutzrechtliche Lösungen. Dennoch wurden, wo sich dies anbot, auch die neuen Handlungsmöglichkeiten staatlicher Stellen berücksichtigt, das einschlägige geltende Datenschutzrecht untersucht, die dadurch entstehenden Grundrechtsgefährdungen abgeschätzt und datenschutzrechtliche Regelungsmöglichkeiten angedeutet.

Da die Untersuchung dem Erkennen von Regelungsdefiziten gilt und auf die Beseitigung solcher Regelungsdefizite zielt, ist der Begriff des Regelungsdefizits, wie er in der folgenden Untersuchung verwendet wird, zu erläutern. Unter einem Regelungsdefizit soll eine normative Situation verstanden werden, in der Regelungen fehlen oder inadäquat sind, um ein Regelungsproblem zu lösen. Diese Bewertung setzt die Feststellung bestehender oder prognostizierter Problemfelder voraus. Deren Beschreibung soll grundlegend in diesem Kapitel erfolgen. Nähere Beschreibungen finden sich auch in der Untersuchung der Regelungsdefizite in Kapitel 3. Eine Regelung fehlt oder ist inadäquat, wenn das Recht die Erwartungen an die rechtliche Lösung eines Regelungsproblems enttäuscht. Diese Bewertung kann sich zum einen auf den Schutzbedarf für Grundrechte und die Schutzpflicht des Gesetzgebers, sich schützend und fördernd vor diese zu stellen, beziehen. Als solche Grundrechte kommen vor allem die informationelle Selbstbestimmung nach Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG, das Telekommunikationsgeheimnis nach Art. 10 Abs. 1 GG, die Verhaltensfreiheit nach Art. 2 Abs. 1 GG und der Gleichbehandlungsgrundsatz nach Art. 3 GG in Betracht. Maßstab für fehlende oder inadäquate Regelungen können auch die Staatszielbestimmungen der Demokratie, des (informationellen) Sozialstaats und des Rechtsstaats in seinen Ausprägungen der Rechts- und Innovationssicherheit sein. Geschlossen ist ein Regelungsdefizit, wenn eine an diesen Maßstäben gemessen adäquate Regelung besteht.

Kassel, Mai 2016 *Alexander Roßnagel*

Übersicht

EXECUTIVE SUMMARY

Hintergrund und Fragestellung der Studie

Die IT-Nutzung steht vor einem weiteren epochalen Schritt. Viele Alltagsumgebungen und Alltagsgegenstände werden mit „intelligenter" und vernetzter Informationstechnik („smarte Informationstechnik im Alltag") ausgestattet. Bereiche, die sich inzwischen deutlich abzeichnen, sind unter anderen Smart Car, Smart Home und Smart Health. Durch das Zusammenspiel dieser Technologien werden immer weitere Lebensregungen in der körperlichen Welt, bis hinein in die höchst privaten Bereiche des Autos, der Wohnung sowie des Gesundheits- und Fitnesszustandes, als Daten verfügbar. Diese sprunghaft ansteigende Vernetzung und Digitalisierung fast aller Lebensbereiche, die Herausforderungen durch das Internet der Dinge und ein sich ständig wandelndes Nutzerverhalten, zum Teil gepaart mit digitaler Sorglosigkeit, lassen Datenschutz, aber auch Cyber-Sicherheit immer mehr gefährdet erscheinen.

Big Data-Analysen ermöglichen es, die Vielzahl der Daten aus unterschiedlichsten Quellen in sehr kurzer Zeit so auszuwerten, dass auf der Grundlage intensivster Persönlichkeitsprofile mit statistischen Verfahren Verhaltensprognosen für Menschen und Gruppen erstellt und für wirtschaftliche Zwecke genutzt werden können.

Das nationale und das europäische Datenschutzrecht stammen in ihren Grundzügen aus der Vor-Internetzeit. Die EU-Datenschutz-Grundverordnung wurde gerade erlassen und wird das Datenschutzrecht auch in Deutschland auf absehbare Zeit stark prägen.

Vor diesem Hintergrund stellen sich die Fragen, ob und wenn ja welche Anpassungen des Datenschutzrechts notwendig wären, um den Risiken dieser Entwicklungen für Grundrechte gerecht zu werden. Hierbei sollte auch die Frage geklärt werden, ob die Datenschutz-Grundverordnung diese notwendigen Anpassungen bereits vornimmt oder ob auch nach Inkrafttreten der Datenschutz-Grundverordnung

politischer Handlungsbedarf und Handlungsspielraum für den deutschen Gesetzgeber bestehen bleiben.

Anpassungsvorschläge

Im Hinblick auf die Risiken für den Datenschutz der Bürger durch die Verbreitung smarter Informationstechnik im Alltag und die Auswertungsmöglichkeiten durch Big Data, ist es dringend notwendig, die vorhandenen Regelungen risikoadäquat anzupassen. Sie sind nicht ausreichend auf die Risiken durch diese Entwicklungen eingestellt.

Wichtig wäre aufgrund der schieren Masse von Datenverarbeitungen für alle Bereiche, den technischen Datenschutz (Privacy by Design) zu fördern und zu gestalten. Datenschutz, der in die Systeme eingebaut ist, muss nicht mühevoll im Einzelfall überprüft werden – eine Aufgabe die auch gar nicht mehr zu leisten wäre. Die Selbstbestimmung der Bürger über ihre Daten sollte durch freiheitsfördernde Architekturen gestärkt werden. Gerade in komplexen und unübersichtlichen Datenverarbeitungssituationen, wie im Autoverkehr mit Smart Cars, sollte darauf hingewirkt werden, dass den Bürgern einfach verständlich gemacht wird, welche Daten überhaupt von wem verarbeitet werden, und es sollten ihnen einfache Möglichkeiten zur Verfügung stehen. um hierzu zuzustimmen oder nicht. Datenschutz durch Technik muss sich vor allem an die Hersteller von Datenverarbeitungssystemen richten und mit geeigneten Anreizen und Sanktionen durchgesetzt werden.

Wichtig ist für eine Alltagswelt der allgegenwärtigen Datenverarbeitung auch die datenschutzrechtliche Vorsorge für den Umgang mit anonymen Daten: Diese sind vom Datenschutzrecht bisher nicht erfasst. Anonyme Daten können aber gerade durch Big Data plötzlich in sehr intensive Persönlichkeitsprofile umschlagen. Das geltende Datenschutzrecht greift dann aber zu spät. Ausgewählte Regelungen sollten daher auf besonders riskante anonyme Datenverarbeitungen angewendet und um flankierende Vorsorgemaßnahmen ergänzt werden.

In Betracht kommt weiterhin eine thematische Einschränkung der datenschutzrechtlichen Einwilligung als rechtliche Grundlage für besonders riskante Datenverarbeitungen (etwa Gesundheitsprofile) oder für Datenverarbeitungen, die nicht nur für den Einwilligenden, sondern auch für andere Personen Risiken entfalten können (zum Beispiel statistische Vorhersagen von Merkmalen mit Big Data für „ähnliche" Personen).

Das Buch enthält viele konkrete Hinweise zur Umsetzung dieser und weiterer Ziele für den adäquaten Datenschutz in einer Welt smarter Informationstechnik im Alltag.

Datenschutz-Grundverordnung

Die Datenschutz-Grundverordnung verfolgt ein überzogenes Verständnis von Technologieneutralität. Technologieneutralität ist sinnvoll, soweit es darum geht, dass rechtliche Regelungen Technikentwicklungen nicht verhindern sollen und rechtliche Regelungen nicht in der Geschwindigkeit technischer Entwicklungen angepasst werden müssen. Die Verordnung versteht aber Technikneutralität als Risikoneutralität. Die gleichen allgemeinen Datenverarbeitungsregeln, die für den Brötchenkauf beim Bäcker um die Ecke gelten, sollen auch für den Umgang mit umfassenden Persönlichkeitsprofilen aus dem Smart Home gelten. Die Verordnung unterlässt adäquate Regulierung der Risiken moderner Informationstechniken und verfehlt damit das Ziel, den Datenschutz zu modernisieren und den aktuellen Herausforderungen anzupassen.

Die Verordnung verfehlt auch das Ziel, den Datenschutz in der Europäischen Union zu vereinheitlichen. Dies liegt erstens daran, dass sie sehr abstrakte Regelungen und viele unbestimmte Rechtsbegriffe enthält, die zu einer extrem unterschiedlichen Anwendung in verschiedene Mitgliedstaaten führen müssen. Zweitens enthält die Verordnung 70 Öffnungsklauseln, die den Mitgliedstaaten erhebliche Freiräume für abweichende Regelungen belassen.

Eine Anpassung des unionsrechtlichen Datenschutzes an die Risiken smarter Informationstechnik im Alltag und an Big Data wird also in zweierlei Hinsicht versäumt. Gerade angesichts der großen Erwartungen und der langen Dauer des Gesetzgebungsverfahrens ist dies enttäuschend.

Auswirkungen auf die Gewährleistung innerer Sicherheit

Smarte Informationstechnik im Alltag erzeugt erheblich mehr digitale Spuren über Alltagshandeln, als dies bisherige Informationstechnik tat. Diese zusätzlichen Spuren können die Aufklärung von verfassungsfeindlichen Bestrebungen, die Verfolgung und Aufklärung von schweren Straftaten und sonstigen Gefahren für die öffentliche Sicherheit erleichtern. Big Data-Verfahren können dazu beitragen, die Spuren leichter zu verfolgen und auszuwerten. Die künftig vielfach erzeugten Persönlichkeitsprofile von nahezu allen Menschen ermöglichen, die Gewohnheiten, Einstellungen, Präferenzen, sozialen Kontakte und Bewegungen einer Person schnell und präzis zu erfahren. Diese Spuren und Profile im Einzelfall für die Gewährleistung innerer Sicherheit auszuwerten, setzt allerdings den Zugriff auf diese voraus. Da sie überwiegend von US-amerikanischen Anbietern erzeugt, erstellt und gespeichert werden, dürfte ein Zugriff auf diese für deutsche Behörden vielfach ausgeschlossen sein. Soweit in den selteneren Fällen die Datenspuren in Deutschland erhoben und ausgewertet werden, können Spuren und Profile im Prinzip auch für Zwecke der inneren Sicherheit genutzt werden. Da ihr Aussagegehalt erheblich höher ist und sie mehr von der jeweiligen Persönlichkeit preisgeben als die Daten bisheriger Telekommunikation und Datenverarbeitung, wird bei einem Zugriff auf diese auch die Tiefe des Grundrechtseingriffs verstärkt. Wie die neuen Aufklärungsmöglichkeiten genutzt werden können, ohne die Grundrechte der Betroffenen stärker als bisher zu gefährden, bedarf noch der gesellschaftlichen Diskussion.

Zusammenfassung und Ausblick

Smarte Informationstechnik im Alltag ermöglicht Erleichterungen von unerwünschten Aufgaben und die Ergänzung unserer körperlichen und geistigen Fähigkeiten. Big Data-Analysen ermöglichen neue Erkenntnisse, die für die Lösung von Problemen in vielen unterschiedlichen Gesellschafts- und Wirtschaftsbereichen genutzt werden können. Diese Technikanwendungen ermöglichen aber – vor allem in ihrer Kombination – auch eine umfassende Überwachung und Rekonstruktion vieler oder gar aller Ereignisse im Leben der Bürger. Ob wir mit diesen Technikanwendungen besser leben als ohne sie, ist letztlich eine Frage des Datenschutzes.

Auf das bestehende Datenschutzrecht kann dabei nur begrenzt vertraut werden, weil die beschriebenen Entwicklungen vielfach dessen gegenwärtiges Schutzprogramm leer laufen lassen. Bedingung für die künftige Verwirklichung informationeller Selbstbestimmung ist ein modifiziertes und ergänztes Schutzprogramm, in dem die Konzepte und Instrumente des Datenschutzes den spezifischen Risiken der Technikanwendungen angepasst sind.

Die Datenschutz-Grundverordnung wird diesem Anspruch nicht gerecht, im Gegenteil, sie verschlimmert die derzeitige Lage an vielen Stellen. Sie lässt aber, das ist die gute Nachricht, den Gesetzgebern in den Mitgliedstaaten viele Spielräume, die Risiken smarter Informationstechnik im Alltag selbst zu regulieren. Der deutsche Gesetzgeber steht damit vor der drängenden Aufgabe, sich der Modernisierung des Datenschutzrechts für eine Welt smarter Informationstechnik im Alltag anzunehmen. Viele konkrete Vorschläge zur Umsetzung dieser Aufgabe enthält das vorliegende Buch.

Aufgaben des Gesetzgebers

Das Nebeneinander von Unionsrecht und deutschem Datenschutzrecht sowie die vielen Öffnungsklauseln für den nationalen Gesetzgeber in der Verordnung führen zu einer sehr schwer zu durchschauenden Gemengelage des geltenden Rechts. Daher muss der deutsche Ge-

setzgeber das deutsche Datenschutzrecht daraufhin überarbeiten, dass aus der Datenschutz-Grundverordnung und aus dem weiter anwendbaren deutschen Datenschutzrecht eine kohärente, widerspruchsfreie und vollzugsfähige Gesamtregelung des Datenschutzrechts wird. Diese Aufgabe sollte auch dafür genutzt werden, soweit dies möglich ist, risikogerechte Regelungen für die neuen Herausforderungen durch „smarte" Informationstechniken im Alltag und Big Data-Analysen zu erlassen, die in der Verordnung fehlen.

Hierfür können viele Regelungsspielräume genutzt werden, die die Verordnung den Mitgliedstaaten übertragen hat. Es ist daher sinnvoll, die politische Diskussion über eine risikogerechte Regelung neuer Grundrechtsrisiken zu beginnen. Auch sollte Einigkeit darüber herbeigeführt werden, ob die Gesetzgeber in der Union, im Bund oder in den Ländern für eine geeignete Fortentwicklung des Datenschutzrechts zuständig sein sollen.

1 Neue Informationstechnik und neue Risiken für die informationelle Selbstbestimmung

Derzeit steht die Nutzung der Informationstechnik vor einem weiteren epochalen Schritt. Dieser kann durch zwei neue Merkmale charakterisiert werden. Das erste Merkmal ist, dass die Fülle der personenbezogenen Daten, die durch die Verknüpfung der körperlichen Welt mit der virtuellen Welt entstehen, explosionsartig vermehrt wird. Indem viele Alltagsgegenstände mit „intelligenter“ und vernetzter Informationstechnik ausgestattet werden, können Informationen aus dem Internet in der körperlichen Welt genutzt werden und werden umgekehrt alle Lebensregungen in der körperlichen Welt auch in der virtuellen Welt verfügbar. Die Möglichkeiten, Nutzerprofile zu erstellen, werden noch umfangreicher und einfacher. Dies hängt auch mit dem zweiten Merkmal zusammen, dass nämlich die Instrumente, diese Datenfülle zu erfassen und auszuwerten, enorm verbessert werden. Big Data-Analysen ermöglichen, sehr große Mengen heterogener Daten aus unterschiedlichsten Quellen in sehr kurzer Zeit so auszuwerten, dass auf der Grundlage von Persönlichkeitsprofilen und statistischen Verfahren Verhaltensprognosen von Einzelnen und Gruppen erstellt und für wirtschaftliche Zwecke genutzt werden können.

1.1 Risiken durch „smarte“ Informationstechnik im Alltag

„Smarte“ Informationstechnik im Alltag wird im Folgenden anhand von drei repräsentativen Beispielen untersucht. Smart Cars stehen vor allem für die Integration von Informationstechnik in einen Gegenstand und deren Vernetzung. „Smart“ Home steht für das Eindringen der Informationstechnik in den Hintergrund der Alltagsumgebung und repräsentiert damit Ubiquitous Computing im eigentlichen Sinn. Schließlich steht „Smart“ Health für den Einsatz von Informationstechnik am oder im Körper und repräsentiert damit Wearable Computing und die Nutzung der vernetzten Informationstechnik für einen spezialisierten Zweck, der jedoch zunehmend „ausfranst“.

1.1.1 Smart Car (Vernetzung)

Die Automobil- sowie die Informations- und Kommunikationstechnik werden zusammenwachsen. Bereits derzeit sind in modernen Autos[1] etwa 80 elektronische Geräte verbaut, die ständig viele Fahrzeugsystem- und -betriebsdaten verarbeiten. Diese Entwicklung des vernetzten Autos zu einem rollenden Rechenzentrum wird künftig erheblich zunehmen.[2]

Vielfältige Sensoren dienen der Zustandsüberwachung und protokollieren indirekt das Fahrverhalten des Fahrers.[3] Sensoren im Innenraum wie Kameras, Mikrofone, Sitzbelegungs- und Temperaturfühler erfassen das Geschehen im Auto. Bisher führen sie jedoch (noch) überwiegend zur flüchtigen Speicherung personenbezogener Daten.

Das vernetzte Auto wird aber auch Daten aus seiner Umgebung verarbeiten. Sensoren für Abstände, Licht, Wetterphänomene sowie Verkehrsteilnehmer und Verkehrszeichen erhöhen seine Sicherheit und Fahrtüchtigkeit. Kameras,[4] Infrarot und Ultraschall erfassen relevante Ereignisse rund ums Auto.[5] Sie erheben in der Regel allerdings kein Vollbild, sondern nur schematische Repräsentanten anderer Verkehrsteilnehmer.[6] GPS und andere Techniken der Lokalisierung stellen permanent Aufenthaltsort und Fahrtroute des Autos fest.

Daten entstehen auch durch die Kommunikation mit dem Auto. Sie gibt dem Hersteller wichtige Informationen, um seine Produkte weiter zu entwickeln und die Sicherheit des Autos präventiv zu gewährleisten. Spezielle Dienste unterstützen den Fahrer, bieten Sicherheitsinformationen und gewährleisten Notrufe. Sie ermöglichen den Austausch mit anderen Fahrzeugen und mit der Verkehrsinfrastruktur

---

1 Betrachtet werden im Folgenden nur Personenkraftwagen.
2 Detailliert *Bönninger*, 2014, 229; *Bönninger*, DuD 2015, 388.
3 Im folgenden Text werden anstelle der Doppelbezeichnungen die Personen- und Funktionsbezeichnungen in männlicher Form verwendet, stehen aber jeweils für die weibliche und männliche Form.
4 Zu Dash-Cams s. z.B. *Fuchs*, ZD 2015, 212; *Reibach*, DuD 2015, 157.
5 S. zu Erfassung von Fußgängern *Schulz/Roßnagel/David*, ZD 2012, 510.
6 S. hierzu *Rieß/Greß*, DuD 2015, 402.

(zum Beispiel Ampeln und Verkehrshindernissen). Allgemeine Internetdienste ermöglichen (Business-)Kommunikation und Infotainment.

Nach Fahrerassistenz und Vernetzung wird das (teil-)autonome Fahren der nächste Entwicklungsschritt sein.[7] Bestimmte Funktionen teilautonomen Fahrens sind bereits entwickelt oder stehen vor der Nutzungsreife wie automatisierter Parkverkehr (Parkpilot), Stopp&Go-Verkehr (Staupilot), Kolonnenverkehr (Elektronische Deichsel) und automatisiertes Fahren in übersichtlichen Situationen auf der Autobahn (Autobahnpilot). Mit der Übernahme von mehr Steuerungskompetenz durch Automaten wird auch die Notwendigkeit ansteigen, alle Zustands- und Umgebungsbedingungen des Autos zu kontrollieren und festzuhalten. Die Datenflut wird notwendigerweise enorm ansteigen.

Die Daten werden in unterschiedlicher Weise gespeichert, verarbeitet und ausgetauscht. Dies ist relevant für die Missbrauchsmöglichkeiten und den datenschutzrechtlichen Regelungsbedarf. Sie werden derzeit überwiegend nur flüchtig, können aber grundsätzlich auch persistent gespeichert werden. Die Formate der Daten und ihre Verarbeitung sind heute überwiegend proprietär und bisher wenig standardisiert.[8] Die Daten können zentral (Hersteller, Cloud, Auftragnehmer) oder dezentral (Auto, Alter Ego) gespeichert werden. Die Datenkommunikation kann identifizierend oder breit gestreut (ohne die Empfänger zu kennen) erfolgen.

Der Wert der Daten kann sehr unterschiedlich sein. Sie können einen hohen ökonomischen Wert haben, der leicht zu realisieren ist. Dies eröffnet vielfältige Missbrauchsmotive und begründet einen hohen Druck auf den Gesetzgeber, diese Möglichkeiten auch nutzen zu können. Viele Daten können grundsätzlich mit Gewinn durch unterschiedliche Interessenten auch für andere Zwecke – wie etwa für Pro-

---

7 S. hierzu *Maurer/Gerdes/Lenz/Winner* 2015; *Lutz*, NJW 2015, 119; *Lutz/Tang/Lienkamp*, NZV 2013, 57.

8 Z.B. die Schnittstelle zur On-Bord-Diagnose (OBD) – s. *Roßnagel* 2014a, 259.

duktverbesserung, Informationsbereitstellung, Risikoeinschätzung, Profilierung und Werbung – verwendet werden. Je nach technischer Gestaltung kann der Zugriff auf sie für andere ausgeschlossen oder möglich sein.

Auch die Datensensitivität kann sehr unterschiedlich sein. Sie entscheidet über die Gebrauchs- und Missbrauchsrisiken für bestimmte Betroffene. Die Aussagekraft der Daten kann sehr hoch sein. Mit ihnen lassen sich Fahr-, Nutzungs-, Kommunikations-, Bewegungs-, Verhaltens- und Beziehungsprofile erstellen.[9] Aus diesen Daten lassen sich auch soziale Netze, Gruppenbeziehungen und Gruppenverhalten erkennen. Big Data ermöglicht, aus ihnen personenbezogene oder auf den Durchschnitt bezogene Verhaltensvorhersagen abzuleiten.[10]

An den Daten, die beim Betrieb und in der Kommunikation zum oder vom vernetzten Automobil entstehen, haben sehr viele unterschiedliche Akteure sehr unterschiedlichen Interessen:[11]

Zunächst gibt es viele unterschiedliche Betroffene, deren Daten erhoben, verarbeitet und genutzt werden sollen. Vorrangig ist es der Halter. Dieser ist oft der Käufer und Eigentümer, kann aber auch etwa bei Leasing oder Eigentumsvorbehalt der Besitzer sein. Verkauft er sein Gebrauchtauto an einen zweiten Halter und dieser an einen weiteren Halter, werden die Daten des Autos auf diese bezogen, ohne dass sie eine Rechtsbeziehung zum Hersteller haben. Bestimmte, den Datenumgang legitimierende Vereinbarungen oder Einwilligungen des Ersthalters mit dem Hersteller oder Verkäufer gelten für den Umgang mit den Daten der weiteren Halter grundsätzlich nicht.[12] Neben dem Halter sind auch die Fahrer betroffen. Da sie vielfach wechseln können (innerhalb der Familie, des Unternehmens, der Behörde oder bei ei-

---

9 S. z.B. *Roßnagel*, NVZ 2006, 284; *Lüdemann/Sengstacken/Vogelpohl*, ZD 2015, 55; *Kinast/Kühnl*, NJW 2014, 3059.

10 S. hierzu Kap. 1.2; s. auch z.B. *Weichert*, ZD 2013, 251; *Roßnagel*, ZD 2013, 562; *Richter* 2015.

11 S. zu ihren Rechtsbeziehungen ausführlich *Roßnagel* 2014a, 257 ff.

12 Mit Ausnahme spezifischer Vereinbarungen mit dem Ersthalter, die dieser auf den nächsten Halter übertragen muss.

nem Autovermieter oder Car-Sharing-Unternehmen) können viele unterschiedliche Personen betroffen sein. In bestimmten Fällen können auch Beifahrer (zum Beispiel durch Kameras) erfasst werden.

Interessiert an Daten der Betroffenen aus ihrem vernetzten Automobil sind viele Gruppen mit unterschiedlichen Interessen. Hersteller, Vertragshändler und Vertragswerkstätten gehören zu einem gemeinsamen Vertriebssystem und sind auf dessen Fahrzeuge spezialisiert. Dieses bietet vielfältige Dienstleistungen rund um die Kraftfahrzeuge der jeweiligen Marke(n) an. Es kann die im Kraftfahrzeug entstehenden Daten benötigen, um seine Fahrzeuge weiter zu entwickeln, um Fehler an den Fahrzeugen seiner Flotten zu erkennen, um Gewährleistungsfälle zu beurteilen, die Fahrzeugwartung sicherzustellen und um Beweise für Fälle der Produkt- und Vertragshaftung zu sichern. Unabhängige Werkstätten und Pannenhilfsdienste sind ebenfalls auf die Informationen in den Bordsystemen angewiesen, um sie zu diagnostizieren, die richtigen Ersatzteile zu finden und gezielte Reparaturen durchzuführen.[13]

Eine weitere Gruppe sind die an Notrufsystemen Beteiligten. Für den Emergency-Call (E-Call)[14] sind dies der Notrufdienst, der Hersteller, der Abschleppdienst, die Verkehrspolizei und der Telekommunikationsdiensteanbieter.[15] Dies gilt für den Breakdown-Call (B-Call), den einige Hersteller anbieten, in vergleichbarer Weise. Sodann gibt es eine weitere Gruppe von Interessenten, die ihre Autos anderen zur Verfügung stellen und über den Aufenthaltsort und den Zustand, aber eventuell auch über die Fahrweise informiert sein wollen, wie die Ei-

---

13 Haben sie keinen Zugriff auf diese Daten und können z.B. keine Fehlerprotokolle auslesen, führt dies zu einem Lock-in-Effekt. Dann kann der Halter sich nicht mehr die Werkstatt seiner Wahl aussuchen, sondern ist an die Vertragswerkstätten des Herstellers gebunden – s. hierzu ausführlich *Roßnagel*, 2014a, 277 ff.

14 S. zu diesem Verordnung 2015/758 vom 29.4.2015, ABl. L 123 vom 19.5.2015, 77; s. hierzu auch Art. 29-Datenschutzgruppe 2006.

15 *Pohle/Zoch*, CR 2014, 412 ff.; *Kinast/Kühnl*, NJW 2014, 3057; *Weichert* 2014, 305 ff.; *Scherer*, MMR 2014, 353.

gentümer von Dienstfahrzeugen, Verantwortliche für das Flottenmanagement, Autovermietungen oder Carsharing-Anbieter.[16]

Wenn demnächst alle neuen Automobile ohnehin über eine Kommunikationsschrittstelle verfügen, werden sich viele weitere Interessenten finden, um diese Schnittstelle zu nutzen.[17] Zu denken ist an die erfolgreichen Dienste im Internet wie Suchdienste, Social Networks, Messenger und ähnliche Dienste, die für Infotainment im Automobil sorgen wollen.[18] Für die Bequemlichkeit und Sicherheit im Auto werden unzählige Apps entwickelt werden und um die Gunst der Halter und Fahrer ringen. Andere Interessenten haben bereits eigene Schnittstellen zum Bordsystem entwickelt oder eigene Geräte in das Auto eingebracht wie Versicherungen[19] oder dynamische Navigationsdienste. Wenn die Sicherheit der Autos gegenüber Angreifern, die über Kommunikationsschnittstellen in das vernetzte Auto eindringen wollen, gewährleistet werden soll, müssen Berechtigungen abgefragt und zusätzliche Daten erhoben und protokolliert werden.[20]

Schließlich gibt es noch die an den Daten interessierten staatlichen Stellen. Nach einem Unfall oder einem Verkehrsverstoß können Polizei und Gerichte Ansprüche auf Daten des Autos geltend machen.[21] Dies kann auch für Unfallgegner gelten.[22] Strittig ist derzeit bereits inwieweit Videos aus Dash-Cams für Beweiszwecke genutzt werden können.[23] Strafverfolgungsbehörden und Nachrichtendienste interessieren sich für die Daten, aus denen Bewegungs-, Kommunikations- und Beziehungsprofile erstellt und Präferenzen und Gewohnheiten

---

16 S. z.B. *Kinast/Kühnl*, NJW 2014, 3058.

17 Erwägungsgrund 16 der Verordnung 2015/758 hält dies ausdrücklich offen.

18 S. hierzu *Hansen,* DuD 2015, 367.

19 Zum Dienst S-Drive der Sparkassen DirektVersicherung s. https://www. sparkassendirekt.de/telematik; s. auch *Pohle/Zoch*, CR 2014, 411; *Kinast/Kühnl*, NJW 2014, 3057; *Reiners*, ZD 2015, 52; *Weichert* 2014, 307f.; *Schwichtenberg*, DuD 2015, 378.

20 S. zu dieser Problematik z.B. *Krauß/Waidner*, DuD 2015, 383; *Hornung*, DuD 2015, 259.

21 S. hierzu auch *Mielchen* 2014, 241 ff.

22 S. näher *Mielchen*, NVZ 2014, 81 ff., 86; *Balzer/Nugel*, NJW 2016, 193.

23 S. z.B. *Atzert/Franck*, RDV 2014, 136; *Balzer/Nugel*, NJW 2014, 1622; *Greger*, NVZ 2015, 114; *Knyrim/Trieb*, ZD 2014, 547.

abgelesen werden können. Schließlich erfasst die Vorratsdatenspeicherung nach den §§ 113a ff. TKG[24] auch alle Kommunikationsverkehrsdaten von und zum Automobil: Diese werden für die jeweils vorgesehene Frist vom Telekommunikationsanbieter lückenlos gespeichert.[25]

Risiken für Grundrechte werden durch die Vernetzung der Automobile vervielfacht. Die Vernetzung verändert das Automobil vom geschützten Privatraum zu einem Teil des Internet. Während das Auto bisher ein Rückzugsraum für Individuum und Familie war, indem der Fahrer pseudonym agierte, wird sich dies künftig radikal verändern. Durch Datenverarbeitung und Vernetzung wird es möglich, das gesamte Fahrverhalten und den Umgang mit dem Auto zu erfassen. Ford-Europa-Chef Jim Farley: „Wir kennen jeden Autofahrer, der die Verkehrsregeln bricht. Und weil GPS in den Autos ist, wissen wir, wo und wie jemand das tut."[26]

Die personenbezogenen Daten, die das Auto erfasst und mit vielen anderen austauscht, sind sehr aussagekräftig und bilden je nach Nutzung des Autos das gesamte mobile Leben ab. Je nach Architektur der vernetzten Systeme befinden sich diese Daten nicht nur im Auto und werden nur kurzfristig gespeichert, sondern befinden sich in Datenbanken oder Clouds von Herstellern, Versicherungen, Arbeitgebern, Autovermietungen, Diensteanbietern und vielen weiteren der genannten Interessenten. Sie können von diesen genutzt werden, den Halter oder Fahrer zu unterstützen, sie können in Konfliktfällen aber auch gegen ihn verwendet werden. Was mit den Daten geschieht, an wen sie weiter gegeben werden und für welche Zwecke sie genutzt werden, haben die Betroffenen nicht mehr unter Kontrolle. Sie wissen nicht, ob und wann sie mit diesen Daten konfrontiert werden. Auch dürften die Daten genutzt werden, um ihnen im geeigneten Moment, in der passenden emotionalen Situation und in der geeigneten perso-

---

24 S. hierzu *Roßnagel*, NJW 2016, 533.

25 Zur Vorratsdatenspeicherung s. auch *EuGH*, NJW 2014, 2196; BVerfGE 125, 260; sowie *Roßnagel/Moser-Knierim/Schweda* 2013; *Roßnagel*, MMR 2014, 372.

26 *Kaiser*, Spione an Bord, Stern vom 15.1.2015, 78.

nalisierten Auswahl „unwiderstehliche“ Angebote zu unterbreiten. Schließlich besteht ein weiteres Risiko prinzipiell darin, dass die personenbezogenen Daten bei der Übertragung von und zum Auto von Dritten ausgelesen und verändert werden.[27]

Die Halter und Fahrer künftiger Autos werden kaum die Chance haben, sich für oder gegen ein vernetztes Auto zu entscheiden. Wenn automobile Mobilität durch Datenverarbeitung und Vernetzung sicherer wird, dürfte es bald nicht mehr verantwortbar erscheinen,[28] mit einem unsicheren, nicht vernetzten Auto am Straßenverkehr teilzunehmen. Außerdem erhöhen Datenverarbeitung und Vernetzung die Bequemlichkeit der Fortbewegung. Sie ermöglichen viele Funktionen im Auto, die bald kaum jemand mehr missen mag. Dass durch sie auch das mobile Leben protokolliert und vielen Interessenten zugänglich gemacht werden kann, wird als alternativlos hingenommen werden.

1.1.2 Smart Home (Ubiquitous Computing)

„Smart Home“ beschreibt die Nutzung von intelligenter Informationstechnik im eigenen Wohnumfeld. Solche intelligente Informationstechnik kann in aller Regel Daten verarbeiten, ist mit dem Internet und anderen Geräten vernetzt und ist fernsteuerbar. Das „intelligente Heim“ entsteht letztlich durch das Zusammenspiel vieler einzelner Komponenten, die überall im Haus verteilt oder verbaut sind. Smart Home kann mithin als ein konkretes Anwendungsbeispiel für die unter den Begriffen Ubiquitous Computing, Internet der Dinge und Pervasive Computing zusammengefassten informationstechnischen Konzepte verstanden werden. Die Steuerung des Smart Home und die Speicherung von Daten können ausgelagert sein oder im Haus selbst liegen.

Der Begriff des Smart Home wird zur Umschreibung von Technik unterschiedlichster Komplexität genutzt, von bereits jetzt verwirklichten Systemen zur Fernsteuerung und Zeitschaltung etwa von Licht und

---

27 S. z.B. *Krauß/Waidner*, DuD 2015, 383.

28 Z.B. auch durch Versicherungsbedingungen oder Prämiengestaltungen.

Rollläden bis hin zur futuristischen Vision umfassender und vollintegrierter Assistenzsysteme, die die Bewohner auch unter Zuhilfenahme kooperierender, autonomer Roboter in (fast) allen Lebenslagen unterstützen können. Die potentielle Funktionalität des Smart Home ist jedoch nicht auf die Assistenz der Bewohner beschränkt, sondern kann etwa auch rein ästhetischen Charakter haben.[29] Insgesamt kann der Begriff des Smart Home eine ganze Reihe von Bereichen umfassen, von Energie und Gesundheit[30] bis hin zu Entertainment und Shopping.

Assistenzsysteme benötigen in der Regel Informationen über die Umgebung, in der sie sich befinden. Diese können entweder bei Inbetriebnahme eingespeist werden (statische Parameter; zum Beispiel Raumgröße, Standort von Möbeln) oder sie werden vom Gerät selbst fortlaufend erhoben (dynamische Parameter; zum Beispiel Temperatur, Standort des Nutzers). In letzterem Fall sind Sensoren erforderlich, die die fraglichen Parameter erfassen. Bereits seit längerer Zeit Stand der Technik ist etwa die Heizungsanlage, die sich den Außentemperaturen anpasst.

Eine besondere Bedeutung auf dem Weg zur Verwirklichung der Vision vollintegrierter und umfassender Assistenzsysteme in den eigenen vier Wänden kommt Smart Television und Smart Metering zu.

Das vernetzte und mit ausreichender Prozessorleistung ausgestattete Fernsehgerät bringt bereits heute viele technische Funktionalitäten

---

[29] „Teil einiger UC-Szenarien ist auch, dass die Wohnung zu einer individuellen Bilderwelt wird, in der in Bilderrahmen, auf Wänden oder in Spiegeln Videobotschaften, Filme, Bilder oder Texthinweise erscheinen, die von einer bestimmten Person oder einem bestimmten Situationskontext automatisch ausgelöst werden, wenn z.B. ein Raum betreten oder zu einer bestimmten Uhrzeit ein Sessel benutzt wird. Durch entsprechende Auslöser lassen sich auch individuell und zielgerichtet die Raumsituation wie beispielsweise die Fußboden- und Wandbeschaffenheit und -farbe gestalten sowie die Bedingungen des Wohnumfeldes nach den individuellen Voreinstellungen von der Beleuchtung bis zur Musik automatisch einstellen." *Bizer u.a.* 2006, 48; *Roßnagel* 2007, 53 ff.; zu den heutigen Vorstellungen von Smart Home s. *Skistims* 2016, 33 ff, 68 ff.

[30] Zu E-Health-Anwendungen s. das folgende Kapitel.

mit, die für das Smart Home charakteristisch sind. Zudem nimmt es meist einen zentralen Platz in den Wohnzimmern, aber auch in Schlafzimmern, Kinderzimmern und Küchen ein, und befindet sich damit bereits im Herz vieler Wohnungen. Auf das Smart TV können neben der Funktionalität als klassischer Fernseher, Video on Demand und Webbrowser verschiedenste weitere Applikationen aufgespielt werden. Zwar fehlen dem Smart TV funktionsbedingt bestimmte für Smartphones charakteristische Sensoren, insbesondere GPS und Gyroskop, jedoch sind zunehmend besonders invasive Sensoren wie Kameras und Mikrofone verbaut. Diese ermöglichen neben Videotelefonie auch Sprachsteuerung und Gestenerkennung.[31] Ferner kann Smart TV durch seine inhärenten Fähigkeiten als Mittel zur Visualisierung des Smart Home und als Mensch-Maschine-Schnittstelle genutzt werden.

Smart Meter(ing) steht für „intelligente" und vernetzte Strom-, Gas- oder Wasserzähler und soll helfen, Ressourcen einzusparen. Seine Bedeutung ergibt sich unter anderem daraus, dass hier die Einführung der Technik gesetzlich vorgeschrieben wird.[32] Zugleich bietet es das Potential, als Steuergerät für den gesamten Haushalt zu dienen.

Des Weiteren zeigen Entwicklungen aus dem Bereich Ambient Assisted Living deutlich die technischen Potentiale des Smart Home auf. Der Begriff bezeichnet altersgerechte Assistenzsysteme zur Entlastung von Pflegepersonal und Familienmitgliedern. Die Zielgruppe des Ambient Assisted Living sind ältere Menschen, Menschen mit Behinderungen und Krankheiten sowie aus sonstigen Gründen pflegebedürftige Menschen. Die Techniken, die derzeit in diesem Bereich entwickelt werden, können jedoch auch allgemein zur Unterstützung von Menschen eingesetzt werden. Ein Beispiel ist das Senioren-Assistenzsystem „SUSI TD",[33] das durch Sensoren physische Hilflo-

---

31 *Dix* 2013, 49; *Skistims* 2016, 62f.

32 S. hierzu mehr unter Kap. 2.4.1.2.

33 Sicherheit und Unterstützung für Senioren durch Integration von Technik und Dienstleistung; entwickelt durch das Fraunhofer-Institut für Experimentelles Software Engineering (IESE) in Kaiserslautern. http://www.iese.fraunhofer.de/de/presse/press_archive/press_2014/PM_2014_22_250714_susi-td.html

sigkeit erkennen soll, worunter insbesondere Stürze fallen dürften. Ein anderes Beispiel ist der Serviceroboter „Care-O-bot".[34] Das Projekt „OPDEMIVA"[35] unter Leitung der Technischen Universität Chemnitz geht noch weiter. Durch ein 3D-Sensorsystem wird der Tagesablauf einer demenzkranken Person erfasst und ausgewertet. Dies ist gekoppelt mit einer Erinnerungsfunktion, die darauf hinweist, dass bestimmte Tätigkeiten durchgeführt werden sollen, wie etwa die Einnahme von Tabletten, wenn zuvor durch das System erkannt wurde, dass die fragliche Tätigkeit unterblieben ist. Die Privatsphäre der Nutzer soll dabei dadurch gewahrt werden, dass die gesammelten Daten das in der Wohnung installierte System nicht verlassen.

Derartige Projekte[36] weisen darauf hin, wie in Zukunft Assistenzsysteme den Menschen im Alltag begleiten könnten. Zudem geben sie auch einen Einblick in die sozialen Implikationen. Gesellschaftliche Veränderungen scheinen mit steigendem Umfang und Effizienz von Assistenzsystemen unausweichlich zu sein. Diese können beispielsweise die Form eines Kompetenzverlustes einnehmen, wenn Menschen bestimmte Fähigkeiten nicht mehr erlernen, da sie in ihrem hochtechnisierten Umfeld nicht mehr benötigt werden. Das kommerzielle Potential für Serviceroboter im Haushalt lässt sich indes am Erfolg der Geräte des Herstellers „iRobot" ablesen.[37]

---

34 Entwickelt durch das Fraunhofer-Institut für Produktionstechnik und Automatisierung (IPA) in Stuttgart. Seit Anfang 2015 ist die vierte Version des Roboters erhältlich. „Als mobiler Informationskiosk im Museum, Baumarkt oder Flughafen, für Hol- und Bringdienste in Heimen oder Büros, für Sicherheitsanwendungen oder als Museumsroboter zur Attraktion – stets ist der Care-O-bot® 4 ein sicherer und nützlicher Helfer des Menschen" – Fraunhofer IPA, Presseinformation v. 15.1.2015, 2, http://www.care-o-bot.de/de/care-o-bot-4.html.

35 Optimierung der Pflege demenzkranker Menschen durch intelligente Verhaltensanalyse; http://www.opdemiva.de.

36 S. zu weitere Projekte des Smart Home *Skistims* 2016, 37 ff.

37 Das Unternehmen vertreibt Heimroboter zur Dachrinnenreinigung, zur Poolsäuberung, zum Bodenwischen und als wohl bekanntestes Produkt den „Roomba" Staubsaugerroboter.

Ein letztes Beispiel für die technischen Potentiale des Smart Home soll Amazon Echo bieten.[38] Dabei handelt es sich um ein cloudbasiertes, sprachgesteuertes Assistenzsystem, das zudem mit weiteren kompatiblen Geräten im Haus, wie beispielsweise bestimmten Lichtschaltern und Steckdosen, vernetzt werden kann. Das System wird seit Juni 2015 in den USA verkauft.

Risiken ergeben sich zunächst bei mangelnder Datensicherheit im Sinn mangelhafter oder nicht vorhandener Schutzmaßnahmen vor unbefugten Zugriffen auf Systeme des Smart Home.[39] Mit sinkender Datensicherheit steigt das Risiko, dass sich Fremde Zugriff auf Daten verschaffen, die das System verarbeitet. Gleichzeitig steigt mit zunehmender Technisierung und Vernetzung die Zahl der Geräte, die für Hacking zugänglich werden. Hacking betrifft damit immer mehr Geräte, die zuvor mangels entsprechender technischer Fähigkeiten keine derartigen Verwundbarkeiten aufwiesen. Die für den Einbrecher wichtige Abwesenheit der Bewohner eines Hauses oder einer Wohnung etwa muss dann nicht mehr durch Observation ausgespäht werden, sondern ergibt sich aus den anfallenden Daten. Gleiches gilt für die Solvenz, soweit der Einsatz entsprechender Informationstechnik im Smart Home als Indikator für die wirtschaftliche Leistungsfähigkeit der Bewohner gewertet werden kann. Überspitzt ausgedrückt könnte für den Einbrecher der Zukunft nicht mehr die Brechstange, sondern Hacking-Software wichtigstes Berufswerkzeug sein. Zudem kann

---

[38] Ähnliche Systeme für mobile Geräte und Heimcomputer sind Apples Siri und Microsofts Cortana. Ebenfalls in diese Richtung geht die von Mattel seit November 2015 in den USA vertriebene Hello Barbie Doll. Dabei handelt es sich jedoch nicht um ein Assistenzsystem, sondern einen computergesteuerten Kommunikationspartner. Die aufgezeichneten Gespräche mit der Puppe können Eltern über ein ToyTalk-Benutzerkonto aus dem Cloudspeicher des Herstellers abrufen. Aus den FAQ, http://hellobarbiefaq.mattel.com/wp-content/uploads/2015/08/hellobarbie-faq-v1.pdf: „Is Hello Barbie recording and storing conversations girls have with the doll? Yes. Hello Barbie has conversations with girls, and these conversations are recorded. […] These conversations are stored securely on ToyTalk's server infrastructure and parents have the power to listen to, share, and/or delete stored recordings any time."

[39] S. hierzu ausführlich *Skistims* 2016, 136 ff.

wirtschaftlicher Schaden entstehen, wenn etwa unbefugt die Solltemperatur der Heizungsanlage erhöht wird.

Die Systeme des Smart Home beeinflussen die physische Welt. Wer Zugriff auf diese Systeme hat, kann damit auch die Bewohner direkt oder indirekt beeinflussen. Über die Manipulation etwa vernetzter Gasöfen oder telemedizinischer Geräte ist sogar eine Gefährdung von Leben und körperlicher Unversehrtheit denkbar. Bereits die hier dargestellten Beispiele zeigen in aller Deutlichkeit, welch essentielle Bedeutung Cybersicherheit für das Smart Home hat. Die Realisierbarkeit von Angriffen auf die Systeme des Smart Home hängt letztlich von der Effektivität der ergriffenen Schutzmaßnahmen ab. Schutzmaßnahmen können von der Verschlüsselung von Datenübertragungen bis hin zur Gestaltung der informationstechnischen Infrastruktur selbst reichen. Wurde eine Sicherheitslücke erkannt, so muss diese sofort geschlossen werden. Dazu müssen Aktualisierungen durch die Hersteller oder Anbieter bereitgestellt und aufgespielt werden. Durch die Möglichkeit des unbemerkten Einbaus von Hintertüren von Seiten der Hersteller erhält die Thematik der Cybersicherheit eine zusätzlich Brisanz.

Darüber hinaus ergeben sich systeminhärente Risiken bereits aus der bestimmungsgemäßen Nutzung der Techniken des Smart Home. Hier ist zuvorderst die Bildung von detaillierten Nutzerprofilen zu nennen, die bei umfassenden Assistenzsystemen und bei lernenden Systemen insgesamt ein grundlegendes Funktionsmerkmal darstellt. Das Leben der Bewohner wird durch die Systeme des Smart Home erfasst, ausgewertet und gespeichert.[40] Der Umfang hängt dabei von Quantität und Qualität der Erfassung ab, insbesondere von den erhobenen Parametern. Personalisierte Angebote sind auf die Identifizierung von Nutzern angewiesen. Hierzu kommen im Kontext von Smart Home je nach Ausgestaltung grundsätzlich fast alle marktüblichen Identifizie-

[40] S. hierzu ausführlich *Skistims* 2016, 127 ff.

rungsverfahren in Betracht, von der Passworteingabe bis hin zur Gesichtserkennung.

Es zeigt sich, dass das Konzept des Smart Home hohe Risiken für die informationelle Selbstbestimmung mit sich bringt. Dies betrifft zunächst vor allem die Bewohner, aber auch Gäste, die sich in einen „fremden Bereich" begeben, „dem sie ähnlich viel Vertrauen entgegenbringen müssen wie ihrem eigenen persönlichen Lebensbereich".[41] Betroffen sind darüber hinaus Handwerker und potentiell auch Angestellte von Lieferdiensten, sofern sie mit Systemen des Smart Home in Kontakt treten. Zudem können durch eine Abstrahierung der im Rahmen der weiter unten beschriebenen Big Data-Analyse gewonnenen Daten Rückschlüsse auf weitere Personengruppen gezogen werden, die ähnliche Lebensumstände und Rahmenbedingungen aufweisen. Es können Durchschnittswerte für andere Verbraucher errechnet werden; Kontextvorhersagen für eine Person können auf Personen mit ähnlichen Basisparametern übertragen werden.[42] Darüber hinaus werden im Smart Home aber auch unkritische Daten erfasst und ausgewertet. Insbesondere Umweltdaten wie die Außentemperatur lassen keine Rückschlüsse auf persönliche oder sachliche Verhältnisse zu. Wie jedoch auch eine scheinbar unkritische Datenerhebung einen massiven Eingriff darstellen kann, soll ein Beispiel zeigen. So konnte in Versuchen experimentell nachgewiesen werden, dass bei kurzen Ablese-Intervallen bei elektronischen Stromzählern „neben der Erkennung von im Haushalt befindlichen Geräten eine Erkennung des Fernsehprogramms und eine Identifikation des abgespielten Videoinhalts möglich ist".[43]

Über die beim Einsatz von komplexer Informationstechnik regelmäßig betroffenen Grundrechte hinaus ist zudem Art. 13 GG einschlägig.[44] Verletzungen grundrechtlicher Positionen werden als besonders inva-

---

41 S. hierzu ausführlich *Skistims* 2016, 133f.
42 Zu Risiken durch Big Data-Analysen s. umfassend Kap. 1.1.4.
43 *Greveler/Justus/Löhr* 2012, 35.
44 S. hierzu *Skistims* 2016, 134f.

siv empfunden, wenn sie die eigene Wohnstätte als geschützten Rückzugsort betreffen, in dem sich allerintimste Handlungen abspielen. So machten etwa die Beschwerdeführer beim Großen Lauschangriff geltend: „Auf das Telefonieren und Briefeschreiben könne gegebenenfalls verzichtet werden, auf eine letzte Rückzugsmöglichkeit in der eigenen Wohnung nicht."[45] Ferner können die Grundrechte der Art. 4 Abs. 1 und 2 GG und Art. 6 Abs. 1 GG tangiert sein. Weitere Probleme ergeben sich beim Einsatz von Techniken des Smart Home durch den Arbeitgeber sowie im Rahmen der Heimarbeit.[46]

Die „Förderung von Smart-Home-Anwendungen" ist indes Teil der Digitalen Agenda der Bundesregierung.[47] Die beispielhaft angeführten Ziele sind hier die „Optimierung von Energiekosten" und die „Telearbeit".[48] Auch für die Werbeindustrie dürfte das Smart Home von höchstem Interesse sein, da nicht nur punktuell, etwa im Auto, vom PC oder vom Smartphone, Anhaltspunkte für erfolgreiche Verkaufsstrategien gesammelt werden können, sondern über die gesamte Wohnlandschaft hinweg. Gleichzeitig kann auch potentiell über die gesamte Wohnumgebung hinweg Werbung präsentiert werden, insbesondere solche, die auf Basis gesammelter Daten auf die adressierte Person abgestimmt ist. Das Anbieten vordergründig kostenloser Dienste im Tausch gegen Daten und dem Akzeptieren von Werbeeinblendungen ist somit gerade im Kontext des Smart Home ein äußerst lukratives Geschäftsmodell. Darüber hinaus ermöglicht die Vernetzung Marktforschung durch die Hersteller direkt beim Kunden. Hierbei werden Daten im laufenden Betrieb anonym erhoben und ausgewertet, um Anhaltspunkte für die Entwicklung zukünftiger Produkte oder die Nachbesserung bestehender Produktreihen zu gewinnen.

Die im Smart Home erfassten Daten haben mithin einen hohen wirtschaftlichen Wert. Diensteanbieter „können aus Verkehrsdaten,

---

45 *BVerfGE* 109, 279 (291).
46 S. hierzu ausführlich *Skistims* 2016, 136 ff.
47 *Bundesregierung*, Digitale Agenda 2014-2017, 14.
48 *Bundesregierung*, Digitale Agenda 2014-2017, 9.

Standortinformationen des Sensors und Inhaltsdaten sowie dem Kontextwissen um typische Aufstellungsorte von Sensoren sogar einen virtuellen Grundriss von Wohnungen mit detaillierten Verhaltensmustern der Anwesenden entwickeln".[49]

Zusammenfassend lässt sich feststellen, dass im Bereich Smart Home bei sehr einfachen und schwach bis gar nicht vernetzten Systemen die Herausforderungen für das Datenschutzrecht überschaubar bleiben. Sie steigen mit dem Grad der Vernetzung und der Granularität der erhobenen Daten jedoch erheblich.

1.1.3 Smart Health

Die Digitalisierung und der Einsatz von Informationstechniken setzen sich im Gesundheitsbereich stetig fort. Es lassen sich in den letzten Jahren zwei parallele Entwicklungsbereiche beobachten, die durch den Oberbegriff Smart Health erfasst werden können und jeweils eine andere Zielsetzung verfolgen. Dem ersten Entwicklungsbereich sind Wearables, wie Fitnessarmbänder und Smartwatches, sowie Gesundheits- und Fitness-Apps zuzuordnen. Diese sind tendenziell auf die Selbstkontrolle des Einzelnen über seinen Gesundheits- und Fitnesszustand ausgerichtet. Sie dienen vorrangig dem Bestreben, die eigene Gesundheit zu erhalten, Maßnahmen der Gesundheitsvorsorge zu treffen und das physische und psychische Wohlbefinden zu steigern, indem sie zum Beispiel eine gesunde und ausgewogene Ernährung, erholsame Schlaf- und Entspannungsphasen sowie ausreichende, körperliche Bewegung und persönliche Fitness unterstützen und fördern. Derartige Anwendungen haben den aktuellen Trend der Selbstvermessung oder auf Englisch „Quantified Self" begründet.

Daneben wird als zweiter Entwicklungsbereich die Weiterentwicklung der Telematik im Gesundheitswesen durch staatliche Maßnahmen betrachtet, die insbesondere durch das Inkrafttreten des E-Health-Gesetzes zum 1. Januar 2016 vorangetrieben wird. Der Gesundheits-

---

[49] *Raabe/Weis*, RDV 2014, 231 (238).

telematik zugerechnet werden die Anwendung von Telekommunikations- und Informationstechniken auf das Gesundheitswesen, insbesondere auf administrative Prozesse, Wissensvermittlungs- und Behandlungsverfahren zwischen allen Beteiligten des Gesundheitswesens insbesondere Krankenhäuser, Ärzte, gesetzliche und private Krankenkassen, Abrechnungsstellen und Patienten. Sie dienen allgemein der Kommunikationserleichterung zwischen den Beteiligten, Effizienzsteigerungen, Rationalisierungen und Qualitätsverbesserungen durch vernetzte Versorgungsketten. Als erster entscheidender Baustein der Gesundheitstelematik ist die verpflichtende Einführung der elektronischen Gesundheitskarte nach mittlerweile 20 Jahren des Ringens zum 1. Januar 2015 anzusehen. Einen Teilbereich der Gesundheitstelematik bildet die Telemedizin. Sie umfasst die Erbringung einer ärztlichen Leistung in den Bereichen Diagnostik, Therapie und Vorsorge unter dem Einsatz von Informations- und Kommunikationstechnik.[50] Sie verfolgt die Zielsetzung, die patientenorientierte gesundheitliche Versorgung zu optimieren. Schließlich stellt das Telemonitoring einen weiteren Teilaspekt der Telemedizin dar. Hierbei steht die Überbrückung einer räumlichen und zeitlichen Distanz durch Informations- und Kommunikationstechnik zwischen Arzt und Patienten im Vordergrund. Telemonitoring umfasst entsprechend die Fernuntersuchung, -diagnose und -überwachung des Patienten durch seinen behandelnden Arzt. Der wesentliche Unterschied zwischen dem ersten und dem zweiten Entwicklungsbereich sind somit die Adressaten und die jeweilige konkrete Zielsetzung.

Die „professionelle" Gesundheitstelematik, die Gesundheitsdienstleistungen unterstützt und Beschäftigte des Gesundheitswesens als Anwender einbezieht, wird überwiegend als E-Health bezeichnet. Auch wenn die Gesundheitsvorsorge mit umfasst ist, dient E-Health nicht primär der allgemeinen Verbesserung der Gesundheit oder gar der Fitness, sondern verfolgt das Ziel, den Eintritt eines pathologischen Zustands zu verhindern oder die Heilung des Patienten herbeizufüh-

[50] *Ulsenheimer/Heinemann,* MedR 1999, 200; *Pflüger,* VersR 1999, 1075.

ren. Modernen Informationstechniken wird ein großes Potenzial zur Verbesserung der Qualität und Wirtschaftlichkeit der medizinischen Versorgung zugesprochen. Es werden unterschiedliche Ausbaustufen von E-Health unterschieden, die im Einzelnen die Information, Kommunikation, Interaktion, Transaktion und Integration umfassen. Wearables richten sich dagegen an jeglichen Konsumenten und zielen nicht primär auf die Heilung eines pathologischen Zustands des Nutzers ab. Sie können grundsätzlich jede gesundheitsbewusste Person dabei unterstützen, ihren Gesundheits- und Fitnesszustand zu erhalten oder zu verbessern. Wearables sind in der Regel nicht für das Arzt-Patienten-Verhältnis oder deren Kommunikation vorgesehen.

Die Trennung zwischen diesen beiden Entwicklungsbereichen lässt sich jedoch nicht immer eindeutig vollziehen und es existieren Überschneidungsmöglichkeiten. Bisher wurde der Patient für das Telemonitoring in der Regel mit speziellen Geräten für die Erfassung und Übermittlung von Vitaldaten an den Arzt sowie die Rückmeldungen von ihm an den Patienten ausgestattet. Zukünftig könnten hierfür auch die Smartphones teilweise in Kombination mit Fitnessarmbändern und Smartwatches der Patienten mit entsprechenden Applikationen eingesetzt werden. Diese Anwendungen sind zwar nicht auf medizinische Zwecke ausgerichtet, sie werden aber bereits von vielen Personen eingesetzt und erheben zahlreiche Vitaldaten, wie Blutzucker, Blutdruck, Gewicht oder Pulsfrequenz und Aktivitätsdaten, zum Beispiel gelaufene Schritte pro Tag, und zeichnen sie auf. Es wäre eine kostengünstige Alternative, diese Daten für das Telemonitoring zu verwenden, da hierdurch der Einsatz spezifischer und kostenintensiver Geräte überflüssig werden würde. Insoweit bestehen keine wesentlichen funktionalen Unterschiede der eingesetzten Technik. Eine umfassende Risikobetrachtung erfordert daher, beide Entwicklungsbereiche einzubeziehen.

Durch Telemedizin kann zum einen die Flexibilität der Patienten, vor allem in ländlichen Strukturen und zum anderen die Vermeidung teurer Krankenhausaufenthalte und Behandlungskosten gewährleistet

werden. Der Patient bekommt eine aktivere Rolle und unterliegt weniger Beeinträchtigungen in seiner freien Lebensgestaltung, da insbesondere Krankenhausaufenthalte und Arztbesuche vermieden werden können. Wearables ermöglichen dem Einzelnen mehr Selbstkontrolle über seinen Fitness- und Gesundheitszustand. Aus den Informationen der Wearables können Handlungsempfehlungen abgeleitet werden, wie zum Beispiel Trainingsprogramme oder Ernährungstipps. Ihre Auswertung kann auch Warnungen bei einem zu intensiven Training auslösen, um Überlastungen oder sogar Verletzungen vorzubeugen. Wearables geben dem Nutzer die Möglichkeit, mehr Verantwortung für die eigene Gesundheit zu übernehmen.

Trotz dieser Vorteile ergeben sich durch die neue Technik und ihre vielseitigen Möglichkeiten auch viele datenschutzrechtliche Herausforderungen und Risiken. Allen vorgestellten Anwendungen ist gemeinsam, dass sie in sehr hohem Umfang Fitness-, Vital- und Gesundheitsdaten generieren, die vor dem Hintergrund der Zielsetzung ihrer Verwendung in der Regel personenbezogen sein werden. Insbesondere Fitness- und Gesundheits-Apps greifen regelmäßig auch auf diverse Daten zu, die sie funktional nicht benötigen, sammeln und auswerten, um sie an Dritte unter anderem zu Marketingzwecken weiterzugeben. Nach dem gläsernen Bürger und dem gläsernen Verbraucher könnte nun der Mensch in Bezug auf seinen Fitness- und Gesundheitszustand gläsern werden. Aus diesen Daten lassen sich zudem Gesundheitsprofile erstellen, die tiefe Einblicke in die Lebensgewohnheiten geben sowie als Basis für Prognosen über die zukünftige gesundheitliche Entwicklung und Heilungschancen verwendet werden können. Einzelne Versicherer haben bereits angekündigt, verhaltensbasierte Tarifmodelle einzuführen, die auf der Generierung von Fitness-, Vital- und Gesundheitsdaten aus dem Smartphone, Fitnessarmband und speziellen Apps basieren.[51] Durch solche Geschäftsmodelle könnte ein finanzieller und gesellschaftlicher Anpassungsdruck erzeugt und sie sind mit

[51] S. z.B. Vitality-Programm der Generali, http://www.generali-deutschland.de/online/portal/gdinternet/de/content/311198/1150478.

dem Risiko verbunden, dass das in Deutschland geltende Solidaritätsprinzip im Gesundheitswesen in Frage gestellt wird.

Aber auch bei der Nutzung außerhalb irgendwelcher Bonusprogramme von Versicherungen besteht neben der Skepsis gegenüber einer übertriebenen Selbstoptimierung die Gefahr der zweckwidrigen Verwendung der Fitness- und Gesundheitsdaten. Von Basisfunktionen abgesehen, können in den meisten Fällen die Apps und Wearables ihr volles Potenzial erst durch Netzverbindung und Account-Verknüpfung entfalten, so dass es unvermeidbar ist, die eigenen Gesundheitsdaten an den Server oder die Cloud des Herstellers oder Anwenders, wie zum Beispiel eine Versicherung, zu übermitteln.[52] Hinzu kommen Bedenken in Bezug auf die Sicherheit von Fitness- und Gesundheits-Apps, da sehr häufig mehr oder minder große Sicherheitslücken auftreten und manche Geräte gänzlich unverschlüsselt kommunizieren.[53] An telemedizinische Anwendungen werden deutlich höhere Sicherheitsanforderungen gestellt. Allerdings besteht die Gefahr, dass diese von Fitness- und Gesundheits-Apps verdrängt werden, da diese sich deutlich schneller entwickeln, kostengünstiger und häufig auch bedienungsfreundlicher sind.

Durch den Wandel zum partizipativen und aufgeklärten Patienten kann das persönliche Vertrauensverhältnis zwischen Arzt und Patient nach und nach aufgelöst werden. Das Risiko fehlerhafter Bedienung der Apps, Hypochondrie, laienhafter Selbst- und Fehldiagnosen, schädlicher Behandlungsmaßnahmen sowie verschleppter Krankheiten aufgrund verspäteter Arztbesuche steigt.[54] Es können trotz der qualitativen und schnellen technischen Entwicklung Gefahren für die Gesundheit entstehen, weil davon auszugehen ist, dass eine App einen Arzt nicht ersetzen kann.

---

52 *Janssen*, c't 3/2015, 114 (115).

53 *Störing*, c't 3/2015, 132 (134).

54 S. BfArM, Sicherheitshinweis für iPhone-/Android-Applikation „Pfizer Rheumatology Calculator", Pfizer, 2.11.2011, http://www.bfarm.de/SharedDocs/Kundeninfos/DE/09/2011/4757-11_Kundeninfo_de.html.

1.2 Risiken durch Big Data-Analysen

1.2.1 Big Data

Der Begriff „Big Data" steht seit einigen Jahren für modernste Datenverarbeitungskonzepte denen geradezu „revolutionierende"[55] Wirkungen für die gesamte Gesellschaft zugeschrieben werden. Immer größere Mengen elektronischer Daten über das Verhalten von Menschen, über Dinge und über Naturphänomene stehen zur Verfügung. Der mit jeder neuen IT-Innovation schneller wachsende Datenberg besteht schon jetzt aus den Inhalten der Social Media, aus den Inhalten von E-Mails, aus Telekommunikationsverbindungsdaten, aus Nutzungsdaten von Online-Computerspielen, aus Online-Shopping-Accounts, aus Standortdaten mobiler Dienste, aus Körperdaten, die mit Wearables im Zusammenhang mit Fitness-Übungen oder im Rahmen der Telemedizin (E-Health) erhoben werden. In naher Zukunft werden die Daten vernetzter Autos, von Smart Homes und von ganzen Smart Cities hinzukommen. Von Big Data wird in Fachkreisen aber nicht bei jedem großen Datenaufkommen gesprochen. Groß waren bereits die bisher bekannten Data Warehouses, deren Analyse (Data Mining) aber Strukturierungsaufwand und Zeit in Anspruch nahm und daher aus heutiger Sicht kaum in der Lage war, die eigentlich in den Daten verborgenen Informationen gewinnbringend zu bergen. Von Big Data wird gesprochen, wenn riesige Datenmengen (volume), die in uneinheitlichen Formaten und unstrukturiert vorliegen (variety), in hoher Geschwindigkeit (velocity) wertsteigernd (value) genutzt werden können. Der technische Ansatz von Big Data besteht darin, die Analyse der Daten verteilt und parallel durchzuführen. Cloud Computing und Software für verteiltes Rechnen (zum Beispiel Apache Hadoop) sind hierfür entscheidende Voraussetzungen.[56]

Der Mehrwert entsteht insbesondere dadurch, dass Daten statistisch miteinander korreliert werden können, bei denen dies bisher nicht mit

---

55 *Mayer-Schönberger/Cukier* 2013.

56 *Horvath* 2013; *Steinebach/Halvani/Schäfer/Winter/Yannikos* 2014, 10 ff.

verhältnismäßigem Aufwand oder in der benötigten Geschwindigkeit möglich war. Hierdurch wird es wiederum möglich, in den Daten Muster zu erkennen und Fragen zu beantworten, die bisher nicht beantwortet werden konnten. Da die Fragen in statistischer Weise korrelativ beantwortet werden, können Handlungsstrategien entwickelt werden, ohne dass zwingend die häufig viel schwerer zu klärende Kausalbeziehung zwischen den korrelierten Merkmalen geklärt werden muss. Außerdem entstehen ganz neue Fragestellungen, die eine veränderte Sicht auf die Welt und neue Handlungsstrategien erlauben. Die Mustererkennung erlaubt es, ohne These an einen Datenbestand heranzugehen, also ohne eine Fragestellung Antworten zu erhalten.

Big Data-Analysen ermöglichen es insbesondere, in kürzester Zeit Wahrscheinlichkeitsprognosen für unbekannte Merkmale von Personengruppen und einzelnen Personen und für zukünftige Ereignisse zu erhalten, inklusive des zukünftigen menschlichen Verhaltens und dies so zeitnah (Echtzeit), dass die generierte Information gewinnbringend in Handlungsstrategien einfließen kann.

Big Data kann damit genutzt werden, um besonders intensive von Beginn an personenbezogene Persönlichkeitsprofile für verschiedenste Zwecke zu erstellen, indem „fehlende" Merkmale statistisch prognostiziert werden.

Aber nicht immer wird auf jeden Einzelfall eine komplexe Big Data-Analyse angewendet. Die Big Data-Analyse hat häufig die Funktion, so viel Datenmaterial zu vergleichen, dass statistische Indikatoren für korrelierende Merkmale mit einer gewissen statistischen „Sicherheit" als handlungsleitende Faktoren zur Verfügung gestellt werden können. Diese einzelnen oder wenigen anonymen statistischen Indikatoren, hinter denen die ganze Rechenleistung steckt, dann auf eine Person anzuwenden, ist in der Regel nicht Teil der Big Data-Anwendung, sondern kann je nach Umfang von einem herkömmlichen Rechner oder sogar von einem Mensch erledigt werden. Daher kommt auch das verbreitete Missverständnis, Big Data habe nichts mit personenbezogenen Daten zu tun, da für die Herstellung des Personenbezugs häufig

nicht Big Data erforderlich sei. Die Merkmalsprognose wäre aber ohne Big Data nicht möglich, da die Merkmalsindikatoren fehlen würden.

Die Wurzeln dieser stochastischen Vorhersage von Ereignissen und Verhalten können mindestens bis zu den frühen Arbeiten Norbert Wieners zurückverfolgt werden, dem Begründer der Kybernetik. Dieser hatte bereits in den 40er Jahren Luftabwehrgeschütze automatisiert, indem er die Flugbahnen gegnerischer Piloten, also menschliches Verhalten, mit Hilfe von Statistik und Wahrscheinlichkeitsrechnung voraussagen ließ.[57] Da es sich bei den Big Data-Prognosen um Wahrscheinlichkeitsangaben handelt, stellen sie keine deterministische Vorhersage der Zukunft dar, sondern sie können auch „falsch" liegen. Das heißt, dass zum Beispiel bei einer 85-prozentigen Wahrscheinlichkeit (eine häufig anzutreffende Größenordnung) eines bestimmten Ereignisses sich stattdessen auch die 15-prozentige Wahrscheinlichkeit realisieren kann, dass dieses Ereignis gerade nicht eintritt. In allen Situationen, in denen keine völlige Gewissheit eines Ereignisses notwendig ist, bieten diese Prognosen trotz dieser Unsicherheit eine ausreichende Entscheidungsgrundlage. Insbesondere wenn es nicht darauf ankommt, in jedem einzelnen Fall recht zu behalten, sondern es ausreicht, über viele Fälle hinweg in der Mehrzahl richtig zu liegen, bieten Big Data-Prognosen eine ausreichende Entscheidungsgrundlage im Nichtwissen.

Big Data-Prognosen ermöglichen außerdem eine Reduktion von Komplexität. Sie brechen die möglichen Merkmale und Verhaltensweisen von Menschen oder Zustände von Dingen auf eine binäre Antwort für eine spezifische Frage herunter (zum Beispiel: „Wird diese Person die X-Partei wählen?"). Eigentlich unklare Zustände werden in (ausreichend) klare Zustände verwandelt, in (näher) Null oder (näher) Eins. Durch diese binäre Reduktion des Möglichkeitsraums werden die prognostizierten Merkmale, Zustände und Verhaltensweisen von Menschen außerdem maschinenverarbeitbar.

---

57 *Wiener* 1962, 208 ff.

Die Einsatzfelder für Big Data sind zahlreich. Das Konzept kann zur Effizienzsteigerung in der Industrie eingesetzt werden, zur simulationsbasierten Forschung, zur Vorhersage von Epidemien, zur Effizienzsteigerung und individualisierten Therapie in der Medizin, zur feinkörnigen bis individuellen Voraussage von Wählerverhalten für politische Kampagnen oder zum Erkennen kognitiver Zustände von Menschen für gezieltes Marketing oder für die Selbstoptimierung. Big Data wird überdies voraussichtlich eine große Rolle dabei spielen, im Rahmen von Smart Home und vernetztem Straßenverkehr menschliche Zustände und die Zustände von Dingen in Echtzeit ausreichend zuverlässig zu bestimmen, um situativ passende Dienste anzubieten. Big Data stellt also kein von den drei untersuchten smarten Informationstechniken scharf abzugrenzendes Themenfeld dar, sondern spielt vielmehr in ihnen eine wichtige Rolle.

Auch im Sicherheitsbereich wird Big Data angewendet. Merkmale bekannter Täter werden analysiert und mit den Daten von Bürgern abgeglichen, um anhand von erkannten Mustern mögliche zukünftige Täter zu identifizieren. Eine aktuell besprochene Ausprägung im Sicherheitsbereich ist auch das „Predictive Policing", bei dem sich die Aussage über zukünftige Straftaten sowohl auf bestimmte Orte und Tageszeiten (wird derzeit in Deutschland in mehreren Bundesländern erprobt[58]) als auch auf die zukünftigen Handlungen einzelner Personen beziehen kann (in den USA bereits im Einsatz[59]). Die Profilbildung im Sicherheitsbereich ist allerdings ein Gebiet, in dem es gerade nicht relativ unerheblich ist, dass es sich bei statistischen Korrelationen um Wahrscheinlichkeitsprognosen handelt, die in manchen Fällen zu einer Falschbewertung führen können. Wird ein Mensch fälschlicherweise als potentieller Attentäter eingeordnet, weil die höhere Wahrscheinlichkeit es nahelegt, kann dies für ihn zu erheblichen Freiheitseingriffen führen. Wird ein Mensch fälschlicherweise nicht als potentieller Attentäter eingeordnet, wiederum weil die höhere Wahrscheinlichkeit

58 *Monroy* 2015; *Gluba* 2014.
59 *Rieke/Robinson/Yu* 2014, 18f.

es nahelegt, kann es zu einem erfolgreichen Attentat kommen. Hier käme es für den Grundrechtsschutz in beiden Fällen nicht auf die richtige Bewertung in der Mehrzahl der Fälle an, sondern auf die richtige Bewertung in jedem einzelnen Fall. Dies kann Big Data allein aber nicht bieten.

1.2.2 Big Data: Personenbezogen oder anonym?

Big Data-Analysen können grundsätzlich mit personenbezogenen Daten oder mit anonymen Daten durchgeführt werden. Diese beiden Konstellationen werden im Folgenden, soweit möglich auseinandergehalten, um die rechtlichen Unterschiede zu verdeutlichen. Grundsätzlich ist der Umgang mit nicht personenbezogenen Daten nicht vom Datenschutzrecht erfasst und daher weitgehend frei zulässig. Allerdings darf, wie bereits angedeutet, dabei nicht übersehen werden, dass eine anonyme Generierung von Merkmalsindikatoren plötzlich in ein sehr intensives Persönlichkeitsprofil umschlagen kann.

Hieraus ergibt sich die besondere Herausforderung von Big Data für das Datenschutzrecht, die schon hier einmal vorweggenommen werden soll. Wird Big Data durchgehend mit personenbezogenen Daten durchgeführt, wird es in den meisten Fällen dem Datenschutzrecht widersprechen, so dass es sich aus Sicht des Rechts um ein Durchsetzungsdefizit oder einen Anpassungsdruck an die soziotechnische Entwicklung handelt. Werden aber Daten ohne Personenbezug erhoben (Wetterdaten, kollektive Wahlprognosen) oder werden personenbezogene Daten nach der Erhebung anonymisiert, unterliegt ihre Analyse keinen datenschutzrechtlichen Einschränkungen. Dennoch wird in diesem Verarbeitungsabschnitt ein intensives Risiko für die informationelle Selbstbestimmung der (potentiellen zukünftigen) Betroffenen geschaffen, denn anonyme statistische Analysen über das Verhalten von Gruppen mit bestimmten Merkmalen können anhand dieser Merkmale plötzlich auf Individuen übertragen werden. In diesem Modell davon zu sprechen, dass Big Data nur anonyme Daten verarbeitet, ist zwar formal korrekt, übersieht aber die möglichen Auswir-

kungen der Analyseergebnisse. Der Personenbezug geschieht in diesem Modell nicht, wie beim klassischen Persönlichkeitsprofil, zu Beginn, sondern am Ende der Datenverarbeitung. Es wird, um es bildlich auszudrücken keine Akte über eine bestimmte Person geführt, sondern es gibt eine Vielzahl dynamischer anonymer Akten, die in einem Augenblick auf eine bestimmte Person konkretisiert werden können. Auf menschliches Verhalten gerichtete anonyme Big Data-Analysen sollten nicht unabhängig von personenbezogener Anwendung betrachtet werden, denn sie bieten für diese die physiologische und psychologische Grundlagenforschung. Außerdem darf auch nicht übersehen werden, dass Big Data selbst nicht nur zur Merkmalsgenerierung eingesetzt werden kann, sondern auch dazu, einen Personenbezug herzustellen und anonyme Daten zu deanonymisieren.[60] Nicht nur die Intensität der Persönlichkeitsprofile, sondern auch die Wahrscheinlichkeit des Personenbezugs steigt damit in einer Big Data-Umgebung. Hierdurch wird es fraglich, ob es noch risikoadäquat erscheint, den Umgang mit anonymen Daten gar nicht datenschutzrechtlich zu regulieren.

1.2.3 Big Data-Analysen mit personenbezogenen Daten

Big Data erlaubt es, Daten aus verschiedensten Quellen wesentlich leichter zu kombinieren als bisher. Diese Daten können aus unterschiedlichsten sozialen Zusammenhängen stammen und zu völlig unterschiedlichen Zwecken erhoben worden sein. Handelt es sich um personenbezogene Daten, stellt dies in aller Regel einen klaren Verstoß gegen das datenschutzrechtliche Zweckbindungsprinzip dar.[61] Hierdurch kann das in der informationellen Selbstbestimmung enthaltene Recht der Betroffenen, selbst zu entscheiden, welche Lebenssachverhalte wem gegenüber offenbart werden und welche nicht,[62] stark gefährdet werden. Durch die Kombination von Informationen, die die Betroffenen versuchen, separat zu halten, wird es erschwert, unter-

60 Ausführlich *Roßnagel*, ZD 2013, 562 (563).
61 S. hierzu unten Kap. 2.3.1.
62 S. *BVerfGE* 65, 1 (41 ff.).

schiedliche soziale Rollen überhaupt noch integer einzunehmen und aufrecht zu erhalten.[63] Dieses Risiko entsteht zwar nicht erst mit Big Data, wird aber durch die Möglichkeit, heterogene Daten effizienter und in hoher Geschwindigkeit miteinander zu verknüpfen, deutlich verschärft.

Überdies besteht durch die Anwendung von Big Data auf Daten aus verschiedensten Zusammenhängen ein stark ansteigendes Risiko der Deanonymisierung eigentlich gar nicht personenbezogener Daten. Das Datenschutzrecht ist anwendbar auf personenbezogene Daten. Das Gegenstück zu personenbezogenen Daten stellen anonyme Daten gemäß § 3 Abs. 6 BDSG dar. Auf anonyme Daten ist das Datenschutzrecht nicht anwendbar. Für die Bewertung, ob ein Datum als personenbezogen oder anonym anzusehen ist, spielt das für die jeweilige verantwortliche Stelle mit verhältnismäßigem Aufwand zu erlangende (Zusatz-) Wissen die zentrale Rolle. Big Data-Analysen können durch ihre hohe Rechenleistung und durch den Zugriff auf verschiedenste Datenquellen den zur Deanonymisierung erforderlichen Aufwand deutlich senken, indem sie weiteres Wissen verfügbar werden lassen. Sie stellen daher das Konzept der Anonymisierung wenn nicht generell, so doch in vielen bisher als anonym bewerteten Situationen in Frage.

Big Data eröffnet wie keine andere Technik zuvor die Möglichkeit, persönliche Merkmale und menschliches Verhalten zu prognostizieren. So können zum Beispiel aus dem Vergleich des Like Button-Verhaltens verschiedener Facebook-Nutzer politische Einstellungen prognostiziert werden.[64] Anhand der Tippdynamik auf dem Smartphone kann statistisch auf den aktuellen Gemütszustand geschlossen werden.[65] Letzteres gelingt auch mit biometrischen Kamerasystemen.[66] Die jeweils fehlenden Merkmale werden dabei durch statistische Ver-

63 S. *Ochs* 2015, 178.
64 *Theile* 2013.
65 *Christl* 2014, 21 f.
66 *Voigt* 2015.

gleiche mit anderen Menschen mit genügend übereinstimmenden anderen Merkmalen in Form von Wahrscheinlichkeitsaussagen prognostiziert.

Diese besonders tiefen und besonders aktuellen Persönlichkeitsprofile bieten die Möglichkeit, Willensentscheidungen und Handlungen der analysierten Person wiederum in engem zeitlichem Zusammenhang („in Echtzeit") zu beeinflussen. Das prominenteste Beispiel für solche Beeinflussungstechniken ist der US-Präsidentschaftswahlkampf 2012. Dort gelang es, für die einzelnen Wahlberechtigten Prognosen ihres ganz individuellen Wahlverhaltens zu errechnen. Daraufhin wurden individuelle Prognosen abgegeben, wie leicht und mit welchen Methoden es möglich wäre, einzelne Personen davon zu überzeugen, ihre prognostizierte Überzeugung zu ändern. Außerdem wurde in sozialen Netzwerken im Freundeskreis der jeweiligen Wahlberechtigten nach geeigneten Trägern dieser maßgeschneiderten Botschaften gesucht. Mit diesem Wissen ausgestattet, wurden dann jene Wahlberechtigten bearbeitet, bei denen eine hohe Wahrscheinlichkeit bestand, dass sie zu überzeugen wären. Man verschwendete also keinen Aufwand auf schwierige oder hoffnungslose Fälle.[67] Big Data lässt derartige, auf den Einzelnen maßgeschneiderte Beeinflussungsstrategien praktikabel, effizient und hochgradig skalierbar werden.

Neben der politischen Beeinflussung ergeben sich auch eine viele kommerzielle Anwendungen, insbesondere im Bereich der Werbung. Erkennt ein Smartphone zum Beispiel, dass sein Nutzer sich gerade in einer euphorischen Stimmung befindet, bietet dieses Wissen die Möglichkeit, ihm passgenau in diesem Moment Werbung und eine Bestellmöglichkeit für etwas einzublenden, von dem man vermutet, dass der Nutzer es mögen könnte. Big Data hilft also zu erkennen, wann bei einem bestimmten potentiellen Kunden (oder Wähler) besonders wenige hemmende Faktoren für eine erwünschte Willensentscheidung

---

[67] Ausführlich zum US-Wahlkampf *Richter*, DÖV 2013, 961.

vorliegen und wie sich solche Faktoren bei diesem Individuum umgehen lassen.

Während im Volkszählungsurteil schon das auch weiterhin relevante Risiko erkannt wurde, Menschen könnten ihr Verhalten in vorauseilendem Gehorsam der Konvention anpassen, wenn sie nicht wüssten, wer was über sie weiß,[68] kommt mit derartigen Big Data-Anwendungen die direkte gezielte und automatisierte Beeinflussung von einzelnen konkreten Entscheidungen in massiv skalierbarem Ausmaß hinzu. Hierdurch ist die in Art. 2 Abs. 1 GG verbürgte Willens- und Handlungsfreiheit direkt und nicht erst über den Umweg des „Chilling Effects" beeinträchtigt. Aus der Ferne und automatisierbar kann mit Informationsimpulsen direkt und im vielversprechendsten Augenblick in den Prozess der individuellen Willensbildung eingegriffen werden.

1.2.4 Big Data-Analysen ohne personenbezogene Daten

Die Prognose von Persönlichkeitsmerkmalen und von menschlichem Verhalten kann aber auch dann verhaltenssteuernd wirken, wenn die Statistik an sich anonym bleibt und die Herstellung des Personenbezugs nicht durch Datenverarbeitungsanlagen, sondern nur im Alltag durch Menschen erfolgt. Wird beispielsweise prognostiziert, dass Personen mit bestimmten leicht erkennbaren äußerlichen Merkmalen mit 85 Prozent Wahrscheinlichkeit unzuverlässige Arbeitnehmer sind, kann dies einen erheblichen Konformitätsdruck erzeugen. Um nicht unter die Prognose zu fallen, müsste ein Bewerber dafür sorgen, dass er die schicksalhaften äußerlichen Merkmale an sich selbst tilgt. In diesem Zusammenhang ist also dann der Problemkreis des „Chilling Effect" berührt.

Ähnlich verhält es sich beim Predictive Policing. Häufig wird argumentiert, es werde nur errechnet, an welchen Orten zu welchen Zeiten Einbrüche stattfinden werden. Personenbezogene Daten würden nicht

[68] *BVerfGE* 65, 1 (43).

verarbeitet.[69] Dies ist formal zutreffend. Die Datenverarbeitungsanlage stellt keinen Personenbezug her. Der Personenbezug wird aber von der menschlichen Polizeistreife in dem Augenblick hergestellt, indem sie ihren statistischen Verdacht, dass es aktuell einen Straftäter gibt, auf Personen überträgt, die zu diesem Profil (Zeit und Ort) passen.

Bei Big Data (und Statistik im Allgemeinen) kann die Analyse der Korrelation von Merkmalen tatsächlich anonym geschehen. Es wird nicht ein personenbezogenes Profil erstellt und nach und nach mit Daten angereichert. Stattdessen werden ohne Personenbezug Muster analysiert und einzelne Merkmale oder kleine Kombinationen von Merkmalen mit erwünschten oder unerwünschten Eigenschaften verknüpft. Personenbezug wird erst in dem Augenblick hergestellt, in dem etwa ein Arbeitgeber der die Statistik kennt, im Bewerbungsgespräch die Merkmale am Gegenüber erkennt und also das bis dahin anonyme Profil auf diesen überträgt. Dieser Personenbezug findet im Kopf des Arbeitgebers statt.

Zwar entsteht auch dieses Risiko nicht erst mit Big Data. Auch bisher wenden Menschen Vorurteile auf Menschen an. Indem durch Big Data aber immer weitere Persönlichkeitsmerkmale zu günstigen oder ungünstigen (anonymen) Indikatoren für andere Merkmale werden, und diese Merkmale nicht auf reinen menschlichen Vorurteilen, sondern auf mathematischen Berechnungen von Computern beruhen, könnte sich der gesellschaftliche Konformitätsdruck deutlich verschärfen.

---

[69] *Borchers* 2015.

2 Risikoschutz durch geltendes Datenschutzrecht?

Im Folgenden wird die Frage untersucht, ob das geltende Datenschutzrecht geeignet ist, die Risiken für die informationelle Selbstbestimmung durch moderne Informationstechniken angemessen zu reduzieren und das Datenschutzniveau zu erhalten. Dieser Untersuchung bezieht sich zum einen auf die allgemeinen Regelungen des geltenden Datenschutzrechts zur Zulässigkeit der Datenverarbeitung, zu den Prinzipien im Umgang mit personenbezogenen Daten. Zum anderen erfolgt eine datenschutzrechtliche Bewertung der drei beispielhaften „smarten" Informationstechniken für den Alltag und der beiden Big-Data-Anwendungen am Maßstab des geltenden Datenschutzrechts.

2.1 Europäisches Datenschutzrecht

Zuerst wird untersucht, welche Regelungen und Maßstäbe das Unionsrecht bietet. Dabei wird im ersten Schritt die Grundrechtecharta als relevanter Teil des Unionsprimärrecht betrachtet und im zweiten Schritt dann die Datenschutzrichtlinie als bedeutendste Regelung des Datenschutzrechts im Sekundärrecht der Union.

2.1.1 Grundrechtecharta

In der Charta der Grundrechte der Europäischen Union (GRCh) vom 7. Dezember 2000[70] hat die Europäische Union zum ersten Mal umfassend Grund- und Menschenrechte kodifiziert.[71] Sie erlangte mit dem Inkrafttreten des Vertrags von Lissabon[72] zum 1. Dezember 2009

[70] Derzeit gültig ist die Fassung vom 26.10.2012, ABl. C 326/391.

[71] „Sie vereint in einem einzigen Text alle in der Union geschützten Grundrechte." Mitteilung der Kommission, Strategie zur wirksamen Umsetzung der Charta der Grundrechte durch die Europäische Union, 19.10.2010, KOM(2010) 573 endg., 3. Diese und andere Erläuterungen zur Charta haben zwar keinen rechtlichen Status, sind jedoch nach Art. 52 Abs. 7 GRCh „gebührend zu berücksichtigen".

[72] Vertrag von Lissabon zur Änderung des Vertrags über die Europäische Union und des Vertrags zur Gründung der Europäischen Gemeinschaft, unterzeichnet in Lissabon am 13.12.2007, ABl. C 306, 1.

Rechtskraft. Die Charta ist rechtlich verbindlich.[73] Aufgrund der Verweisung in Art. 6 Abs. 1 EUV steht sie auf einer Stufe mit dem Vertrag über die Europäische Union (EUV) und dem Vertrag über die Arbeitsweise der Europäischen Union (AEUV)[74] und ist damit Teil des EU-Primärrechts.[75] „Mit dem Inkrafttreten des Vertrags von Lissabon hat die Europäische Union damit nicht nur einen vollwertigen, in Geltung stehenden Grundrechtskatalog erhalten, sondern ist jetzt mit einem pluralen Regime sich gegenseitig verstärkender Grundrechtsquellen ausgestattet."[76] Nach Art. 51 Satz 1 CRCh gilt die Charta „für die Organe und Einrichtungen der Union unter Einhaltung des Subsidiaritätsprinzips und für die Mitgliedsstaaten ausschließlich bei der Durchführung des Rechts der Union". Dazu gehört auch solches mitgliedsstaatliche Handeln, das lediglich in den Geltungsbereich des Unionsrechts fällt, was in einer Einzelfallprüfung festgestellt werden muss.[77] In den Erläuterungen zur Charta heißt es: „Die Charta findet keine Anwendung bei Grundrechtsverletzungen, die keinen Bezug zum Unionsrecht aufweisen. Die Mitgliedstaaten haben eigene Systeme zum Schutz der Grundrechte durch die nationalen Gerichte, an deren Stelle nicht die Charta tritt."[78]

Die im Kontext des Datenschutzes und der dargestellten technologischen Herausforderungen primär relevanten Rechte der Charta finden sich in Art. 7 und 8 GRCh.

---

73 *Esser*, in: Löwe/Rosenberg 2012, Bd. 11, EMRK/IPBPR Einf., Rn. 135.

74 Diese enthalten ebenfalls Bestimmungen zum Datenschutz, nämlich in Art. 39 EUV und Art. 16 AEUV.

75 S. auch KOM(2010) 573 endg., 3: „Mit dem Vertrag von Lissabon wurden die in der Charta verankerten Rechte, Freiheiten und Grundsätze anerkannt und dieser dieselbe Rechtsverbindlichkeit wie den Verträgen verliehen."

76 *Wehlau/Lutzhöft*, EuZW 2012, 45 (50). Es ergibt sich beispielsweise für Deutschland eine vierfache Absicherung, nämlich durch die GRCh, die EMRK, das GG und die jeweilige Landesverfassung.

77 *EuGH*, Urteil vom 26.2.2013, Rs. C-617/10.

78 KOM(2010) 573 endg., 11.

Art. 7 GRCh ist weitestgehend wortgleich[79] mit Art. 8 Abs. 1 EMRK und gesteht jeder Person ein „Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung und ihrer Kommunikation" zu. Art. 7 GRCh ist damit in vier Bereiche unterteilt. „Der Begriff des Privatlebens entzieht sich dem Versuch einer allgemeingültigen Definition. Jedenfalls versteht das Europäische Gericht für Menschenrechte unter dem Recht auf Achtung des Privatlebens mehr als ein bloßes ‚right to be let alone'. In einem weiten Sinne sind alle Bereiche des Lebens, die andere nicht betreffen, der Privatsphäre zuzuordnen."[80] Damit wird klar, dass anders als durch Art. 2 Abs. 1 GG keine allgemeine Handlungsfreiheit ermöglicht werden soll.[81] Beim Recht auf Achtung des Privatlebens handelt es sich dennoch um ein weit gefasstes Grundrecht; neben dem Schutz persönlicher Daten umfasst es auch den Schutz der physischen wie psychischen Integrität einer Person, sofern diese nicht bereits durch andere Rechte erfasst sind.[82] In ihm spiegelt sich unter anderem „die liberale Idee der Selbstbestimmung wider".[83] Die Art. 7 GRCh entsprechende Grundrechtsschranke ist entsprechend der Rückgriffsregelung des Art. 52 Abs. 3 GRCh Art. 8 Abs. 2 EMRK zu entnehmen. Danach ist ein Eingriff insbesondere dann gerechtfertigt, wenn er „notwendig ist für die nationale oder öffentliche Sicherheit, für das wirtschaftliche Wohl des Landes, zur Aufrechterhaltung der Ordnung, zur Verhütung von Straftaten, zum Schutz der Gesundheit oder der Moral oder zum Schutz der Rechte und Freiheiten anderer".

---

79 Mit Ausnahme der Ersetzung des Wortes „Korrespondenz" durch „Kommunikation", die der fortschreitenden technischen Entwicklung geschuldet ist. Dok. CHARTE 4487/00 CONVENT 50, 10. *Nettesheim*, in: Grabenwarter 2014, § 9, Rn. 17.

80 *Bernsdorff*, in: Meyer 2014, Art. 7 GRCh, Rn. 19. So auch *Meyer-Ladewig* 2011, Art. 8 EMRK, Rn. 7: „Der Begriff wird umfassend verstanden und ist einer abschließenden Definition nicht zugänglich."

81 *Bernsdorff*, in: Meyer 2014, Art. 7 GRCh, Rn. 15.

82 *EGMR*, Fall S und Marper vs. Vereinigtes Königreich, Urteil vom 4.12.2008 – 30562/04 und 30566/04; *Bernsdorff*, in: Meyer 2014, Art. 7 GRCh, Rn. 19.

83 *Nettesheim*, in: Grabenwarter 2014, § 9, Rn. 3.

Art. 8 Abs. 1 GRCh begründet ein Recht auf Schutz personenbezogener Daten und ist lex specialis gegenüber Art. 7 GRCh.[84] Art. 8 Abs. 2 Satz 1 GRCh enthält eine Präzisierung des Schutzes, wonach Daten „nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden" dürfen. Somit muss die Datenverarbeitung einem legitimen Zweck dienen und verhältnismäßig sein. Das Gebot der Verhältnismäßigkeit der Datenverarbeitung manifestiert sich in dem Prinzip der Datenvermeidung oder Datensparsamkeit.[85] Dabei meint Verarbeitung personenbezogener Daten jegliche Verwendung der Daten vom Zeitpunkt der Erhebung an. Art. 8 Abs. 2 Satz 2 GRCh erweitert den Schutz noch um ein Auskunfts- und Berichtigungsrecht. Art. 8 GRCh stützt sich auf das europäische Sekundärrecht zum Datenschutz.[86] Dieses enthält bereits umfangreiche Regelungen zum Datenschutz, weshalb nur wenige Bereiche verbleiben, in denen das Datenschutzrecht des Art. 8 GRCh keine Anwendung findet.[87] Demnach ist für die Zulässigkeit eines Eingriffs in das durch Art. 8 Abs. 1 GRCh begründete Recht auf das europäische Sekundärrecht zum Datenschutz zu verweisen.[88] Art. 8 GRCh kann zusammenfassend als eine Zusammenfassung des geltenden europäischen Datenschutzrechts verstanden werden.

Art. 52 Abs. 1 GRCh enthält als „allgemeine Einschränkungsklausel" die Voraussetzungen, unter denen Rechte aus der Charta eingeschränkt werden können.[89] Danach muss jede Einschränkung unter Beachtung des Verhältnismäßigkeitsgrundsatzes „gesetzlich vorgesehen sein und den Wesensgehalt dieser Rechte und Freiheiten achten".

---

84 Auch Art. 16 Abs. 1 AEUV enthält ein Recht auf Datenschutz. Dieses ist als Wiederholung von Art. 8 GRCh zu verstehen, so dass die Regelungen des Art. 8 Abs. 2 und 3 sowie 52 Abs. 1 GRCh auch für Art. 16 AEUV gelten. *Sobotta*, in: Grabitz/ Hilf/Nettesheim 2015, Art. 16 AEUV, Rn. 8.

85 *Sobotta*, in: Grabitz/Hilf/Nettesheim 2015, Art. 16 AEUV, Rn. 8.

86 S. hierzu die Darstellung in Kap. 5.8.

87 *Sobotta*, in: Grabitz/Hilf/Nettesheim 2015, Art. 16 AEUV, Rn. 14.

88 *Bernsdorff*, in: Meyer 2014, Art. 8 GRCh, Rn. 17.

89 *Lenaerts*, EuR 2012, 3 (7).

Bei Grundrechten, die denen der Europäischen Menschenrechtskonvention entsprechen, regelt Art. 52 Abs. 3 GRCh jedoch davon abweichend, dass auf die jeweilige Schrankenregelung der Konvention Rückgriff zu nehmen ist. Bei der Auslegung der Grundrechtecharta kann daher auch auf Urteile des Europäischen Gerichts für Menschenrechte zurückgegriffen werden. Der durch die Grundrechtecharta garantierte Schutz darf folglich niemals hinter dem durch die Konvention garantierten zurückbleiben.[90]

Ferner ist bei der Ausübung der beschriebenen Grundrechte ein Ausgleich mit den Grundrechten eines privaten Datenverarbeiters im Sinn eines Interessenausgleichs zu suchen.[91] Die Datenverarbeitung durch einen Privaten stellt ebenfalls eine Ausübung von Grundrechten dar. Hier ist insbesondere an die in Art. 15 bzw. 16 GRCh enthaltene Berufsfreiheit und die unternehmerische Freiheit zu denken, aber auch an die Freiheit der Meinungsäußerung und die Informationsfreiheit aus Art. 11 GRCh.

Als Auslegungshilfe für den europäischen wie auch den nationalen Gesetzgeber wurde eine Grundrechts-Checkliste veröffentlicht.[92] Sie dient als Hilfe zur Anwendung der Charta über die Vorgaben des Art. 52 GRCh hinaus und ist für die Ex-ante-Kontrolle von Gesetzgebungsakten von Relevanz.[93] Als weitere Auslegungshilfe für die Grundrechte der Charta, als „Erkenntnisquelle für die Gewinnung von Grundrechten und deren Auslegung“,[94] dienen nach Art. 52 Abs. 4 GRCh die „gemeinsamen Verfassungsüberlieferungen der Mitgliedsstaaten“.

---

90 *Lenaerts*, EuR 2012, 3 (12).

91 S. z.B. *EuGH*, Urteil vom 9.11.2010, Rs. C‑92/09 und C‑93/09, Rn. 48: „Das Recht auf Schutz der personenbezogenen Daten kann jedoch keine uneingeschränkte Geltung beanspruchen, sondern muss im Hinblick auf seine gesellschaftliche Funktion gesehen werden.“

92 KOM(2010) 573 endg., 6.

93 *Wehlau/Lutzhöft*, EuZW 2012, 45 (46).

94 *Schwarz*, Der Staat 2011, 533 (536).

2.1.2 Datenschutzrichtlinie

Die europäische Datenschutzrichtlinie (DSRL)[95] trat im Dezember 1995 in Kraft. Ihre Umsetzung in nationales Recht durch die Mitgliedstaaten der Europäischen Gemeinschaft hatte bis Ende Oktober 1998 zu erfolgen.[96] Die entsprechenden Anpassungen deutschen Rechts erfolgten jedoch erst im Jahr 2001. Ziel der Richtlinie war vor allem die Herstellung eines europaweit einheitlichen Datenschutzniveaus, um die als Handelshindernis im freien Verkehr von Waren, Personen, Dienstleistungen und Kapital empfundenen Differenzen im Datenschutzniveau der Mitgliedsstaaten bei der Verarbeitung personenbezogener Daten zu reduzieren[97] und den europäischen Binnenmarkt zu stärken.[98] Hierzu sollte die Datenschutzrichtlinie sowohl für den nichtöffentlichen wie auch für den öffentlichen Bereich einen verbindlichen Standard, ein „gleichwertiges Schutzniveau"[99] schaffen. Die Frage, ob die Datenschutzrichtlinie eine Voll- oder Mindestharmonisierung darstellt, hat der Europäische Gerichtshof 2011 zugunsten der Vollharmonisierung entschieden.[100] Der nationalstaatliche Spielraum bei der Umsetzung „ergibt sich aus den allgemeinen Rechtsbegriffen, Ausnahmemöglichkeiten und Optionen sowie einigen speziellen Regelungsaufträgen, die in der Datenschutzrichtlinie 95/46/EG selbst angelegt sind".[101] Ergänzt wurde die Datenschutzrichtlinie vor allem

---

95 Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24.10.1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. L 281, 31.

96 Heute gilt die Datenschutzrichtlinie für die 28 Mitgliedstaaten der EU sowie Liechtenstein, Norwegen und Island, die ebenfalls Teil des Europäischen Wirtschaftsraums sind.

97 S. Erwägungsgründe 7 bis 9 DSRL. Der Erlass der Datenschutzrichtlinie war entsprechend auf Art. 100a des EG-Vertrags gestützt – s. *EuGH*, Urteil vom 20.5.2003, Rs. C-465/00, Rn. 39.

98 S. Erwägungsgründe 3 bis 5 DSRL.

99 Erwägungsgrund 8 DSRL.

100 *EuGH*, Urteil vom 24.11.2011, Rs. C‑468/10 und C‑469/10; s. auch Urteil vom 6.11.2003, Rs. C-101/01 und Urteil v. 16.12.2008, Rs. C-524/06.

101 *Brühann*, EuZW 2009, 639 (642).

durch die Richtlinie 2002/58/EG,[102] die als ein Versuch verstanden werden kann, erkannten Defiziten der Richtlinie für den Bereich der elektronischen Kommunikation zu begegnen.[103]

Personenbezogene Daten sind nach Art. 2 lit. a) DSRL „alle Informationen über eine bestimmte oder bestimmbare natürliche Person". Eine Verarbeitung findet nach Art. 2 lit. b) DSRL statt durch „jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede Vorgangsreihe im Zusammenhang mit personenbezogenen Daten".

Der Anwendungsbereich der Datenschutzrichtlinie ist jedoch nicht umfassend. Art. 3 Abs. 2 DSRL formuliert Ausnahmen von ihrer Anwendung. Ihr Anwendungsbereich ist auf die Ausübung von Tätigkeiten, die in den Anwendungsbereich von Unionsrecht fallen, beschränkt.[104] Ferner findet die Datenschutzrichtlinie keine Anwendung bei ausschließlich persönlichen oder familiären Tätigkeiten.[105] Eine weitere Ausnahme enthält Art. 3 Abs. 2 DSRL. Dieser stellt klar, dass die Richtlinie „auf keinen Fall auf Verarbeitungen betreffend die öffentliche Sicherheit, die Landesverteidigung, die Sicherheit des Staates […] und die Tätigkeiten des Staates im strafrechtlichen Bereich" Anwendung findet.

Art. 6 Abs. 1 DSRL enthält „Grundsätze in Bezug auf die Qualität der Daten". Dies sind Treu und Glauben, die Rechtmäßigkeit der Verarbeitung, Zweckbindung und Erheblichkeit, sachliche Richtigkeit und Datenaktualität sowie Bindung der Höchstspeicherdauer an die Zweckerreichung. Eine Verarbeitung personenbezogener Daten ist nur unter den Voraussetzungen des Art. 7 DSRL zulässig. Danach ist die Zulässigkeit der Verarbeitung entweder von der ausdrücklichen und in-

---

[102] Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12.7.2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation.

[103] Zu den Defiziten der Richtlinie s. Kap. 3.3.

[104] *Ehmann/Helfrich* 1999, Art. 3 DSRL, Rn. 17.

[105] *Ehmann/Helfrich* 1999, Art. 3 DSRL, Rn. 22; *Simitis*, in: Simitis 2014, Einf. BDSG, Rn. 224.

formierten Zustimmung[106] des Betroffenen oder dem Vorliegen eines anderen Erlaubnistatbestands abhängig. Hierzu gehört die Erforderlichkeit „für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist", für die „Erfüllung einer rechtlichen Verpflichtung", für die „Wahrung lebenswichtiger Interessen der betroffenen Person", für die „Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt" und für die Verwirklichung eines berechtigten Interesses.

Art. 8 Abs. 1 DSRL benennt schließlich besondere Kategorien personenbezogener Daten. Die Verarbeitung von Daten, die Auskunft über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen oder die Zugehörigkeit zu einer Gewerkschaft, die Gesundheit oder das Sexualleben geben, ist untersagt.[107] Art. 8 Abs. 2 DSRL enthält jedoch Ausnahmen von diesem Grundsatz.

Dem Betroffenen gegenüber hat die datenverarbeitende Stelle nach Art. 10 und 11 DSRL eine Informationspflicht. Informationspflichten gegenüber der betroffenen Person sind von zentraler Bedeutung, damit die Person wissen kann, „wer was wann und bei welcher Gelegenheit über sie weiß"[108]. Umgekehrt stehen dem Betroffenen der datenverarbeitenden Stelle gegenüber Rechte zu. Nach Art. 12 DSRL hat der Betroffene ein Auskunftsrecht in Form eines Rechts auf die Bestätigung, ob und welche ihn betreffenden Daten verarbeitet werden,[109] weiterhin ein Recht auf Berichtigung, Löschung oder Sperrung personenbezogener Daten.[110] Ein gegen die Datenverarbeitung gerichtetes

---

106 *Ehmann/Helfrich* 1999, Art. 7 DSRL, Rn. 12 ff.

107 *Ehmann/Helfrich* 1999, Art. 8 DSRL, Rn. 8. Zu den Ausnahmetatbeständen siehe *Ehmann/Helfrich* 1999, Art. 8 DSRL, Rn. 14 ff.

108 *BVerfGE* 65, 1 (43).

109 S. auch Erwägungsgrund 41 DSRL.

110 *Ehmann/Helfrich* 1999, Art. 12 DSRL, Rn. 52 ff.

Widerspruchsrecht ergibt sich in bestimmten Fällen[111] aus Art. 14 DSRL.

Nach Maßgabe von Art. 13 DSRL können die in den Artikeln 6 Abs. 1, 10, 11 Abs. 1 und 12 DSRL enthaltenen Grundsätze jedoch eingeschränkt werden, wenn dies zu einem der dort beschriebenen Zwecke notwendig ist. Dies sind die „Sicherheit des Staates, die Landesverteidigung, die öffentliche Sicherheit", die Bekämpfung von Straftaten und Verstößen gegen berufsständische Regeln, wichtige wirtschaftliche oder finanzielle Interessen, damit verbundene „Kontroll- Überwachungs- und Ordnungsfunktionen" und der „Schutz der betroffenen Person und die Rechte und Freiheiten anderer Personen".

Die Zulässigkeit automatisierter Einzelentscheidungen wird durch Art. 15 DSRL begrenzt,[112] während Art. 16 und 17 DSRL schließlich Vorgaben für die Vertraulichkeit und Sicherheit der Datenverarbeitung in Form der Einrichtung üblicher Standardmaßnahmen enthalten.[113] Weiterhin normiert Art. 18 DSRL eine Pflicht zur Meldung bestimmter Verarbeitungen an eine Kontrollstelle.[114]

Die Übermittlung von Daten an Drittstaaten, die nicht über ein angemessenes Schutzniveau verfügen, ist nach Art. 25 Abs. 1 und 4 DSRL ferner auf bestimmte Ausnahmesituationen beschränkt.[115] Eine pauschalisierte Erklärung zur Angemessenheit des Schutzes in einem Drittstaat, wie sie in der Safe Harbour-Entscheidung[116] enthalten war, ist nach dem Urteil des Europäischen Gerichtshofs vom 6. Oktober

---

111 Nämlich in den Fällen einer Verarbeitung im Sinne von Art. 7 lit. e) und f) DSRL. S. hierzu detailliert *Ehmann/Helfrich* 1999, Art. 14 DSRL, Rn. 6 ff.

112 *Ehmann/Helfrich* 1999, Art. 15 DSRL, Rn. 4 ff.

113 *Ehmann/Helfrich* 1999, Art. 17 DSRL, Rn. 3.

114 Zu den Ausnahmen zur Meldepflicht s. Art. 18 Abs. 2 bis 5 DSRL.

115 S. hierzu Art. 26 DSRL. Zentral ist hierbei die Zulässigkeit der Übermittlung, wenn „die betroffene Person ohne Zweifel ihre Einwilligung gegeben hat" (Art. 26 Abs. 1 lit. a) DSRL).

116 Entscheidung der Kommission vom 26.7.2000 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des von den Grundsätzen des „sicheren Hafens" und der diesbezüglichen „Häufig gestellten Fragen" (FAQ) gewährleisteten Schutzes, vorgelegt vom Handelsministerium der USA, ABl. L 215 vom 25.8.2000, 7.

2015[117] zwar noch immer zulässig, die Kompetenz der nationalen Datenschutzbehörden zur Überprüfung des tatsächlichen Vorliegens eines angemessenen Schutzniveaus darf jedoch nicht durch die Europäische Kommission beschnitten werden.

2.2 Nationales Datenschutzrecht

Nachdem in einem Überblick der europäische Rahmen für den Datenschutz dargestellt worden ist, soll nachfolgend das für den Untersuchungsgegenstand einschlägige nationale Datenschutzrecht vorgestellt werden. Dieses ist zum Teil durch die europarechtlichen Vorgaben geprägt worden, hat aber umgekehrt deren Entwicklung beeinflusst. Da die Rechtsordnung einem hierarchischen Aufbau folgt und somit die Normsetzung und auch die Auslegung der untergeordneten einfachgesetzlichen Vorschriften immer im Licht des übergeordneten Rechts zu erfolgen hat, ist zwischen dem Verfassungsrecht und den einfachgesetzlichen Vorschriften zu unterscheiden.

2.2.1 Informationelle Selbstbestimmung

Eine der wohl bedeutendsten Ausprägungen des allgemeinen Persönlichkeitsrechts gemäß Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG ist das Recht auf informationelle Selbstbestimmung. Der Inhalt und die Reichweite dieses Grundrechts werden nach wie vor durch das Volkszählungsurteil des Bundesverfassungsgerichts vom 15. Dezember 1983 bestimmt.[118] Es ist als Reaktion auf die besonderen Risiken der automatisierten Datenverarbeitung vor dem Hintergrund der gesellschaftlichen Diskussion um die Volkszählung zu verstehen. Das Datenschutzrecht trat in eine neue Phase ein, indem erstmals in Deutschland höchstrichterlich festgestellt wurde, dass dem Daten-

---

[117] *EuGH*, Urteil vom 6.10.2015, Rs. C-362/14. Das Abkommen wurde vom *EuGH* in dem Urteil für ungültig erklärt.

[118] *BVerfGE* 65, 1 (42 ff.); s. zur Wiederholung der Kernpassagen in der ständigen Rspr. *BVerfGE* 78, 77 (84); 84, 92 (194 ff.); zum Volkszählungsurteil *Simitis*, NJW 1984, 398 ff.; *Krause*, JuS 1984, 268; *Steinmüller*, DuD 1984, 91 ff.; *Schlink*, Der Staat 25 (1986), 233 ff.; *Busch*, DVBl 1984, 385; *Mückenberger*, KJ 1984, 1; *Hufen*, JZ 1984, 1072; *Vogelgesang* 1987, 51 ff.; *Heußner*, AuR 1985, 311 ff.

schutz Verfassungsrang zukommt.[119] In dieser Entscheidung leitet das Gericht aus dem allgemeinen Persönlichkeitsrecht „die aus dem Gedanken der Selbstbestimmung stammende Befugnis des Einzelnen ab, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen". Das Bundesverfassungsgericht hat sich des Mittels bedient, das allgemeine Persönlichkeitsrecht so weiter zu entwickeln, dass es den tatsächlichen Veränderungen durch moderne Informationstechnik Rechnung trägt.

Die informationelle Selbstbestimmung schützt vor den Risiken der automatischen Verarbeitung digitaler Daten. Um den Schutzbereich dieses Grundrechts als Ausprägung des allgemeinen Persönlichkeitsrechts zu konkretisieren, werden nur Daten einbezogen, die einen Bezug zu einer konkreten Person aufweisen und somit personenbezogen sind. Das Recht schützt vor dem Feststellen, Verwenden, Speichern, Weitergeben und Veröffentlichen dieser Daten. Der Betroffene soll grundsätzlich selbst entscheiden können, wann und innerhalb welcher Grenzen er persönliche Lebenssachverhalte offenbart und wie er gegenüber Dritten auftritt.[120] Die informationelle Selbstbestimmung umfasst daher die Ausprägungen der Selbstbestimmung und der Selbstdarstellung jeweils in Form der Selbstverleugnung und Selbstoffenbarung. Dogmatisch bedeutsam an der Entscheidung des Bundesverfassungsgerichts ist die Abkehr von der bis dahin vorherrschenden „Sphärentheorie",[121] die je nach Betroffenheit der Intim-, Privat- oder Sozialsphäre von einer unterschiedlichen Schutzbedürftigkeit und Eingriffsresistenz ausging. Im Volkszählungsurteil machte das Bundesverfassungsgericht den Schutz der Daten nicht mehr von der Sphäre abhängig, aus der sie stammen.[122] Es erkannte, dass es aufgrund der durch die modernen Informations- und Kommunikationstechniken möglichen Verarbeitung und Verknüpfung der Informationen unter

---

119 *BVerfGE* 84, 239 (278).

120 *Starck*, in: v. Mangoldt/Klein/Starck 2010, Bd. 1, Art. 2 Abs. 1 GG, Rn. 114, 117.

121 *Simitis*, NJW 1984, 398 (402); *Kunig*, in: v. Münch/Kunig 2012, Bd. 1, Art. 2 GG, Rn. 41; *Trute*, in: Roßnagel 2003, 164.

122 S. hierzu auch *Geminn/Roßnagel*, JZ 2015, 703; *Nebel*, ZD 2015, 517.

den „Bedingungen der automatisierten Datenverarbeitung kein belangloses Datum mehr“ gibt.[123] Jede Datenverarbeitung gegen den Willen der betroffenen Person ist daher ein Eingriff in das Recht auf informationelle Selbstbestimmung.

Der informationellen Selbstbestimmung kommt vorrangig die klassische Abwehrfunktion zu, indem sie vor staatlichem Handeln schützt. Grundrechtsverpflichtete sind gemäß Art. 1 Abs. 3 GG ausschließlich die Gesetzgebung, die vollziehende Gewalt und die Rechtsprechung. Dem Staat werden somit klare Grenzen gesetzt, dass er nicht beliebig und willkürlich persönliche Informationen von den Bürgern einfordern darf, sondern diese grundsätzlich berechtigt sind, eine Auskunft abzulehnen. Das Bundesverfassungsgericht fordert – wie bei allen anderen Grundrechten – für einen Grundrechtseingriff in die informationelle Selbstbestimmung eine gesetzliche Erlaubnis.[124] Darüber hinaus kommt der informationellen Selbstbestimmung auch eine Schutzfunktion zu. Beeinträchtigungen des Grundrechts erfolgen spätestens seit der Privatisierung des Post- und Telekommunikationswesens sowie der Etablierung unternehmerischer Kundendatenbanken, zum Beispiel für Kundenbindungsprogramme, Kreditscoring und personalisierte Werbung, nicht mehr primär durch den Staat. Zahlreiche private Stellen haben den wirtschaftlichen Wert von personenbezogenen Datensammlungen längst erkannt. Der Ausspruch „Wissen ist Macht“ gilt mehr denn je. In Bezug auf private Stellen ist damit allerdings vorrangig die Wirtschaftsmacht gemeint. Verfassungsrechtliche Aufgabe des Staates ist es, diesen Beeinträchtigungen der informationellen Selbstbestimmung durch private Stellen vorzubeugen und dem einzelnen Bürger rechtliche Instrumente zur Verteidigung seines Grundrechts zur Verfügung zu stellen.

---

123 *BVerfGE* 65, 1 (45).

124 § 4 Abs. 1 BDSG sieht als allgemeine, einfachgesetzliche Vorschrift für einen zulässigen Umgang mit personenbezogenen Daten die Varianten der Erlaubnis durch dieses Gesetz oder eine andere Rechtsvorschrift oder die Einwilligung des Betroffenen vor.

Neben dieser auf den Einzelnen bezogenen Schutzrichtung ist die informationelle Selbstbestimmung nach der Überzeugung des Bundesverfassungsgerichts zugleich Grundlage eines freien und demokratischen Rechtstaats. Die Furcht vor einer umfassenden Datenverarbeitung kann eine Abschreckung vor der Ausübung anderer Grundrechte zur Folge haben: „Wer damit rechnet, dass etwa die Teilnahme an einer Versammlung oder einer Bürgerinitiative behördlich registriert wird und dass ihm dadurch Risiken entstehen können, wird möglicherweise auf eine Ausübung seiner entsprechenden Grundrechte (Art. 8, 9 GG) verzichten."[125] Dies führt zu einer Beeinträchtigung nicht nur der individuellen Entfaltungschancen des Einzelnen, sondern auch des Gemeinwohls, da die Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist.[126] Schutzzweck ist die Sicherung der allgemeinen Handlungsfreiheit, des Willensbildungsprozesses und der Meinungsfreiheit, aber auch die Gewährleistung der Grundlagen für einen freiheitlich demokratischen Rechtsstaat. Die informationelle Selbstbestimmung soll verhindern, dass die Verhaltensweisen des Einzelnen jederzeit registriert werden sowie durch Speicherung und Verarbeitung als Information dauerhaft zur Verfügung stehen. Diese Verbindung mit dem kommunikativen und somit gesellschaftlichen Aspekt verleiht dem Recht auf informationelle Selbstbestimmung ein besonderes Gewicht, das sich insbesondere in Abwägungsprozessen auswirkt.[127]

2.2.2 Datenschutzrecht und Zulässigkeit der Datenverarbeitung

Die zentrale Kodifikation des deutschen Datenschutzrechts ist das Bundesdatenschutzgesetz. Daneben finden in jedem Bundesland ein Landesdatenschutzgesetz und weitere sogenannte bereichsspezifische Vorschriften Anwendung, die auf die Besonderheiten spezieller Le-

125 *BVerfGE* 65, 1 (43); s. dazu *Trute*, in: Roßnagel 2003, 164.
126 *BVerfGE* 65, 1 (43).
127 *Hornung* 2005, 139f.

bensbereiche zugeschnitten sind, um den dort spezifischen Gefahren für das Grundrecht der informationellen Selbstbestimmung Rechnung zu tragen. Soweit die bereichsspezifischen Gesetze genauere, weitergehende oder abweichende Regeln zum Bundesdatenschutzgesetz treffen, gehen sie diesem gemäß § 1 Abs. 3 Satz 1 BDSG als lex specialis vor.

Kommen Telekommunikationstechniken zum Einsatz, ist für diese regelmäßig der Anwendungsbereiche des Telekommunikationsgesetzes eröffnet. Soweit für Internetanwendungen personenbezogene Daten verarbeitet werden, greift das Telemediengesetz ein.

Für die beschriebenen Einsatzgebiete der Informationstechnik können sich darüber hinaus noch weitere fachspezifische Datenschutzvorschriften ergeben. In den Teilbereichen des Smart Grid und Smart Metering von Smart Home sind die datenschutzrechtlichen Vorgaben des Energiewirtschaftsgesetzes insbesondere § 21g EnWG vorrangig zu beachten.[128] Dieser bildet die Grundlage für den Umgang mit den personenbezogenen Daten, die aus dem Messsystem oder mit Hilfe des Messsystems erhoben, verarbeitet oder genutzt werden. Geregelt sind insbesondere die zulässigen Zwecke der Datenverarbeitung, und es erfolgt eine Einschränkung der datenumgangsberechtigten Stellen.

Für den Bereich des E-Health gelten spezifische Datenschutzvorschriften in verschiedenen Gesetzen. Zum einen gibt es für den Gesundheitsbereich mit den Landeskrankenhausgesetzen[129] sowie dem 10. Kapitel „Versicherungs- und Leistungsdaten, Datenschutz, Datentransparenz“ des SGB V und den allgemeinen Datenschutzvorschriften im SGB X spezifische Datenschutzvorschriften. Im E-Health-Bereich wird der Datenschutz durch einen Vertraulichkeitsschutz der Informationen in der Ausprägung der ärztlichen Schweigepflicht ergänzt. Rechtsdogmatisch ordnet § 1 Abs. 3 Satz 2 BDSG ausdrücklich

---

128 S. *Jandt*, smart.ER 2014, 2014, 10; *Jandt/Roßnagel/Volland,* ZD 2011, 99.

129 Zu den unterschiedlichen Bezeichnungen dieser Gesetze in den verschiedenen Bundesländern s. *Jandt/Roßnagel/Wilke,* RDV 2011, 225.

die Parallelgeltung von Berufsgeheimnissen und besondere Vertraulichkeitsverpflichtungen wie die ärztliche Schweigepflicht und den Datenschutzgesetzen an.

Big Data-Analysen können in zahlreichen Einsatzfeldern mit entsprechend vielfältigen Zielsetzungen verwendet werden.[130] Für sie gelten daher unterschiedliche Regelungen, die für den jeweiligen Anwendungsbereich spezifisch sind.

2.3 Datenschutzprinzipien

Für den Schutz der informationellen Selbstbestimmung ist zu fragen, welche Bedingungen bei der Verarbeitung personenbezogener Daten gegeben sein müssen, um die Selbstbestimmung zu gewährleisten. Die Antwort auf diese Frage geben die Datenschutzprinzipien. Sie sind die wesentlichen Zielsetzungen des Schutzkonzepts des Datenschutzrechts, wie sie sowohl im EU-Datenschutzrecht als auch in zahlreichen deutschen Datenschutznormen wiederzufinden sind. Die wichtigsten dieser Prinzipien werden nachfolgend erläutert.

2.3.1 Zweckbindung

Personenbezogene Daten dürfen grundsätzlich nur zu jeweils vorher bestimmten Zwecken erhoben, verarbeitet und genutzt werden (Art. 6 Abs. 1 lit. b) DSRL).[131] Diese Zwecke müssen für den Betroffenen erkennbar sein. Zweckänderungen, also die Verarbeitung oder Nutzung personenbezogener Daten zu anderen als den ursprünglichen Zwecken, bedürfen einer gesonderten Erlaubnis, zum Beispiel gemäß §§ 14 Abs. 2 und 28 Abs. 2 BDSG. Die Zweckbindung ist technisch sicherzustellen,[132] zum Beispiel sind gemäß Ziffer 8 der Anlage zu § 9 BDSG Daten, die zu unterschiedlichen Zwecken erhoben wurden, getrennt zu verarbeiten.

---

130 S. Kap. 1.1.4.

131 Allgemein *BVerfGE* 65, 1 (46); *v. Zeschwitz*, in: Roßnagel 2003, 229 ff.

132 *Schultze-Melling*, in: Taeger/Gabel 2013, § 9 BDSG, Rn. 84.

2.3.2 Erforderlichkeit

Der Grundsatz der Erforderlichkeit beschränkt den Umgang mit personenbezogenen Daten auf das für die Erreichung des jeweiligen Zwecks erforderliche Maß (Art. 6 Abs. 1 lit. c) und e) DSRL).[133] Kann der verfolgte legitime Zweck mit einem geringeren Maß an Datenerhebung, -verarbeitung oder -nutzung genauso gut verwirklicht werden, ist der beabsichtigte Umgang nicht erforderlich. Erforderlichkeit der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten besteht also, wenn im Einzelfall keine ebenso effektive Alternative mit geringerer Eingriffstiefe vorhanden ist.

2.3.3 Datenvermeidung und Datensparsamkeit

Der Grundsatz der Datenvermeidung und Datensparsamkeit, der in § 3a BDSG zum Ausdruck kommt, soll dazu führen, dass so wenig personenbezogene Daten wie möglich verarbeitet werden. Er bezieht sich hierfür nicht erst auf die Erforderlichkeit einer konkreten Datenverarbeitung, sondern zielt bereits auf die Zwecksetzung. Er verlangt, den jeweiligen Zweck so zu wählen (zum Beispiel Flatrate-Tarif statt nutzungsspezifische Abrechnung), dass durch die Gestaltung und Auswahl von Datenverarbeitungssystemen die Verarbeitung personenbezogener Daten vermieden und vermindert werden kann.[134]

2.3.4 Datensicherheit

Die verantwortlichen Stellen haben gemäß § 9 BDSG (Art. 17 DSRL) technische und organisatorische Maßnahmen zu treffen, die erforderlich sind, um die Ziele des Bundesdatenschutzgesetzes, zu verwirklichen und einem Missbrauch von oder Fehlern im Umgang mit personenbezogenen Daten vorzubeugen. Erforderlich sind solche Maßnahmen allerdings nur, soweit sie zum Schutzzweck in einem angemessenen Verhältnis stehen. Technisch konkrete Ziele der zu ergreifenden Maßnahmen sind in der Anlage zu § 9 BDSG beschrieben: Zutrittskon-

---

133 *BVerfGE* 65, 1 (46).

134 Ausführlich *Roßnagel*, in: *Eifert/Hoffmann-Riem* 2011, 41.

trolle, Zugangskontrolle, Zugriffskontrolle, Weitergabekontrolle, Eingabekontrolle, Auftragskontrolle, Verfügbarkeitskontrolle, Trennung von Daten, die zu unterschiedlichen Zwecken erhoben wurden. Gemäß § 109 TKG und § 13 Abs. 7 TMG bestehen spezifische Pflichten zur Sicherung personenbezogener Daten für Telekommunikations- und Telemediendiensteanbieter. Die Anbieter haben demnach beim technischen Schutz personenbezogener Daten den Stand der Technik zu beachten.

2.3.5 Betroffenenrechte

Zur Verwirklichung ihrer informationellen Selbstbestimmung und um den Risiken unrichtiger oder unzulässiger Datenerhebung, -verarbeitung und -nutzung entgegenzuwirken, sind den Betroffenen Rechte auf Benachrichtigung, Auskunft, Korrektur und Löschung hinsichtlich der über sie gespeicherten Daten einzuräumen.[135] Solche finden sich zum Beispiel in den §§ 19 ff. und 33 ff. BDSG (Art. 10 ff. DSRL). Daneben sind zum Beispiel in den §§ 7 und 8 BDSG (Art. 23 DSRL) Schadensersatzansprüche bei unzulässigem Datenumgang vorgesehen. Die Schadensersatzansprüche gegen private Stellen sind dabei als Verschuldenshaftung, die gegen öffentliche Stellen als Gefährdungshaftung ausgestaltet. Dies bedeutet, dass die Betroffenen gegenüber den öffentlichen Stellen lediglich den unzulässigen Datenumgang nachweisen müssen, um mit dem Anspruch im Prozess erfolgreich zu sein. Private Stellen hingegen können sich gemäß § 7 Satz 2 BDSG bezüglich ihres Verschuldens exkulpieren.[136]

2.3.6 Datenschutzkontrolle

Öffentliche und private Stellen, die personenbezogene Daten automatisiert verarbeiten, haben gemäß § 4f Abs. 1 Satz 1 BDSG (Art. 18 Abs. 2 DSRL) einen behördlichen oder betrieblichen Datenschutzbeauftragten zu bestellen. Aufgabe des Datenschutzbeauftragten ist es

---

135 *BVerfGE* 65, 1 (46); *Dix*, in: Simitis 2014, § 33, Rn. 1 ff. und § 35 Rn. 1 ff.
136 *Roßnagel/Pfitzmann/Garstka* 2001, 179 ff.

gemäß § 4g BDSG, in seiner Behörde oder in seinem Betrieb auf die Einhaltung der Datenschutzregelungen hinzuwirken. Zuständig für die öffentliche Kontrolle der Einhaltung der Bestimmungen der Datenschutzgesetze des Bundes und der Länder sind für den öffentlichen Bereich die Datenschutzbeauftragten des Bundes (§§ 21-26 BDSG) und der Länder (Art. 28 DSRL).

2.3.7 Zulässigkeit der Datenverarbeitung

Jeder Umgang mit personenbezogenen Daten, ohne das Einverständnis des Betroffenen ist ein Grundrechtseingriff, sowohl von staatlichen als auch von privatrechtlichen Stellen.[137] Gegenüber staatlichen Stellen besteht ein direktes Abwehrrecht. Eingriffe in die informationelle Selbstbestimmung durch den Staat müssen gerechtfertigt sein. Zwischen Privaten gilt zwar kein unmittelbarer Grundrechtsschutz. Im Rahmen seiner Schutzpflicht für das Grundrecht hat aber der Staat die Rechtsbeziehungen zwischen Privaten so zu gestalten, dass die Grundrechte nicht verletzt werden. Dieser Pflicht ist er im Hinblick auf die informationelle Selbstbestimmung durch die Datenschutzgesetze nachgekommen. Auch private Stellen dürfen daher ohne Einwilligung des Betroffenen nur insoweit mit personenbezogenen Daten umgehen, als ein gesetzlicher Tatbestand dies erlaubt (Art. 6 Abs. 1 lit. a) und Art. 7 lit. a) DSRL). Gemäß der abschließenden Aufzählung in § 4 Abs. 1 BDSG ist die Verwendung personenbezogener Daten dem entsprechend nur insoweit zulässig, als ein Datenschutzgesetz sie erlaubt oder der Betroffene eingewilligt hat.

2.3.7.1 Beteiligte der Datenverarbeitung

Personenbezogene Daten sind gemäß § 3 Abs. 1 BDSG alle Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person. Diese Person wird im Bundesdatenschutzgesetz als „Betroffener" bezeichnet. Als „verantwortliche Stelle" wird gemäß § 3 Abs. 7 BDSG jede Person oder Stelle be-

---

[137] *Roßnagel*, ZD 2013, 562 (563) m.w.N.

zeichnet, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt. Die verantwortliche Stelle ist der Adressat der datenschutzrechtlichen Erlaubnisnormen und unterliegt der Kontrolle durch die Aufsichtsbehörden.

2.3.7.2 Einwilligung und Erlaubnisvorschriften

Soweit keine speziellen Vorschriften bestehen, die den Umgang mit personenbezogenen Daten erlauben, richtet sich die Zulässigkeit des Umgangs nach den allgemeinen Erlaubnistatbeständen des Bundesdatenschutzgesetzes.

2.3.7.2.1 Einwilligung

Eine Einwilligung, die den Umgang mit personenbezogenen Daten erlaubt, muss gemäß § 4a Abs. 1 Satz 1 BDSG eine freiwillige Entscheidung des Betroffenen sein. Dieser muss gemäß Satz 2 über den beabsichtigten Umgang mit den ihn betreffenden Daten umfassend informiert sein.[138] Die Einwilligung muss ohne Zwang erfolgen. Sie muss grundsätzlich eine bestimmte Form einhalten. Dies ist gemäß § 4a Abs. 1 Satz 3 BDSG die Schriftform (eigenhändige Unterschrift). Sie kann aber unter besonderen Umständen auch in anderer Form abgegeben werden. Eine Einwilligung in den Umgang mit besonderen Arten personenbezogener Daten nach § 3 Abs. 9 BDSG, wie zum Beispiel die von Fitness- und Gesundheits-Apps erhobenen Gesundheitsdaten, ist gemäß § 4a Abs. 3 BDSG nur wirksam, wenn sie sich ausdrücklich auf diese Daten bezieht.

Gemäß § 94 TKG kann die Einwilligung im Anwendungsbereich des Telekommunikationsgesetzes auch elektronisch erklärt werden. Der Dienstanbieter muss aber sicherstellen, dass die Teilnehmer ihre Einwilligung bewusst und eindeutig erteilen. Die Einwilligung muss protokolliert werden, damit die Teilnehmer jederzeit einsehen können, wann und in welchem Umfang sie eingewilligt haben. Die Einwilli-

[138] *Bergmann/Möhrle/Herb* 2011, § 4a BDSG, Rn. 5 und 11.

gung muss jederzeit mit Wirkung für die Zukunft widerrufen werden können. Unter den Voraussetzungen von § 13 Abs. 2 TMG ist auch bei Telemediendiensten die elektronische Abgabe der Einwilligung möglich. Die Voraussetzungen entsprechen denen aus § 94 TKG. Zum Beispiel kann bei Telemediendiensten die Einwilligung durch das Setzen eines Häkchens unter einer Datenschutzerklärung auf einer Internetseite oder durch ähnliche eindeutig und bewusst genutzte Verfahren erklärt werden.[139]

2.3.7.2.2 Erlaubnisvorschriften für öffentliche Stellen

Die allgemeinen Rechtsgrundlagen der Datenverarbeitung durch öffentliche Stellen des Bundes finden sich in den §§ 12 bis 18 BDSG. Die allgemeinen Rechtsgrundlagen für die öffentlichen Stellen der Länder finden sich in den Landesdatenschutzgesetzen. Sie ähneln oder entsprechen strukturell denen des Bundesdatenschutzgesetzes, das hier beispielhaft erläutert wird.

§ 13 Abs. 1 BDSG erlaubt das Erheben personenbezogener Daten soweit, wie dies zur Erfüllung der Aufgaben einer verantwortlichen Stelle erforderlich ist. Die öffentliche Stelle ist hierbei auf die Zwecke beschränkt, die sie im Rahmen der ihr zugewiesenen Aufgaben zu erfüllen hat. Nur eine Datenverarbeitung, die zum Erreichen dieser Zwecke erforderlich ist, ist zulässig. Das Erheben der besonderen Arten personenbezogener Daten im Sinn des § 3 Abs. 9 BDSG ist nur nach den strengeren Voraussetzungen des § 13 Abs. 2 BDSG zulässig. Das Speichern, Verändern oder Nutzen personenbezogener Daten ist gemäß § 14 Abs. 1 Satz 1 BDSG zulässig, soweit es zur Erfüllung der Aufgaben der verantwortlichen Stelle erforderlich ist und für die Zwecke erfolgt, für welche die Daten erhoben wurden. Das Speichern, Verändern oder Nutzen zu anderen Zwecken ist nur unter den Voraussetzungen des § 14 Abs. 2 BDSG zulässig. Die §§ 15 und 16 regeln die Übermittlung personenbezogener Daten an andere öffentliche und an private Stellen.

---

[139] Hierzu *Jandt/Schaar/Schulz*, in: Roßnagel 2013, §13 TMG, Rn. 72f.

Für öffentliche Stellen des Bundes gelten aber gemäß § 12 Abs. 1 BDSG die § 13 ff. nur, soweit sie nicht als öffentlich-rechtliche Unternehmen am Wettbewerb teilnehmen. In diesem Fall gelten wie für private Stellen die §§ 27 ff. BDSG. Außerdem gelten gemäß § 12 Abs. 4 BDSG § 28 Abs. 2 Nr. 2 und §§ 32 bis 35 BDSG anstelle der §§ 13 bis 16 und 19 bis 20 BDSG, soweit personenbezogene Daten für frühere, bestehende oder zukünftige Beschäftigungsverhältnisse erhoben, verarbeitet oder genutzt werden.

Die Erlaubnisvorschriften für die Strafverfolgung finden sich in der Strafprozessordnung. Die Erhebung und Verarbeitung personenbezogener Daten durch die Strafverfolgungsbehörden kann sich nach je nach Ermittlungsschritt auf unterschiedliche Rechtsgrundlagen insbesondere in den §§ 94 ff. StPO stützen. So kann sich die Befugnis zur Sicherstellung oder Beschlagnahme von Gegenständen gemäß § 94 Abs. 1 StPO auch auf bestimmte Daten beziehen, wie zum Beispiel solche in sichergestellten Dokumenten, aber auch E-Mails, die sich nicht in der Übertragung befinden.[140] Die Überwachung von Telekommunikationshalten richtet sich zum nach § 100a StPO, die Erhebung von Verkehrsdaten nach §100g StPO Die Bestandsdatenauskunft ist gemäß den Voraussetzungen in § 100j StPO zulässig.

Die Erlaubnisvorschriften für die Gefahrenabwehr vor allem in den Polizeigesetzen der Länder. So ist für die Gefahrenabwehr in Hessen die Erhebung personenbezogener Daten nach § 13 des Hessischen Gesetzesüber die öffentliche Sicherheit und Ordnung (HSOG) zulässig, wenn sie zur Abwehr einer Gefahr erforderlich ist und die weiteren Voraussetzungen der Norm vorliegen. Einen speziellen Erhebungstatbestand für Telekommunikationsdaten enthält § 15a HSOG. Die Speicherung und Weiterverarbeitung erhobener personenbezogener Daten richtet sich nach § 20 ff. HSOG. Auch im Gefahrenabwehrrecht gilt der Zweckbindungsgrundsatz, wie etwa in § 13 Abs. 5 Satz 1 HSOG zu erkennen ist.

---

140 *Ritzert*, in: Graf 2015, § 94 StPO, Rn. 1

2.3.7.2.3 Erlaubnisvorschriften für nicht-öffentliche Stellen

Die grundlegenden Erlaubnisnormen für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch nicht-öffentliche Stellen finden sich in den §§ 28 bis 29 BDSG.

§ 28 Abs. 1 Satz 1 Nr. 1 bis 3 BDSG erlaubt das Erheben, Speichern, Verändern und Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke, soweit es für einen Vertrag mit dem Betroffenen erforderlich ist, soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist oder soweit die Daten allgemein zugänglich sind.

Die Vertragsdatenverarbeitung (Nr. 1) spielt für die Privatwirtschaft eine wichtige Rolle, da eine solche Datenverarbeitung für die Durchführung von Verträgen essentiell ist. Wann eine Datenverarbeitung im Sinn der Nr. 1 vorliegt, ist nach dem jeweiligen Vertragszweck zu bestimmen. Im Rahmen der Nr. 2 und 3 muss im Unterschied zu Nr. 1 eine Abwägung mit den Interessen des Betroffenen vorgenommen werden, die zur Unzulässigkeit der Datenverarbeitung führen kann. Ein berechtigtes Interesse der verantwortlichen Stelle im Sinn der Nr. 2 ist ein nach vernünftiger Erwägung der Sachlage gerechtfertigtes Interesse. Dieses kann rein wirtschaftlicher oder auch ideeller Natur sein.[141] Die notwendige Interessenabwägung kann insbesondere dann zugunsten des Betroffenen ausschlagen und die Datenverarbeitung hierdurch unzulässig werden, wenn die Daten dazu verwendet werden, umfassende Persönlichkeitsprofile der Betroffenen zu erstellen. Ein offensichtliches Überwiegen der Interessen des Betroffenen im Sinn der Nr. 3 liegt dann vor, wenn eine Verletzung der Interessen des Betroffenen ohne weiteres erkennbar ist. Der verantwortlichen Stelle wird hier aber, wie auch bei Nr. 2, nur eine summarische Prüfung auferlegt.[142]

---

141 *Simitis*, in: Simitis 2014, § 28, Rn. 104.
142 *Simitis*, in: Simitis 2014, § 28, Rn. 163.

§ 28 Abs. 3 und 4 BDSG regeln die Verarbeitung oder Nutzung personenbezogener Daten für Zwecke des Adresshandels oder der Werbung, Abs. 6 bis 9 das Erheben, Verarbeiten und Nutzen personenbezogener Daten im Sinn des § 3 Abs. 9 BDSG.

§ 28a BDSG regelt die Übermittlung personenbezogener Daten an Auskunfteien wie zum Beispiel die SCHUFA. § 28b BDSG beschreibt die Zulässigkeitsvoraussetzungen für den Einsatz von Scoring-Werten, zum Beispiel bei der Kreditvergabe. § 29 BDSG beschreibt die strengen Anforderungen an die geschäftsmäßige Datenverarbeitung insbesondere durch Auskunfteien und Adresshändler. § 30a BDSG regelt den geschäftsmäßigen Umgang mit personenbezogenen Daten für Zwecke der Markt- und Meinungsforschung

2.3.7.2.4 Erlaubnisvorschriften für Telekommunikationsdiensteanbieter

Die §§ 91 ff. TKG regeln den Schutz personenbezogener Daten der Teilnehmer und Nutzer von Telekommunikation bei der Erhebung und Verwendung dieser Daten durch Unternehmen und Personen, die geschäftsmäßig Telekommunikationsdienste in Telekommunikationsnetzen erbringen oder an deren Erbringung mitwirken. Auf eine Gewinnerzielungsabsicht kommt es dabei nicht an. Auch Behörden, Schulen, Krankenhäuser, Hotels und andere Stellen mit eigenem Telekommunikationsnetz sind grundsätzlich in den Anwendungsbereich des § 91 Abs. 1 Satz 1 TKG einbezogen.[143] Die beispielhaft betrachteten smarten Informationstechniken sind weitreichend auf die Signalübertragung in Form von Telekommunikation angewiesen. Ihre Anbieter nutzen Telekommunikation sind aber selten auch Anbieter von Telekommunikationsdiensten im Sinn des Telekommunikationsgesetzes. Die Daten ihre Nutzer werden aber auch von den Anbietern von Telekommunikationsdiensten erhoben, verarbeitet und genutzt, so dass der Telekommunikationsdatenschutz eine grundlegende Rolle für sie spielt.

---

[143] *Eckhardt*, in: Spindler/Schuster 2015, § 88 TKG, Rn. 25f.

Das Telekommunikationsgesetz unterscheidet datenschutzrechtlich zwischen Bestandsdaten, Verkehrsdaten und Abrechnungsdaten. Bestandsdaten dürfen gemäß § 95 Abs. 1 TKG erhoben werden, soweit dies für die genannten Zwecke erforderlich ist. Unter den Voraussetzungen des § 95 Abs. 2 TKG dürfen Bestandsdaten für Werbung genutzt werden. Bei Beendigung des Vertrags sind die Bestandsdaten nach Abs. 3 bis zum Ablauf des folgenden Kalenderjahres zu löschen. Der Umgang mit Verkehrsdaten ist durch § 96 TKG begrenzt. Gemäß § 96 Abs. 1 TKG dürfen die in den Nummern 1 bis 5 genannten Verkehrsdaten erhoben und verwendet werden, soweit dies für die in den §§ 91 bis 107 TKG genannten Zwecke erforderlich ist. Hierzu gehören auch Anschlusskennungen, IP-Adressen, Berechtigungskennungen und Standortdaten. § 98 TKG regelt die Datenverwendung beim Angebot standortbezogener Dienste. Solche Dienste werden häufig auf Smartphones und anderen mobilen internetfähigen Geräten genutzt, etwa Navigationsdienste, ortsbezogene Werbedienste, Social Apps mit Standorterkennung der Teilnehmer oder Jogging-Apps, die den Streckenverlauf protokollieren. Die hierfür erforderlichen spezifischen Standortdaten dürfen nur im erforderlichen Maß und innerhalb des dafür erforderlichen Zeitraums verarbeitet werden. Die Daten müssen anonymisiert werden oder die Teilnehmer müssen eingewilligt haben.[144]

Die alten Vorschriften über eine Vorratsdatenspeicherung in den §§ 113a und 113b TKG, die eine anlasslose Speicherung der Verkehrsdaten für sechs Monate vorschrieben und eine Übermittlung für Strafverfolgung, Gefahrenabwehr und Aufgaben der Geheimdienste regelten waren mit Urteil des Bundesverfassungsgerichts vom 2. März 2010[145] als nichtig erklärt worden. Sie verletzten das Fernmeldegeheimnis aus Art. 10 Abs. 1 GG.[146] Am 8. April 2014 hatte außerdem der Europäische Gerichtshof auch die der Regelung zugrunde liegende

144 Hierzu *Eckhardt*, in: Spindler/Schuster 2015, § 98 TKG, Rn. 13 ff.
145 *BVerfGE* 125, 260.
146 Hierzu *Roßnagel*, NJW 2010, 1238.

EG-Richtlinie[147] aufgehoben.[148] Zum 18.12.2015 wurde in Deutschland unabhängig von europarechtlichen Vorgaben eine neue Vorratsdatenspeicherung eingeführt. Die Neuregelung in den § 113a ff. TKG enthält einige Änderungen gegenüber den Vorgängerregelungen. Insbesondere ist die generelle Speicherdauer für die Daten auf zehn Wochen und für Standortdaten auf vier Wochen reduziert worden und es wurden umfangreiche Regelungen über die Datensicherung eingefügt.[149] Gegen das Gesetz wurden bereits Verfassungsbeschwerden eingereicht. Daher bleibt abzuwarten, ob die neuen Regelungen vor dem Bundesverfassungsgericht und dem Europäischen Gerichtshof bestehen werden.

2.3.7.2.5 Erlaubnisvorschriften für Telemediendiensteanbieter

Gemäß § 1 Abs. 1 Satz 1 TMG sind Telemediendienste alle elektronischen Informations- und Kommunikationsdienste, soweit sie nicht Telekommunikationsdienste, die ganz in der Signalübertragung bestehen, und auch nicht Rundfunk sind. Die Voice over IP-Telefonie stellt zum Beispiel keinen Telemediendienst, sondern einen Telekommunikationsdienst dar.[150] Zum Rundfunk gehören neben Fernsehen und Hörfunk auch Live-Streaming (zusätzliche zeitgleiche Übertragung herkömmlicher Rundfunkprogramme über das Internet) und Web-Casting (ausschließliche Übertragung herkömmlicher Rundfunkprogramme über das Internet). Radio- und Fernsehtext, Teleshopping und Video-on-Demand gehören aber zu den Telemediendiensten.[151] Weitere Telemediendienste sind Online-Shops für Waren und Dienstleistungen mit direkter Bestellmöglichkeit, die Online-Presse, Chatrooms, Suchmaschinen, Soziale Netzwerke[152] und Online-Spiele.[153] Chatrooms und Twitter-Tweets sind Telemediendienste und keine Telekom-

147 RL 2006/46/EG
148 *EuGH*, Urteil vom 8.4.2014, Rs. C-293/12 und C-594/12.
149 Zur Neuregelung *Roßnagel*, NJW 2016, 533.
150 BT-Drs. 16/3078, 13.
151 BT-Drs. 16/3078, 13.
152 *Roßnagel*, NVwZ 2007, 743.
153 S. *Backu*, ZD 2012, 59 (62).

munikationsdienste, weil sie die Nachrichten nicht nur von einem Nutzer zu einem anderen Nutzer schicken, sondern sie auch speichern und öffentlich anzeigen (hosten). Viele der heutzutage auf mobilen Geräten verbreiteten Apps werden als Telemediendienste einzuordnen sein, soweit sie erheblich mehr als die reine Signalübertragung bieten,[154] und somit auch zahlreiche Anwendungen smarter Informationstechnik im Alltag, wie zum Beispiel Apps für das Smart Home, für das Smart Car oder für Smart Health. Anbieter von Telemediendiensten können gemäß § 1 Abs. 1 Satz 2 TMG sowohl öffentliche als auch private Stellen sein.

Erlaubnisvorschriften für den Umgang mit personenbezogenen Daten der Nutzer sind in den §§ 14 und 15 TMG enthalten. Bestandsdaten dürfen nach § 14 Abs. 1 TMG erhoben werden, soweit sie im konkreten Fall erforderlich sind. Im Einzelfall dürfen auf Anfrage Bestandsdaten nach § 14 Abs. 2 TMG für die Strafverfolgung, für die Gefahrenabwehr und für die Erfüllung der Aufgaben von Verfassungsschutz, Nachrichtendiensten und Bundeskriminalamt, auch zur Durchsetzung der Rechte am geistigen Eigentum an die jeweiligen Behörden übermittelt werden. Der Diensteanbieter muss hierzu aber nicht wie bei der Vorratsdatenspeicherung der Telekommunikationsanbieter bestimmte Daten nur für diesen Zweck speichern. Er muss nur das weitergeben, was er ohnehin zulässigerweise gespeichert hat.[155] Nutzungsdaten dürfen gemäß § 15 Abs. 1 Satz 1 TMG erhoben und verwendet werden, soweit dies erforderlich ist, um die Inanspruchnahme der Dienste zu ermöglichen und abzurechnen. Der Diensteanbieter darf gemäß § 15 Abs. 3 Satz 1 TMG für Werbezwecke, zur Marktforschung und zur bedarfsgerechten Gestaltung Nutzungsprofile unter Pseudonym erstellen, sofern der Nutzer nicht widerspricht. Gemäß § 15 Abs. 5 Satz 3 TMG dürfen Nutzungsdaten in anonymisierter Form für die Marktforschung an andere Diensteanbieter übermittelt werden.

---

154 *Maier/Ossoinig*, VuR 2015, 330 (332); *Wilmer* 2015, 12f.; zur Unterscheidung von Apps in Telekommunikationsdienste und Telemediendienste s. auch *Kremer*, CR 2012, 438 (440f.).

155 *Roßnagel,* NVwZ 2007, 743 (748).

Ansonsten sind Nutzungsdaten nach dem jeweiligen Nutzungsvorgang unmittelbar zu löschen. Wie für Bestandsdaten gilt für Nutzungsdaten gemäß § 15 Abs. 5 Satz 4 TMG die Erlaubnis des § 14 Abs. 2 TMG, sie auf Anfrage an die dort genannten Behörden und Personen zu übermitteln.

2.4 Bestehendes Datenschutzniveau

Die bestehenden Regelungen werden im folgenden Abschnitt auf die genannten Risiken der neuen technischen Herausforderungen bezogen. Es wird beschrieben, welches Schutzniveau diese bieten können. Im folgenden Kapitel wird dann untersucht, welche Regelungsdefizite bestehen, wenn die bestehenden Datenschutzregelungen auf die künftigen technischen Möglichkeiten zur Anwendung kommen.

2.4.1 „Smarte" Informationstechnik im Alltag

Spezifische Regelungen, die auf die spezifischen Datenschutzrisiken „smarter" Informationstechnik im Alltag und auf Big Data bezogen sind, fehlen. Nur in einzelnen Anwendungsfeldern – wie beim eCall, beim Smart Metering oder bestimmten Formen des Smart Health – bestehen spezifischen Sondervorschriften. Ansonsten aber kann Datenschutz in künftigen Konfliktfällen nur auf die allgemeinen Datenschutzregelungen zurückgreifen, die ursprünglich für andere Probleme und Konflikte gedacht waren. Sie wurden für ein bestimmtes Konzept von Datenschutz erlassen, richten sich an bestimmte Adressaten und suchen einen Ausgleich, der den damals in den Blick genommenen Konflikten adäquat ist.

Das geltende normative Schutzkonzept kann grundsätzlich auch für die Anwendungen „smarter" Informationstechnik im Alltag und von Big Data taugliche normative Lösungen bieten, die die erwarteten Interessenkonflikte betreffen.[156] Dies setzt aber voraus, dass

[156] S. näher *Roßnagel/Jandt/Müller/Gutscher/Heesen* 2006, 137.

- nur wenige Instanzen mit klarer Rollenzuweisung beteiligt sind. Soweit der Staat Überwachungsdaten erhebt, der Arbeitgeber mit Logistikdaten auch Daten seines Arbeitnehmers speichert, der Vermieter in seinem Haus Daten über den individuellen Energieverbrauch seiner Mieter verarbeitet, der Verkäufer dem Kunden nur mit RFID-Marken versehene Waren anbietet, oder die Autoversicherung das Fahrverhalten der Versicherungsnehmer für die Prämienberechnung aufzeichnet, besteht eine klare und einfache „Frontstellung" zwischen Datenverarbeiter und Betroffenem.
- die Verhältnisse überschaubar sind. Soweit nur wenige Beteiligte einzelne Schritte der Erhebung, Verarbeitung und Nutzung eindeutig personenbezogener Daten in Dateien durchführen und damit eindeutige Zwecke verfolgen, herrschen klar strukturierte Prozesse, deren Wirkungen einzelnen Verantwortlichen zuzurechnen sind.
- die zu beurteilenden Handlungen nur Einzelfälle betreffen. Soweit der Umgang mit den Daten bekannt oder aufklärbar ist und die Zusammenhänge und Verantwortlichkeiten durchschaubar sind, können der Betroffene oder die Datenschutzaufsicht sich auf das Ereignis konzentrieren und ihre Kontrollrechte geltend machen.

In solchen Konstellationen wird „smarte" Informationstechnik im Alltag und Big Data die Möglichkeiten der Interessendurchsetzung zwischen den Beteiligten verschieben und für die Datenverarbeiter auch neue Missbrauchsmöglichkeiten eröffnen. Dennoch entsprechen die neuen Problemstellungen dem „Erwartungshorizont" des Datenschutzrechts und es ist weiterhin möglich, die rechtliche Erlaubnis einer Datenverwendung zu überprüfen und datenschutzrechtliche Grundsätze wie Transparenz für den Betroffenen sowie Zweckbindung und Erforderlichkeit der Datenverarbeitung zur Anwendung zu bringen.[157]

[157] S. hierzu *Roßnagel* 2007, 120 ff.

2.4.1.1 Smart Car

Im vernetzten Auto entstehen viele Daten unterschiedlicher Kategorien, werden verarbeitet, übertragen und gespeichert. Sie unterfallen dem Datenschutzrecht nur dann, wenn sie personenbezogene Daten im Sinn des § 3 Abs. 1 BDSG sind. Dies ist der Fall, wenn die Daten Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person sind. Die Fahrzeugsystem-, -betriebs-, -standort- und Kommunikationsdaten sind immer Daten, die zumindest dem Halter zugeordnet werden können, denn es sind Daten, die sein Auto betreffen.[158] Die anfallenden Daten sind überwiegend personenbezogen oder personenbeziehbar, weil die unterschiedlichen Interessenten sie mit vertretbarem Aufwand in einem überschaubaren Zeitraum einer Person zuordnen können.[159] Selbst wenn die Daten rein technische Sachverhalte betreffen, können sie personenbeziehbar sein, wenn das Auto identifizierbar ist, etwa über die Kfz-ID oder das Kfz-Kennzeichen.[160] Dann ist in der Regel mit vertretbarem Aufwand auch der Halter identifizierbar. Alle technischen Daten, die einem Auto zugeordnet werden können, sind damit auch dem Halter zuordenbar.[161] Soweit die Daten aggregiert oder rein statistischer Natur sind, fehlt ihnen meist der Personenbezug. Das Gleiche gilt, wenn sie tatsächlich anonym oder pseudonym sind.[162] Jedenfalls sind aber alle Automobil-Daten rechtlich relevant.

Schließlich könnte erwogen werden, dass Datenverarbeitung im Auto ein Umgang mit personenbezogenen Daten „ausschließlich für persönliche oder familiäre Tätigkeiten" sei und deswegen nach § 1 Abs. 2 Nr. 3 BDSG aus dem Geltungsbereich des Datenschutzrechts heraus-

158 S. hierzu auch *Roßnagel* 2014a, 265f.
159 S. *Tinnefeld*, in: Roßnagel 2013, 490 ff.
160 S. zu „intelligenten" Kennzeichen *Lüdemann/Sengstacken/Vogelpohl*, ZD 2015, 55.
161 S. *Weichert*, SVR 2014, 204; *Roßnagel*, SVR 2014, 283f.
162 S. *Roßnagel/Scholz*, MMR 2000, 721 ff.; *Roßnagel* 2014a, 266.

falle.[163] Dieses Argument kann ohnehin nur für Datenverarbeitungen durch den Halter oder Fahrer vorgebracht werden und ist schon dann nicht mehr haltbar, wenn Personen aus der Öffentlichkeit betroffen sind oder Daten an andere Stellen weitergegeben werden.[164]

Die Zulässigkeit der Erhebung, Verarbeitung und Nutzung personenbezogener Daten hängt im Wesentlichen davon ab, wer in welcher Rolle mit den Daten zu welchem Zweck umgehen möchte. Dies beeinflusst auch die Antwort auf die Frage, wer gegenüber wem welche datenschutzrechtlichen Pflichten hat oder Ansprüche geltend machen kann.

Adressat des Datenschutzrechts ist die „verantwortliche Stelle". Dies ist nach § 3 Abs. 7 BDSG diejenige Stelle, die über Ob und Wie der Datenverarbeitung entscheidet. Wollen Interessierte personenbezogene Daten für eigene Zwecke verarbeiten, könnten sie als verantwortliche Stelle angesehen werden.[165]

Ob der Datenumgang dem Halter oder Fahrer als Betroffenen zuzurechnen ist oder dem Hersteller oder anderen Interessenten als verantwortlichen Stellen, hängt davon ab, wer den entscheidenden Einfluss auf den Datenumgang ausübt. Wenn der Halter oder der Fahrer die Funktionen der technischen Systeme beeinflussen oder zumindest den Zugriff auf diese steuern kann, ist ihm die automatische Erzeugung und Verarbeitung der Daten zuzurechnen. Dann greift kein Datenschutzrecht, weil der Betroffene nicht schützenswert ist, wenn er mit seinen eigenen Daten umgeht.[166] Ist dies nicht der Fall, ist der Hersteller oder ein anderer Interessent als verantwortliche Stelle anzusehen. Sind zum Beispiel Auto-Systeme so gesichert, dass Veränderun-

---

[163] So vorgetragen für Bildaufnahmen von DashCams – s. zu den widerstreitenden Argumenten *Reibach*, DuD 2015, 157; *Kinast/Kühnl*, NJW 2014, 3057; *Knyrim/Trieb*, ZD 2014, 547; *Atzert/Franck*, RDV 2014, 136; *Balzer/Nugel*, NJW 2014, 1622; *Greger*, NVZ 2015, 114.

[164] Zur notwendigen Einschränkung dieser Ausnahme bei Ubiquitous Computing s. *Roßnagel* 2007, 192f.

[165] S. hierzu *Wedde*, in: Roßnagel 2003, 534 ff.

[166] *Dammann,* in: Simitis 2014, § 3, Rn. 226.

gen nur mit der Genehmigung des Herstellers vorgenommen werden können,[167] dann ist dieser auch die verantwortliche Stelle, die den Umgang mit den Daten verantwortet.[168]

Hat der Betroffene in den Umgang mit seinen Daten eingewilligt, ist dieser nach § 4a BDSG zulässig. Die Einwilligung ist jedoch nur wirksam, wenn sie informiert, freiwillig, ausreichend bestimmt und formgerecht erfolgt ist.[169]

Soweit die verantwortlichen Stellen die Daten für die Erfüllung von Verträgen benötigen, die sie mit dem Halter oder dem Fahrer geschlossen haben, können sie nach § 28 Abs. 1 Satz 1 Nr. 1 BDSG mit dessen dafür erforderlichen Daten umgehen.[170] Solche Verträge können die Funktionalität und Sicherheit im Auto oder Mehrwertdienste rund ums Auto betreffen, die vor allem von Herstellern angeboten werden dürften. Allerdings sollten die Dienste und ihr Informationsbedarf nach dem Prinzip der Datensparsamkeit gestaltet sein.[171]

Zusatzdienste etwa zur Verkehrsführung, zu Sehenswürdigkeiten oder zur Kommunikation oder zur Unterhaltung sowie alle Car2X-Anwendungen dürften meist Dritte anbieten, allgemeine Dienste in Internet zum Suchen und Bereitstellen von Information oder zur Teilnahme an Netzwerken die großen und kleinen Internetanbieter. Diese sind Telemediendienste im Sinn des § 1 Abs. 1 TMG. Das Gleiche gilt auch für Online-Diagnoseservices der Hersteller oder Vertragswerkstätten. Die für ihre Erbringung erforderliche Verarbeitung von personenbezogenen Bestands- oder Nutzungsdaten ist nach §§ 14 oder 15

---

167 Dies fordert z.B. Anhang I der Verordnung (EU) 566/2011 zur Änderung des Anhang I Nr. 2.3.1 der Verordnung (EG) 692/2008 für die OBD-Systeme, die emissionsmindernde Einrichtungen im Kraftfahrzeug steuern.

168 S. näher *Roßnagel* 2014a, 267.

169 Nach § 13 Abs. 2 TMG kann die Einwilligung in den Umgang von Bestands- und Nutzungsdaten auch elektronisch erfolgen – s. hierzu *Jandt/Schaar/Schulz*, in: Roßnagel 2013, § 13 TMG, Rn. 66 ff.

170 S. z.B. *Buchner*, DuD 2015, 372; für Versicherungen *Schwichtenberg*, DuD 2015, 378.

171 S. zu diesem ausführlich *Roßnagel* 2011, 41.

TMG zulässig. Soweit Inhaltsdaten verarbeitet werden, richtet sich die Zulässigkeit nach § 28 Abs. 1 Satz 1 Nr. 1 BDSG.[172]

Die Änderung des Zwecks der Datenverarbeitung oder die Erhebung, Verarbeitung und Nutzung personenbezogener Daten ohne vertragliche Grundlage ist gemäß § 28 Abs. 1 Satz 1 Nr. 2 BDSG zulässig, soweit dies zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt. Ein berechtigtes Interesse, das ausreichend Berücksichtigung finden muss, ist zum Beispiel die Beweisführung mit Daten aus dem Auto. Bestehen Beweisfragen eines Unfalls, eines Verkehrsverstoßes oder einer Vertrags-, Produkt- oder Produzentenhaftung, können oft nur die Daten aus dem Auto Auskunft über das wahre Geschehen oder tatsächliches Verschulden geben.[173] Ein Überwiegen der berechtigten Interessen ist etwa auch dann anzunehmen, wenn die Daten ausschließlich für technische Zwecke genutzt und danach sofort gelöscht werden. Dagegen ist das Überwiegen des berechtigten Interesses bei Zweckänderungen zugunsten von Werbung, Marktforschung, Leistungs- und Verhaltenskontrollen oft zu bezweifeln.[174] Auch dürften die schutzwürdigen Interessen des Betroffenen immer überwiegen, wenn die Daten Rückschlüsse auf persönliches Fahrverhalten, Aufenthaltsorte, Gewohnheiten oder Vorlieben des Betroffenen ermöglichen und sie für längere Zeit aufbewahrt werden sollen. Die Berufung auf berechtigte Interessen rechtfertigt niemals die Erstellung und Nutzung eines umfassenden Persönlichkeitsprofils.[175]

Bei Ortsdaten kommt es darauf an, ob sie vom Endgerät des Fahrzeugs mittels GPS oder vom Telekommunikationsanbieter ermittelt und an den Telemedienanbieter übermittelt werden. Im ersten Fall ist

---

172 S. *Weichert*, SVR 2014, 246; *Kinast/Kühnl*, NJW 2014, 3059; *Buchner*, DuD 2015, 372 ff.
173 S. z.B. *Mielchen*, NVZ 2014, 81 ff., 86; *Balzer/Nugel*, NJW 2016, 193.
174 S. z.B. *Kinast/Kühnl*, NJW 2014, 60; *Roßnagel* 2006, 142.
175 S. z.B. *Roßnagel* 2014a, 269.

ihre Verarbeitung und Nutzung nach § 15 Abs. 1 TMG zulässig, wenn sie für das Erbringen des Dienstes notwendig sind. Im zweiten Fall ist nach § 98 TKG zusätzlich erforderlich, dass die Daten zuvor anonymisiert worden sind oder der Betroffene in die Erhebung und Übermittlung an den Telemediendiensteanbieter eingewilligt hat.[176]

Eine spezialgesetzliche Ermächtigung zur Erhebung und Verarbeitung personenbezogener Daten findet sich für OBD-Systeme in Art. 5 Abs. 3 der Verordnung (EG) 715/2007 und in Art. 4 der Verordnung (EG) 692/2008. Sie wurden durch die Verordnung (EU) 566/2011 und die Verordnung (EU) 459/2012 bestätigt. Die OBD-Systeme müssen sicherstellen, dass die Emissionsminderungssysteme in jedem Kraftfahrzeug ihre Funktion erfüllen[177] und erheben hierfür die für diese Überwachung erforderlichen System- und Betriebsdaten. Diese Daten müssen von Werkstätten, die die Wartung und Instandsetzung durchführen sollen, ausgelesen werden.[178]

Eine zweite spezialgesetzliche Regelung findet sich für eCall-Systeme in Art. 6 der Verordnung (EU) 2015/758 über Anforderungen für die Typgenehmigung zur Einführung des auf dem 112-Notruf basierenden bordeigenen eCall-Systems in Fahrzeugen vom 29. April 2015.[179] In dieser wird die verpflichtende Einführung eines bordeigenen eCall-Systems in bestimmte PKW bis 2018 geregelt. In Art. 6 dieser Verordnung werden bestimmte Vorgaben für den Datenschutz wie eine strenge Zweckbindung der Daten, die Begrenzung der Datenspeicherung auf die Notfallsituation und den Ausschluss der Rückverfolgbarkeit des Autos außerhalb von Notfallsituationen geregelt.

Neben den verantwortlichen Stellen interessieren sich viele Dritte für die Daten aus dem Auto und möchten von den verantwortlichen Stellen die Übermittlung oder Weiterübermittlung dieser Daten errei-

176 S. z.B. *Jandt* 2008, 155 ff.; *Roßnagel* 2014a, 270.
177 S. Anhang IX Nr. 2.5 der Verordnung (EG) 692/2008.
178 S. z.B. *Roßnagel* 2014a, 270.
179 Verordnung (EU) 2015/758 vom 29.4.2015, ABl. L 123/77.

chen.[180] Viele wollen verdeckte Auswertungsmöglichkeiten nutzen, wie zum Beispiel Werberinge. Eine Übermittlung von personenbezogenen Daten an Dritte ist nach § 28 Abs. 2 BDSG im Wesentlichen nur zulässig, wenn die bereits genannten Gründe des § 28 Abs. 1 Satz 1 Nr. 1 oder 2 BDSG bei dem Dritten vorliegen.

Staatliche Stellen haben spezifische, ihnen gesetzlich eingeräumte Zugriffs- oder Informationsrechte, wie etwa Gerichte, Polizei und Nachrichtendienste. Solche Beschlagnahme- oder Zugriffsrechte sind für den Zweck der Strafverfolgung zum Beispiel in §§ 94, 100a, 100f, 100g und 110 StPO geregelt. Für die Gefahrenabwehr finden sich solche Erlaubnisvorschriften vor allem in den Polizeigesetzen der Länder wie etwa in §§ 13 15a und 20 ff. HSOG. Damit stehen die personenbezogenen Daten im Auto diesen Behörden bei einem Verdacht, einer Gefahr oder den Voraussetzungen einer nachrichtendienstlichen Datenerfassung weitgehend offen.

Die Betroffenen können gegenüber den verantwortlichen Stellen eigene Rechte geltend machen. Sie haben Rechte auf Einflussnahme (Berichtigung, Sperrung, Löschung, Unterlassung nach § 35 BDSG) und Transparenz (Benachrichtigung und Auskunft nach §§ 33 und 34 BDSG). Eventuell können sie zusätzlich die Herausgabe von Daten und die Möglichkeit ihrer Nutzung fordern[181] und Schadensersatz nach § 7 BDSG oder § 823 Abs. 1 und 2 BGB verlangen.

2.4.1.2 Smart Home

Bereichsspezifisches Datenschutzrecht im Kontext des Smart Home ist derzeit noch selten. Dies mag darin begründet liegen, dass die aus datenschutzrechtlicher Sicht problematischsten Ausformungen eines Smart Home sich bisher höchstens in einem prototypischen Stadium ihrer Entwicklung befinden. Den Rahmen für den Betrieb eines Smart Home geben in Deutschland aus datenschutzrechtlicher Sicht insbe-

[180] S. Kap. 1.4.1.
[181] S. näher *Roßnagel* 2014a, 275 ff.

sondere §§ 13 ff. und 28 ff. BDSG, §§ 14 ff. TMG und §§ 95 ff. TKG vor.[182]

Auch Gerichte haben den Bereich des Smart Home bisher nur sehr spärlich adressiert. So hat etwa das Bundesverfassungsgericht bisher lediglich festgestellt, dass unvernetzte Steuerungsanlagen vom geltenden Recht unproblematisch handhabbar sind: „Soweit ein derartiges System nach seiner technischen Konstruktion lediglich Daten mit punktuellem Bezug zu einem bestimmten Lebensbereich des Betroffenen enthält – zum Beispiel nicht vernetzte elektronische Steuerungsanlagen der Haustechnik –, unterscheidet sich ein staatlicher Zugriff auf den vorhandenen Datenbestand qualitativ nicht von anderen Datenerhebungen. In einem solchen Fall reicht der Schutz durch das Recht auf informationelle Selbstbestimmung aus, um die berechtigten Geheimhaltungsinteressen des Betroffenen zu wahren."[183]

Ein besonderer Schutz besteht, wenn durch Anwendungen des Smart Home „besondere Arten personenbezogener Daten" verarbeitet werden. Dies sind nach Art. 3 Abs. 9 BDSG „Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben". In der Praxis besonders relevant dürfte hier die Verarbeitung von Gesundheitsdaten durch telemedizinische Anwendungen sein.[184] Der Katalog der besonders schützenswerten Datenkategorien ist die direkte Umsetzung von Art. 8 Abs. 1 DSRL.

Staatliche Zugriffsrechte auf die Daten des Smart Home ergeben sich seit Dezember 2015 im Rahmen der Vorratsdatenspeicherung nach § 100g Abs. 2 StPO und §§ 113a bis 113g TKG.[185] § 113b Abs. 1 TKG erlaubt die Speicherung von Verkehrsdaten für zehn Wochen und von Standortdaten für vier Wochen. Weitere Zugriffs- und Informationsrechte im Kontext des Smart Home ergeben sich im Rahmen der Si-

182 S. hierzu ausführlich *Skistims* 2016, 366 ff.
183 *BVerfGE* 120, 274 (313 f.).
184 S. hierzu detailliert Kap. 2.4.1.3.
185 S. hierzu ausführlich *Roßnagel*, NJW 2016, 533; s. auch Kap. 2.3.7.2.4.

cherstellung und Beschlagnahme von Gegenständen nach § 94 StPO, der Telekommunikationsüberwachung nach § 100a StPO, der akustischen Wohnraumüberwachung nach § 100c StPO und der Erhebung von Verkehrsdaten nach § 109g Abs. 1 StPO.

Eine umfassende Regelung hat bisher lediglich der Bereich des Smart Metering erfahren. Die entsprechenden Regelungen im deutschen Recht zu Strom- und Gaszählern lassen sich im Wesentlichen auf die Richtlinien 2009/72/EG[186]und 2009/73/EG[187] (als Teil des sog. Dritten Binnenmarktpakets) sowie auf die Richtlinie 2006/32/EG,[188] der wiederum die Richtlinie 2012/27/EU[189] nachfolgte, zurückführen. Für den Bereich der Elektrizitätsversorgung sollte ein Mitgliedsstaat, wenn in ihm die Wirtschaftlichkeitsprüfung positiv ausfällt,[190] „mindestens 80 % der Verbraucher bis 2020 mit intelligenten Messsystemen" ausstatten".[191]

In Deutschland werden die maßgeblichen rechtlichen Regelungen zum Smart Metering nach einer geplanten Neuordnung des rechtlichen Rahmens durch das Gesetz zur Digitalisierung der Energiewende,[192] das als Gesetzentwurf der Bundesregierung vorliegt, im Energiewirtschaftsgesetz (EnWG)[193] und dem neu zu schaffenden Messstellenbetriebsgesetz (MsbG) zu finden sein.[194] Darüber hinaus sollen die

---

186 Richtlinie 2009/72/EG vom 13.7.2009 über gemeinsame Vorschriften für den Elektrizitätsbinnenmarkt, ABl. L 211/55.

187 Richtlinie 2009/73/EG vom 13.7.2009 über gemeinsame Vorschriften für den Erdgasbinnenmarkt, ABl. L 211/94.

188 Richtlinie 2006/32/EG vom 5.4.2006 über Endenergieeffizienz und Energiedienstleistungen, ABl. L 114/64.

189 Richtlinie 2012/27/EU vom 25.10.2012 zur Energieeffizienz, ABl. L 315/1.

190 Ernst & Young, Kosten-Nutzen-Analyse für einen flächendeckenden Einsatz intelligenter Zähler im Auftrag des Bundesministeriums für Wirtschaft und Technologie vom Juli 2013.

191 Anhang I Abs. 2 der Richtlinie 2009/72/EG.

192 Zur Kritik an dem Gesetz s. stellvertretend Verbraucherzentrale Bundesverband 2015; Bundesrat-Drs. 543/15 vom 18.12.2015.

193 Gesetz über die Elektrizitäts- und Gasversorgung vom 7.7.2005, BGBl. I, 1970, 3621.

194 Für eine ausführliche Darstellung der bis zur Neuregelung geltenden Rechtslage s. *Jandt/Roßnagel/Volland*, ZD 2011, 99.

Vorschriften des Mess- und Eichgesetzes[195] Messrichtigkeit und Messbeständigkeit gewährleisten.

Ein intelligentes Messsystem ist nach der geplanten Neuregelung in § 2 Nr. 7 MsbG definiert als „eine über ein Smart-Meter-Gateway in ein Kommunikationsnetz eingebundene moderne Messeinrichtung zur Erfassung elektrischer Energie, das den tatsächlichen Energieverbrauch und die tatsächliche Nutzungszeit widerspiegelt". In den §§ 21 und 22 MsbG sind konkrete Mindestanforderung zur Ausgestaltung intelligenter Messsysteme enthalten, die ausweislich des § 2 Nr. 6 MsbG „zur Gewährleistung des Datenschutzes, der Datensicherheit und Interoperabilität" festgelegt werden. Insbesondere soll der „Stand der Technik" als Maßstab dienen. Dieser ist nach § 22 Abs. 2 MsbG dann gegeben, wenn durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) erstellte Schutzprofile und Technische Richtlinien eingehalten werden. Den Nachweis der Erfüllung der Vorgaben des § 22 MsbG bietet die verpflichtende Zertifizierung von Smart Meter Gateways durch das BSI nach § 24 MsbG.

Von besonderer Bedeutung ist die in §§ 30 und 31 MsbG enthaltene gesetzliche Pflicht zum Einbau von intelligenten Messsystemen vorbehaltlich der technischen und wirtschaftlichen Vertretbarkeit. Der Einbau ist nach § 29 MsbG verpflichtend für „Letztverbraucher mit einem Jahresstromverbrauch über 6000 Kilowattstunden" sowie bei Letztverbrauchern, mit denen eine Vereinbarung nach § 14a EnWG besteht, und bei „Anlagenbetreibern mit einer installierten Leistung über 7 Kilowatt". Möglich ist der Einbau nach § 31 Abs. 3 MsbG aber auch bei Letztverbrauchern mit einem niedrigeren Jahresstromverbrauch.

Die datenschutzrechtlichen Regelungen wandern infolge der Neuregelung von den wegfallenden §§ 21g und 21h EnWG in die §§ 49 ff.

[195] Gesetz über das Inverkehrbringen und die Bereitstellung von Messgeräten auf dem Markt, ihre Verwendung und Eichung sowie über Fertigpackungen vom 25.7.2013, BGBl. I, 2722, 2723.

MsbG. § 53 MsbG zu den Informationsrechten des Nutzers entspricht dabei im Wesentlichen § 21h EnWG. § 49 MsbG benennt die zum Umgang mit den erhobenen Daten berechtigen Stellen, während § 50 MsbG detailliert die Grundlagen für die Erhebung, Verarbeitung und Nutzung benennt.[196] Die Messintervalle bezüglich entnommener Elektrizität sollen nach § 55 MsbG grundsätzlich viertelstündlich erfolgen. § 46 MsbG enthält eine Verordnungsermächtigung zur näheren Ausgestaltung bestimmter Aspekte der im Messstellenbetriebsgesetz enthaltenen Regelungen.[197]

2.4.1.3 Smart Health

Ein einheitliches Schutzkonzept für Smart Health existiert nicht, denn die rechtlichen Schutzkonzepte für Wearable Computing und E-Health-Anwendungen unterscheiden sich sehr. Werden Wearables und die dazugehörigen Apps von privaten Unternehmen ohne eine medizinische Zielsetzung angeboten, gelten allein die Datenschutzvorschriften des Telemediengesetzes und des allgemeinen Datenschutzrechts. Für E-Health-Anwendungen existiert dagegen ein deutlich umfangreicheres Schutzkonzept, da für den Telematik-Bereich spezifische Vorschriften in unterschiedlichen Gesetzen zu berücksichtigen sind. Diese weisen jeweils einen bestimmten Fokus auf und gehen von einer konkreten Situation aus. Während das Datenschutzrecht und die ärztliche Schweigepflicht auf personenbezogene Daten bzw. auf Gesundheitsinformationen abzielen, richtet sich das E-Health-Gesetz an informationstechnische Infrastrukturen im medizinischen Bereich. Aufgrund der Einbindung der elektronischen Gesundheitskarte als wesentlicher Baustein des E-Health enthält das E-Health-Gesetz auch – einige wenige – datenschutzrechtliche Vorschriften.

---

[196] Dies sind neben der Einwilligung des Anschlussnutzers die Erforderlichkeit zur Erfüllung von Verträgen, anlässlich vorvertraglicher Maßnahmen, zur Erfüllung rechtlicher Verpflichtungen und im Rahmen der Ausübung hoheitlicher Befugnisse.

[197] § 2 Nr. 27 MsbG definiert eine Zählerstandsgangmessung als „die Messung einer Reihe viertelstündig ermittelter Zählerstände von elektrischer Arbeit und stündlich ermittelter Zählerstände von Gasmengen“.

Schließlich finden sich im SGB V besondere Vorschriften für den Sozialdatenschutz.

2.4.1.3.1 Datenschutzrecht

Der Gesundheitsbereich hat datenschutzrechtlich seit jeher eine Sonderstellung erfahren. Diese ist bereits im Bundesdatenschutzgesetz angelegt, indem Gesundheitsdaten gemäß § 3 Abs. 9 BDSG den besonderen Arten personenbezogener Daten zugerechnet werden. Diese Datenkategorie wird bereits im Bundesdatenschutzgesetz durch spezifische Vorschriften geschützt,[198] da aufgrund des mit ihnen verbundenen Verwendungszusammenhangs von ihrer Sensitivität ausgegangen wird.[199] Darüber hinaus sind in mehreren weiteren Gesetzen spezifische Datenschutzvorschriften für den Gesundheitsbereich angesiedelt. Diese Zersplitterung ist vornehmlich dem deutschen Gesundheitssystem geschuldet insbesondere mit unterschiedlichen Leistungserbringern, wie zum Beispiel Ärzten und Krankenhäusern, und Leistungsträgern, wie den gesetzlichen und privaten Krankenversicherungen. Adressatenbezogen sind insbesondere spezifische Datenschutzvorschriften für den Gesundheitsbereich in den Krankenhausgesetzen der Länder[200] sowie in 10. Kapitel „Versicherungs- und Leistungsdaten, Datenschutz, Datentransparenz“ des SGB V.

Je nachdem, in welchem Kontext der Umgang mit den Gesundheitsdaten erfolgt, werden die Begriffe der Patientendaten und der Sozialdaten verwendet. Beide dieser Datenkategorien weisen Schnittmengen mit den Gesundheitsdaten gemäß § 3 Abs. 9 BDSG auf. Der Begriff der Patientendaten wird in den Krankenhausgesetzen der Länder verwendet, ohne dass eine Legaldefinition vorgenommen wird. Entstanden ist er aus dem Kontext des Behandlungsvertrags zwischen Arzt

---

198 S. im Einzelnen §§ 4a Abs. 3, 4d Abs. 5 Nr. 1, 13 Abs. 2, 14 Abs. 5 und Abs. 6, 16 Abs. 1 Nr. 2 Satz 2, 28 Abs. 6 bis 9, 30a Abs. 1 Satz 2 und 42a Nr. 1 BDSG.

199 Umfassend hierzu unter Hervorhebung des Systemwiderspruchs, Datenkategorien besonders hervorzuheben, *Simitis*, in: Simitis 2014, § 3 BDSG, Rn. 250 ff.

200 Zu den unterschiedlichen Bezeichnungen dieser Gesetze in den verschiedenen Bundesländern s. *Jandt/ Roßnagel/Wilke,* RDV 2011, 225.

und Patienten, der seit dem Inkrafttreten des Patientenrechtegesetzes im Februar 2013 in § 630a BGB als eigenständige Vertragsform ausdrücklich normiert ist.[201] Der Umgang mit Patientendaten ergibt sich unmittelbar aus der Dokumentationspflicht des Arztes gemäß § 630f BGB. Demnach ist der Behandelnde verpflichtet, zum Zweck der Dokumentation in unmittelbarem zeitlichem Zusammenhang mit der Behandlung eine Patientenakte in Papierform oder elektronisch zu führen. Dieser Begriff der Patientendaten wird von den datenschutzrechtlichen Vorschriften der Krankenhausgesetze der Länder aufgegriffen[202] und der Umgang mit den Patientendaten deutlich beschränkt, zum Beispiel gemäß § 12 HKHG. § 67 Abs. 1 SGB X definiert Sozialdaten als personenbezogene Daten, die von Sozialleistungsträgern erhoben, verarbeitet und genutzt werden. Zu diesen zählen unter anderem die gesetzlichen Krankenversicherungen. In diesem Sozialversicherungsverhältnis werden regelmäßig zum Beispiel medizinische Diagnosen, Rezepte über Medikamente und Behandlungen und behandelnde Ärzte verarbeitet, die als Sozial- und als Gesundheitsdaten zu qualifizieren sind.[203] Sozialdaten unterliegen gemäß § 35 SGB I dem Sozialgeheimnis und der Umgang mit ihnen ist nur unter den Voraussetzungen der §§ 67 bis 85a SGB X zulässig.

Im Bundesdatenschutzgesetz werden für Gesundheitsdaten höhere Anforderungen an die datenschutzrechtliche Einwilligung gestellt; es bestehen besondere Erlaubnisvorschriften und eine besonders strenge Zweckbindung.[204] Eine Verpflichtung zusätzliche technische Schutzmaßnahmen bei einem Umgang mit Gesundheitsdaten vorzunehmen, besteht über die allgemein verpflichtenden technisch-organisatorischen Maßnahmen gemäß der Anlage zu § 9 BDSG nicht. Schließlich statuiert § 42a Nr. 2 BDSG eine Informationspflicht der verantwortlichen Stelle gegenüber den Aufsichtsbehörden und den Betroffenen,

---

201 *Bergmann/Middendorf*, in: Bergmann/Pauge/Steinmeyer 2014, § 630a BGB, Rn. 1 ff.
202 In den §§ 630a ff. BGB finden sich keine datenschutzrechtlichen Vorschriften.
203 S. ausführlich *Kühling/Seidel,* in: Kingreen/Kühling 2015, 38 ff.
204 S. die §§ 4a Abs. 3, 13 Abs. 2, 28 Abs. 6 bis 9 und 29 Abs. 5 BDSG.

wenn personenbezogene Daten, die einem Berufsgeheimnis unterliegen, Dritten unrechtmäßig zur Kenntnis gelangen.

Die datenschutzrechtlichen Erlaubnistatbestände für Gesundheitsdaten richten sich entweder an die medizinischen Berufsgruppen – insbesondere die Vorschriften in den Krankenhausgesetzen der Länder und § 28 Abs. 7 BDSG – oder gehen in Bezug auf andere verantwortliche Stellen von einem Vorrang der Einwilligung aus und normieren in der nachrangigen Erlaubnisvorschrift hohe Anforderungen.[205] Die Sondervorschriften für Gesundheitsdaten schließen den Umgang mit ihnen auf der Grundlage von allgemeinen Erlaubnisvorschriften aus. Das Bundessozialgericht vertritt zudem, dass die krankenversicherungsrechtlichen Vorschriften zum Sozialdatenschutz in den §§ 284 ff. SGB V abschließend sind. Gesetzliche Krankenversicherungen können daher Übermittlungen von Sozialdaten ihrer Versicherten an private Dienstleister zur Rechnungserstellung nicht über eine datenschutzrechtliche Einwilligung legitimieren.[206] Sofern die Vorschriften des Sozialgesetzbuches für andere Zwecke eine Einwilligung vorsehen, muss sie sich gemäß § 4a Abs. 3 BDSG ausdrücklich auf Gesundheitsdaten beziehen.

Nutzt eine Person Wearables, um Vital- und Fitnessdaten zu erheben und anschließend mit einer Gesundheits- oder Fitness-App auf seinem Endgerät lokal auszuwerten, handelt es sich bei den Daten, wie zum Beispiel Pulsfrequenz, Herzschlag und Insulinwert, zumindest teilweise um Gesundheitsdaten. Solange diese Daten nur dem Betroffenen selbst zugänglich sind und von ihm nicht weitergegeben werden, liegt kein datenschutzrechtlich relevanter Verarbeitungsvorgang vor. Werden die Daten durch die Nutzung einer Gesundheits- oder Fitness-App automatisch an den Server oder in die Cloud des Anbieters übermittelt, greift das Schutzprogramm des Datenschutzrechts für Ge-

[205] S. § 28 Abs. 6 BDSG, der auf den Schutz lebenswichtiger Interessen, offenkundig öffentlich gemachte Daten, die Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche und die Durchführung wissenschaftlicher Forschung abstellt.

[206] *BSGE* 102, 134.

sundheitsdaten. Die datenschutzrechtlichen Erlaubnistatbestände für Gesundheitsdaten richten sich entweder an die medizinischen Berufsgruppen – insbesondere die Vorschriften in den Krankenhausgesetzen der Länder und § 28 Abs. 7 BDSG – oder gehen in Bezug auf andere verantwortliche Stellen von einem Vorrang der Einwilligung aus und normieren in der nachrangigen Erlaubnisvorschrift hohe Anforderungen.[207] Die Sondervorschriften für Gesundheitsdaten schließen den Umgang mit ihnen auf der Grundlage von allgemeinen Erlaubnisvorschriften aus und eine Einwilligung muss sich gemäß § 4a Abs. 3 BDSG ausdrücklich auf Gesundheitsdaten beziehen. Beim Umgang mit Gesundheitsdaten durch Apps dürfen diese Sondervorschriften nicht unterlaufen werden. Da die Voraussetzungen von § 28 Abs. 6 BDSG in der Regel nicht vorliegen werden, kommt allenfalls eine wirksame Einwilligung der Betroffenen als Legitimierung in Betracht. Durch das nicht eindeutige Verständnis der Gesundheitsdaten und die nicht für die Anwendbarkeit auf Apps ausgerichteten Erlaubnistatbestände besteht eine hohe Rechtsunsicherheit hinsichtlich eines datenschutzkonformen Umgangs mit diesen sensitiven Daten. Des Weiteren tritt auch in diesem Kontext das Problem ausländischer Anbieter der Apps zutage, die die deutschen oder auch europäischen Datenschutzvorschriften nicht umsetzen.

Für den E-Health-Bereich wird das datenschutzrechtliche Schutzniveau vorrangig durch die spezifischen Datenschutzvorschriften der Krankenhausgesetze der Länder und des Sozialrechts bestimmt. Ergänzend sind die Vorschriften des Bundesdatenschutzgesetzes zu berücksichtigen.

2.4.1.3.2 Ärztliche Schweigepflicht

Für den Gesundheitsbereich weist die ärztliche Schweigepflicht einen engen sachlichen Zusammenhang zum Datenschutzrecht auf. Bei die-

[207] S. § 28 Abs. 6 BDSG, der auf den Schutz lebenswichtiger Interessen, offenkundig öffentlich gemachte Daten, die Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche und die Durchführung wissenschaftlicher Forschung abstellt.

ser stehen nicht Daten und deren – elektronische oder digitale – Verarbeitung im Fokus, sondern allgemein Informationen, die dem Arzt im Rahmen einer Behandlung vom Patienten anvertraut werden und Dritten nicht zur Kenntnis gelangen sollen. Datenschutzrecht und Geheimnispflicht begrenzen den zulässigen Umgang mit diesen Daten bzw. Informationen und verfolgen das identische Schutzziel der Vertraulichkeit. § 1 Abs. 3 Satz 2 BDSG ordnet die Parallelgeltung dieser beiden Regelungskomplexe durch die Feststellung an, dass Verpflichtungen zur Wahrung von Berufsgeheimnissen, die nicht auf gesetzlichen Vorschriften beruhen, von den datenschutzrechtlichen Vorschriften unberührt bleiben.

Die ärztliche Schweigepflicht ist gesetzlich nicht geregelt. Sie wird aber auf § 203 StGB und das allgemeine Persönlichkeitsrecht des Patienten gestützt.[208] Ausdrücklich gefordert wird die Verschwiegenheitspflicht in § 9 Abs. 1 Muster-Berufsordnung für die deutschen Ärztinnen und Ärzte (MBO-Ä). Danach ist der Arzt standesrechtlich verpflichtet, über ihm anvertraute oder bekannt gewordene Tatsachen zu schweigen. Der strafrechtlichen Schweigepflicht gemäß § 203 StGB unterliegen neben dem Arzt auch Angehörige eines anderen Heilberufs, der für die Berufsausübung oder die Führung der Berufsbezeichnung eine staatlich geregelte Ausbildung erfordert. Diesen Personen stehen ihre berufsmäßig tätigen Gehilfen und die Personen gleich, die bei ihnen zur Vorbereitung auf den Beruf tätig sind.[209] Eine Verletzung der ärztlichen Schweigeplicht kann gemäß § 203 Abs. 1 Nr. 1 StGB mit Freiheitsentzug bis zu einem Jahr bestraft werden.[210] Außerdem kann gegen den Arzt gemäß § 70 Abs. 1 StGB ein Berufsverbot verhängt werden. Die Rechtswidrigkeit der Tat und somit die Strafbarkeit des Arztes entfällt nur dann, wenn der durch das Geheimnis Geschützte – also der Patient – wirksam in die Offenbarung der Geheimnisse eingewilligt hat oder wenn gesetzliche Offenbarungspflichten beste-

---

208 *Deutsch*, AcP 1992 (192), 162 ff.

209 Zum weiteren Inhalt und Umfang der ärztlichen Schweigepflicht s. *Jandt/Roßnagel*, MedR 2011, 140.

210 S. z.B. *Abel*, in: Roßnagel 2003, 1336.

hen.[211] Im Kontext der ärztlichen Verschwiegenheitspflicht wird die Erteilung der Befugnis zur Weitergabe von Patientengeheimnissen regelmäßig als Erklärung zur Entbindung von der ärztlichen Schweigepflicht bezeichnet.[212]

Die ärztliche Schweigepflicht unterstellt ebenso wie die Datenschutzvorschriften, dass Gesundheitsdaten überwiegend von Schweigepflichtigen und besonders sensibilisierten Personen sowie in geschützten Umgebungen erhoben werden. Zu nennen sind insbesondere Ärzte, Arzthelfer, Krankenschwestern und Pfleger in Krankenhäusern, Seniorenheimen und Arztpraxen, von Gesundheits- und Pflegediensten, in Apotheken sowie Kranken- und Lebensversicherungen.[213] Im Ergebnis wird die Weitergabe dieser Informationen zweifach abgesichert und ein Verstoß hiergegen hat nicht nur die datenschutzrechtlichen Konsequenzen von §§ 43 und 4 BDSG zur Folge, sondern wirkt sich unmittelbar strafrechtlich aus. Dieses Schutzkonzept greift wiederum nur für E-Health-Anwendungen, nicht aber für Wearables. Bei diesen sind die den Vorschriften zugrundeliegenden Annahmen gerade nicht gegeben. Die Gesundheitsdaten werden nicht im Rahmen der ärztlichen Behandlung erhoben, sondern von jeder Person selbst in allen denkbaren Alltagssituationen. Die ärztliche Schweigepflicht entfaltet bei Wearables keine zusätzliche Schutzfunktion.

2.4.1.3.3 E-Health-Gesetz

Die Entwicklung und Integration moderner Informations- und Kommunikationstechnologien zur Verbesserung der Qualität und Wirtschaftlichkeit der medizinischen Versorgung fordert eine Infrastruktur mit klaren rechtlichen Rahmenbedingungen, die die Beteiligten in der Gesundheitsversorgung so miteinander verbindet, dass sie sicher und schnell miteinander kommunizieren können. Nachdem nach 20 Jahren

---

[211] Die Möglichkeit der Einwilligung wird bei § 203 StGB aus der Formulierung „unbefugt" abgeleitet.

[212] S. z.B. ULD Schleswig-Holstein, https://www.datenschutzzentrum.de/medizin/arztprax/entbind.htm. Diese Formulierung findet sich aber nicht in den Gesetzen.

[213] S. auch *Schaffland/Wiltfang,* BDSG 2015, § 3 BDSG, Rn. 107.

des Ringens zum 1.1.2015 die elektronische Gesundheitskarte als ein wesentlicher Baustein der Telematik-Infrastruktur eingeführt wurde, ist am 29.12.2015 das Gesetz für sichere digitale Kommunikation und Anwendungen im Gesundheitswesen (E-Health-Gesetz) in Kraft getreten.[214] Dieses umfasst dezidierte Vorgaben für die digitale Transformation des Gesundheitswesens, die von den Akteuren im Gesundheitswesen bei der Realisierung von Anwendungen der Telemedizin umzusetzen sind. Dieser Rechtsrahmen für eine sichere Telematik-Infrastruktur ist zwar nicht auf den Datenschutz fokussiert, dennoch finden sich einige bereichsspezifische Regelungen vor allem in Bezug auf den Umgang mit den auf der elektronischen Gesundheitskarte gespeicherten Patientendaten und Sozialdaten, wie zum Beispiel die Änderung des § 291a SGB V. Obwohl die spezifischen datenschutzrechtlichen Regelungen für die elektronische Gesundheitskarte letztlich nur in einer einzigen Vorschrift konzentriert worden sind, enthält § 291a SGB V detaillierte Anforderungen an den Umgang mit den auf ihr gespeicherten Daten.[215] Durch die grundsätzliche Unterscheidung zwischen Pflichtanwendungen gemäß Abs. 2 und freiwilligen Anwendungen der Karte gemäß Abs. 3 wird es dem Versicherten ermöglicht, den Umfang der gespeicherten Daten zu beschränken. Abs. 4 legt in einer abschließenden Aufzählung den zugriffsberechtigten Personenkreis fest und sichert diese faktisch durch die insbesondere in Abs. 5 vorgeschriebenen technischen Zugriffsschutzmaßnahmen. Ergänzend bestimmt Abs. 5c Stellen, die für die Bestätigung der Zugriffsberechtigungen zuständig sind. Die gesetzlichen Erlaubnistatbestände für den Datenzugriff sind in Abs. 5a normiert. Schließlich sind in Abs. 6 Löschungsansprüche und -rechte sowie Protokollpflichten und in Abs. 8 ein zusätzlicher Schutz vor missbräuchlicher Verwendung vorgesehen.

Die durch das E-Health-Gesetz eingeführten Gesetzesänderungen wirken sich nur auf den Entwicklungsbereich der Telematik im Ge-

214 BGBl. I, 2408.

215 S. hierzu *Hornung*, in: Hänlein/Kruse/Schuler 2012, § 291a, Rn. 5 ff.

sundheitswesen aus. Wearables und Gesundheits- und Fitness-Apps werden grundsätzlich nicht durch das E-Health-Gesetz adressiert. Sollten diese aber mit dem Einsatz elektronischer Gesundheitskarten gekoppelt werden, zum Beispiel indem sie über eine Schnittstelle von Wearables für die sichere Datenspeicherung verwendet werden, sind die Vorschriften des E-Health-Gesetzes zu beachten. Bisher scheint aber gerade dies von den Entwicklern der Fitness- und Gesundheits-Apps vermieden zu werden, um die mit dem E-Health-Gesetz verbundenen deutlich höheren Sicherheitsanforderungen nicht erfüllen zu müssen.

2.4.1.3.4 Medizinproduktegesetz

Das Medizinproduktegesetz (MPG) soll gemäß § 1 MPG den Verkehr mit Medizinprodukten regeln und dadurch für die Sicherheit, Eignung und Leistung der Medizinprodukte sowie die Gesundheit und den erforderlichen Schutz der Patienten, Anwender und Dritten sorgen. Gemäß § 3 Nr. 1 MPG sind Medizinprodukte definiert als alle einzeln oder miteinander verbunden verwendeten Instrumente, Apparate, Vorrichtungen, Software, Stoffe und Zubereitungen aus Stoffen oder andere Gegenstände. Neben der Hardware wird auch die für ein einwandfreies Funktionieren erforderliche Software umfasst, wenn sie dazu bestimmt ist, einen der in der Norm angeführten Zwecke zu erfüllen.[216] Dabei kommt es bezüglich der Zweckbestimmungen eines Produkts gemäß § 3 Nr. 10 MPG maßgeblich auf die Herstellerangaben an.[217] Zahlreiche Medizinprodukte, wie zum Beispiel Insulinpumpen, Herzschrittmacher, Blutzuckermessgeräte oder Hörgeräte, enthalten bereits datenverarbeitende Komponenten und diese werden gerade auch vor dem Hintergrund zunehmender Individualisierung und

---

[216] Gemäß § 3 Nr. 1 a) bis d) MPG sind dies die Erkennung, Verhütung, Überwachung, Behandlung oder Linderung von Krankheiten, die Erkennung, Überwachung, Behandlung, Linderung oder Kompensierung von Verletzungen oder Behinderungen, die Untersuchung, Ersetzung oder Veränderung des anatomischen Aufbaus oder eines physiologischen Vorgangs oder die Empfängnisregelung.

[217] *EuGH*, EuZW 2013, 117; *BGH*, NJW-RR 2014, 46; *Rehmann*, in: Rehmann/Wagner 2010, § 3 MPG, Rn. 11 m.w.N.

Lernfähigkeit der Geräte stetig zunehmen. Dennoch wurden in das Medizinproduktegesetz keine spezifischen Regelungen für den Umgang mit den personenbezogenen Daten aufgenommen. Lediglich § 2 Abs. 4 MPG trifft die Feststellung, dass Rechtsvorschriften über Geheimhaltung und Datenschutz unberührt bleiben.[218] Insofern wird die Parallelgeltung sowohl des allgemeinen und spezifischen Datenschutzrechts als auch der standesrechtlichen und strafrechtlichen Geheimhaltungspflicht explizit angeordnet. Die Einordnung als Medizinprodukt kann sich allerdings immer dann auswirken, wenn die gesetzlichen Datenschutzvorschriften Raum für eine Interessenabwägung lassen. Der Fokus von Medizinprodukten liegt auf der ordnungsgemäßen Funktionsfähigkeit sowie der ordnungsgemäßen Datenverarbeitung, um Gefahren durch fehlerhafte Datenverarbeitung für die Gesundheit und das Leben der Patienten zu vermeiden.[219] Letztlich sind daher die informationelle Selbstbestimmung und das Recht auf Leben und körperliche Unversehrtheit gegeneinander abzuwägen. Vor diesem Hintergrund wird zum Beispiel dem Grundsatz der Datensparsamkeit eine deutlich geringere Bedeutung zukommen. Besonders aufgrund der datenzentrierten Patientenbehandlung ist es sehr wichtig, dass die zur Behandlung benötigten Daten jederzeit verfügbar und unverändert sind und dass diese sensitiven Daten von Unbefugten nicht zur Kenntnis genommen werden können.[220]

Ebenso wie das E-Health-Gesetz findet das Medizinproduktegesetz nur auf den E-Health-Bereich Anwendung. Die Hersteller von Wearables sowie die Anbieter von Gesundheits- und Fitness-Apps sind bemüht, die Einordnung als Medizinprodukt zu vermeiden, um die höheren Sicherheitsanforderungen nicht umsetzen zu müssen.

---

218 S. *Spyra,* MPR 2015, 15 (18f.).
219 *Spyra*, MPR 2015, 15 (16).
220 *Spyra*, MPR 2015, 15 (16).

2.4.1.3.5 Zugriffbefugnisse

Staatliche Stellen haben auf die bei Smart Health erhobenen und gespeicherten Gesundheitsdaten grundsätzlich die gleichen Zugriffs- und Informationsrechte wie bei anderen Datenkategorien, so dass auf die Ausführungen zu Smart Car verwiesen werden kann.[221] Lediglich bei Telekommunikationsdiensten stellen die relevanten Vorschriften mit § 100g StPO höhere Zugriffsanforderungen an die Verkehrsdaten gegenüber den Bestandsdaten, über die gemäß § 100j StPO Auskunft verlangt werden kann. Die datenschutzrechtliche Differenzierung zwischen personenbezogenen Daten und besonderen Arten personenbezogener Daten wird bei den Zugriffsbefugnissen nicht aufgegriffen. § 97 Abs. 1 Nr. 2 StPO normiert allerdings ein Beschlagnahmeverbot für Aufzeichnung, zu denen auch Ton-, Bild- und Datenträger gehören,[222] und Nr. 3 für Gegenstände, auf die sich ein Zeugnisverweigerungsrecht erstreckt. Voraussetzung ist gemäß § 97 Abs. 2 StPO, dass sich die Aufzeichnungen und Gegenstände im Gewahrsam des zur Zeugnisverweigerung Berechtigten befinden. Auch die Erhebung von Verkehrsdaten ist gemäß § 100g Abs. 4 Satz 1 StPO unzulässig, wenn sie sich gegen einen Berufsgeheimnisträger richtet, dem gemäß § 53 Abs. 1 Satz 1 Nr. 1 bis 5 StPO ein Zeugnisverweigerungsrecht zusteht, und die weiteren Voraussetzungen vorliegen. Bestimmten Berufsträgern wird gemäß § 53 StPO ein Zeugnisverweigerungsrecht zugestanden. Gemäß Nr. 3 der Vorschrift zählen zu den Zeugnisverweigerungsberechtigten Ärzte und ähnliche Berufe im Gesundheitsbereich. Gemäß § 35a StPO erstreckt sich das Zeugnisverweigerungsrecht auch auf Hilfspersonen der Ärzte.

Für den Smart Health-Bereich ergibt sich somit ein differenziertes Bild hinsichtlich der staatlichen Zugriffsbefugnisse. Auf Gesundheitsdaten, die im Rahmen des Wearable Computing durch den Betroffenen selbst erhoben und gegebenenfalls von den App-Anbieter gespeichert und verarbeitet werden, ist über die genannten strafprozessualen Vor-

[221] S. Kap. 2.4.1.1.
[222] *BVerfG*, NStZ 2002, 377.

schriften der Zugriff grundsätzlich zulässig. Befinden sich die Gesundheitsdaten dagegen im E-Health-Bereich im Gewahrsam eines Arztes oder werden auf dessen Geräten generiert und gespeichert, schließt das Zeugnisverweigerungsrecht gemäß § 53 Abs. 1 Nr. 3 StPO den staatlichen Zugriff aus.

2.4.2 Big Data-Analysen

Ausdrückliche Regelungen zu Big Data finden sich im Datenschutzrecht bisher nicht. Big Data berührt aber viele Bereiche und Regelungen des Datenschutzrechts. Dienen Big Data-Analysen der Effizienzsteigerung in der Industrie, erfordert dies voraussichtlich den Umgang mit Beschäftigtendaten. Für diese existiert mit § 32 BDSG zumindest eine bereichsspezifische Vorschrift, durch die der Umgang mit personenbezogenen Daten im Beschäftigungsverhältnis geregelt wird. Für den Einsatzbereich Medizin kann auf die bereichsspezifischen Vorschriften für E-Health verwiesen werden. Soll individuelles Wählerverhalten analysiert werden kommen sowohl das Wahlgeheimnis aus Art. 38 Abs. 1 Satz 1GG als auch das allgemeine und das für das Internet spezifische Datenschutzrecht in Betracht.[223] Das Bundesdatenschutzgesetz ist auch maßgeblich für den Einsatzbereich des Marketings. Bereichsspezifische Vorschriften bestehen allerdings für das weite Einsatzfeld der öffentlichen Sicherheit und Gefahrenabwehr. Diese obliegt der Zuständigkeit der Strafverfolgungsbehörden und der Polizei. Hierbei handelt es sich um öffentlich-rechtliche Stellen. Für den Bereich der Gefahrenabwehr sind die Polizeigesetze des Bundes und der Länder maßgeblich, die jeweils bereichsspezifische Datenschutzvorschriften normieren, wie die §§ 21 bis 37 BPolG[224] oder die §§ 13 bis 16 HSOG. Erfolgt die Big Data-Analyse zu Zwecken der Strafverfolgung, sind die Vorschriften der Strafprozessordnung vorrangig gegenüber dem Bundesdatenschutzgesetz. In dieser finden sich bereichs-

---

223 Hierzu ausführlich *Richter*, DÖV 2013, 961.

224 Gemäß § 37 BPolG finden §§ 3 Abs. 2 und 8 Satz 1, 4 Abs. 2 und 3, 4b, 4c, 10 Abs. 1, 13, 14 Abs. 1, 2 und 5, 15, 16, 18 Abs. 2 Satz 2 und 3 sowie 19a und 20 BDSG keine Anwendung.

spezifische Vorschriften für den Umgang mit personenbezogenen Daten nicht zusammengefasst in einem Kapitel, sondern sie sind über das Gesetz verteilt, etwa in § 100g StPO für die Erhebung von Verkehrsdaten, § 100j StPO für die Bestandsdatenauskunft oder § 163d StPO für die Speicherung und den Abgleich von Daten aus Kontrollen.

2.4.2.1 Big Data-Analysen mit personenbezogenen Daten

Wird Big Data angewendet, um personenbezogene Merkmale zu prognostizieren, indem anonyme Ergebnisse von Big Data-Analysen auf eine Person angewendet werden oder indem eine Big Data-Analyse von Anfang an personenbezogen betrieben wird, ist diese Datenverarbeitung an den gesetzlichen Erlaubnistatbeständen zu messen, soweit keine Einwilligung der Betroffenen vorliegt, die diese Prognosen aus den vorhandenen Daten erlaubt.

2.4.2.1.1 Private Stellen

Für den Bereich der Privatwirtschaft kommen insbesondere die Tatbestände des § 28 BDSG in Frage. Für die Profilbildung im Zusammenhang mit bestehenden Schuldverhältnissen kommt § 28 Abs. 1 Satz 1 Nr. 1 BDSG in Frage, für die Profilbildung außerhalb von Schuldverhältnissen insbesondere Nr. 2 und Nr. 3. Nach diesen Erlaubnistatbeständen wird die Profilbildung mit Big Data-Techniken oder aufgrund von anonymen Big Data-Ergebnissen häufig rechtswidrig sein. Im Rahmen von Nr. 1 wird sie häufig für den konkreten Verarbeitungszweck (zum Beispiel Bestellung einer bestimmten Ware) nicht erforderlich sein. Im Rahmen von Nr. 2 wird die Interessenabwägung häufig zugunsten der schutzwürdigen Interessen der Betroffenen ausschlagen. Im Rahmen von Nr. 3 können zwar veröffentlichte Daten erhoben werden. Allerdings stellt die Auswertung dieser Daten zur Merkmalserkennung einen neuen Verarbeitungsschritt dar, bei dem die im Rahmen der Vorschrift notwendige Interessenabwägung ebenfalls häufig zugunsten der Betroffenen ausschlagen dürfte.[225] Dies

[225] *Weichert*, ZD 2013, 251 (257).

wird insbesondere dann der Fall sein, wenn bewusst nicht offenbarte Merkmale oder sogar emotionale Zustände für die Verhaltenssteuerung prognostiziert werden.

§ 28b BDSG stellt besondere Anforderungen an Verfahren, mit denen Wahrscheinlichkeitsprognosen für das Verhalten von Personen errechnet werden, wenn diese Prognosen zur Entscheidung über die Begründung, Durchführung oder Beendigung eines Vertragsverhältnisses eingesetzt werden. Die Norm regelt, und gestattet damit im Rahmen ihrer Voraussetzungen, insbesondere das Scoring, das darauf gerichtet ist, ob ein potentieller Vertragspartner seine Zahlungspflichten erfüllen wird, zum Beispiel bei Krediten oder anderen Dauerschuldverhältnissen.[226] Nicht durch § 28b BDSG gestattet ist das Scoring von Stellenbewerbern, da der im Verhältnis zu § 28 BDSG speziellere § 32 BDSG nicht in § 28b Nr. 2 BDSG (sogleich) genannt ist.[227] Die Norm ist insgesamt auf Entscheidungen über Vertragsverhältnisse beschränkt.

§ 28b BDSG stellt in Nr. 1 bis 4 Anforderungen an die Verfahren. Für den Fall der Berechnung des Wahrscheinlichkeitswerts durch eine Auskunftei müssen die Voraussetzungen für eine Übermittlung der genutzten Daten nach § 29 BDSG und in allen anderen Fällen die Voraussetzungen einer zulässigen Nutzung der Daten nach § 28 BDSG vorliegen. Die zur Berechnung des Wahrscheinlichkeitswerts genutzten Daten müssen nach wissenschaftlich anerkannten mathematisch-statistischen Verfahren nachweisbar für die Berechnung der Wahrscheinlichkeit des bestimmten Verhaltens erheblich sein. Für die Berechnung des Wahrscheinlichkeitswerts dürfen nicht ausschließlich Anschriftendaten genutzt werden. Im Fall der Nutzung von Anschriftendaten muss der Betroffene vor Berechnung des Wahrscheinlichkeitswerts über die vorgesehene Nutzung dieser Daten unterrichtet worden werden. Diese Anforderungen gelten im Anwendungsbereich des § 28b BDSG auch für Big Data-Verfahren.

---

226 *Mackenthun*, in: Taeger/Gabel 2013, § 28b BDSG, Rn. 6.
227 *Ehmann*, in: Simitis 2014, § 28b BDSG, Rn. 2 ff.

§ 30a BDSG regelt die Zulässigkeit des Umgangs mit personenbezogenen Daten zur geschäftsmäßigen Markt- und Meinungsforschung. Diese stellt nach der Gesetzesbegründung eine wichtige Entscheidungsgrundlage für wirtschaftliche und politische Akteure dar.[228] Adressaten der Norm sind alle Anbieter von Markt- und Meinungsforschung, die geschäftsmäßig handeln, also nicht nur einmal, sondern wiederholt[229] derartige Forschung betreiben. Was Markt- und Meinungsforschung genau ist, definiert das Gesetz nicht. Die amtliche Begründung stellt sie folgendermaßen dar: „Sie stellt für öffentliche und private Auftraggeber mittels wissenschaftlicher Methoden und Techniken notwendige Informationen als empirische Grundlage und zur Unterstützung wirtschaftlicher, gesellschaftlicher und politischer Entscheidungen bereit … ."[230] Damit kommen alle Stellen in Frage, die personenbezogene Daten erheben, um damit Aussagen über das Verhalten der Bevölkerung für eigene Zwecke oder die Zwecke anderer Stellen zu gewinnen.[231] § 30a BDSG ist damit die zentrale Erlaubnisvorschrift für alle Stellen, deren Geschäftsmodell die Merkmalserkennung mittels Big Data ist oder die sich hierauf spezialisieren, um andere Zwecke strategisch zu unterstützen.

Für die Zwecke der Markt- und Meinungsforschung ist der Umgang mit personenbezogenen Daten durch geschäftsmäßige Markt- und Meinungsforscher gemäß § 30a Abs. 1 BDSG zulässig, wenn kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Erhebung, Verarbeitung oder Nutzung hat, oder die Daten aus allgemein zugänglichen Quellen entnommen werden können oder die verantwortliche Stelle sie veröffentlichen dürfte und das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Erhebung, Verarbeitung oder Nutzung gegenüber

---

228 BT-Drs. 16/13657, S. 19f.; hierzu *Munz*, in: Taeger/Gabel 2013, § 30a BDSG, Rn. 2; *Ehmann*, in: Simitis 2014, § 30a BDSG, Rn. 4.

229 *Ehmann*, in: Simitis 2014, § 30a BDSG, Rn. 56.

230 BT-Drs. 16/13657, S. 19f.

231 *Munz*, in: Taeger/Gabel 2013, § 30a BDSG, Rn. 13.

dem Interesse der verantwortlichen Stelle nicht offensichtlich überwiegt.

Gemäß § 30a Abs. 2 BDSG dürfen Daten, die für Zwecke der Markt- und Meinungsforschung erhoben werden, nur für diese Zwecke verarbeitet oder genutzt werden. Sie sind gemäß Abs. 3 Satz 1 zu anonymisieren, sobald dies nach dem Zweck des Forschungsvorhabens möglich ist und gemäß Satz 2 bis dahin zu pseudonymisieren. Diese Regelungen sollen verhindern, dass die statistischen Schlüsse, die aus den Daten gewonnen werden, zur personalisierten Ansprache verwendet werden können. Dies ist ein Geschäftsmodell, das mit Big Data-Verfahren technisch massenhaft möglich wird. Es ist von § 30a BDSG aber gerade nicht erlaubt.

Big Data-Verfahren können auch im Hinblick auf Beschäftigungsverhältnisse relevant werden. § 32 Abs. 1 Satz 1 BDSG erlaubt den Umgang mit personenbezogenen Daten soweit dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung erforderlich ist. Weitere Anforderungen enthält Abs. 1 nicht. Werden mit Big Data immer mehr Indikatoren für unerwünschtes zukünftiges Verhalten entdeckt, wird es aus Sicht der Arbeitgeber auch erforderlich erscheinen, diesen Indikatoren in der Bewerbungsphase oder durch Verarbeitung der Beschäftigtendaten nachzuspüren. Dabei kann der Personenbezug anonym errechneter Indikatoren auch rein menschlich, nämlich durch Beobachten oder Nachfragen, hergestellt werden.[232] Gemäß § 32 Abs. 2 BDSG besteht auch gegen solche nicht automatisierte Verarbeitungen grundsätzlich Schutz. Die Kontrolle solcher nicht automatisierter Datenverarbeitungen dürfte aber sehr schwer umzusetzen sein.

Im Bewerbungsverfahren gelten bezüglich des Nachfragens schon lange besondere Regeln. Bestimmte Fragen, zum Beispiel nach einer Schwangerschaft, gelten als unzulässig und müssen nicht wahrheits-

[232] S. hierzu Kap. 1.2.4.

getreu beantwortet werden.[233] Die Rechtslage zum ausdrücklichen Erfragen von Merkmalen ist damit relativ eindeutig. Allerdings bietet Big Data die Möglichkeit, immer neue Indikatoren für Merkmale herauszufinden und statt der Merkmale diese Indikatoren abzufragen. Allerdings ist das Fragerecht dadurch beschränkt, dass die abgefragte Information selbst für die Ausübung der Tätigkeit erheblich sein muss.[234] Zu bestimmen, welche Indikatoren dabei zulässig sein sollen und auf welche Merkmale sie jeweils verweisen, dürfte in Zukunft eine große Herausforderung für die Rechtsprechung sein.

§ 32 Abs. 1 Satz 2 BDSG enthält besondere Anforderungen für den Umgang mit Beschäftigtendaten zur Aufdeckung von Straftaten, insbesondere tatsächliche Anhaltspunkte für eine Straftat im Beschäftigungsverhältnis. Zu beachten ist, dass gemäß Abs. 2 bei der Aufdeckung von Straftaten vor der ersten Datenanalyse ein tatsächlicher Anhaltspunkt für strafbares Verhalten vorliegen muss. Präventive Massenscreenings der Mitarbeiter, für die sich Big Data durchaus eignen würde, erlaubt die Norm keineswegs.[235]

2.4.2.1.2 Öffentliche Stellen: Big Data in der Strafverfolgung und Gefahrenabwehr

Anwendungsfelder im öffentlichen Bereich, für die sich Potentiale durch Big Data ergeben, sind insbesondere die Gefahrenabwehr und die Strafverfolgung. Sie stehen daher für den öffentlichen Bereich im Zentrum der Untersuchung.

Die Polizei hat die Aufgaben der Gefahrenabwehr und der Strafverfolgung. Ihre Befugnisse im Bereich der Strafverfolgung sind bundeseinheitlich in der Strafprozessordnung geregelt. Im Bereich der Gefahrenabwehr sind die Befugnisse in den Polizeigesetzen des Bundes und der Länder geregelt. Im Folgenden werden sie am Beispiel des Polizei-

---

233 Überblick m.w.N. bei *Seifert*, in: Simitis 2014, § 32 BDSG, Rn. 32 ff.

234 *Linck*, in: Schaub 2015, § 26, Rn. 16.

235 *Seifert*, in: Simitis 2014, § 32 BDSG, Rn. 103; *Zöll*, in: Taeger/Gabel, 2013, § 32 BDSG, Rn. 49.

gesetzes des Landes Hessen auf ihre Vereinbarkeit mit Big Data-Verfahren untersucht.

Für die Gefahrenabwehr ist die Erhebung personenbezogener Daten nach § 13 HSOG zulässig, wenn sie zur Abwehr einer Gefahr erforderlich ist. Als Gefahr gilt dabei eine Situation, die bei ungehindertem Geschehensablauf mit hinreichender Wahrscheinlichkeit in einen Schaden für ein geschütztes Rechtsgut münden würde.[236] Die Erhebung personenbezogener Daten zur Gefahrenabwehr ist damit auf konkrete Einzelfälle beschränkt. Daneben darf die Polizei Daten aus öffentlich zugänglichen Quellen erheben, wie zum Beispiel aus öffentlichen Profilen in sozialen Netzwerken. Die Erhebung aus öffentlich zugänglichen Quellen stellt keinen Grundrechtseingriff dar. Allerdings bedarf das gezielte Zusammentragen und Auswerten solcher Daten einer Rechtsgrundlage.[237] Gemäß § 13 Abs. 5 HSOG ist aber jede Erhebung personenbezogener Daten zu unbestimmten oder noch nicht bestimmbaren Zwecken ausdrücklich unzulässig. Auch die Erhebung von Telekommunikationsdaten ist nach § 15a HSOG nur bei Vorliegen einer gegenwärtigen Gefahr für Leib, Leben oder Freiheit einer Person im konkreten Einzelfall und einer richterlichen Anordnung zulässig. Eine Datenerhebung, die dazu dient, Big Data zu sammeln, um sie später für noch unbekannte Zwecke auszuwerten, ist somit zur Gefahrenabwehr nicht zulässig.

Für die Strafverfolgung ist das Erheben von öffentlich zugänglichen Informationen aus dem Internet grundsätzlich ohne Ermächtigungsgrundlage zulässig, allerdings nur im Rahmen eines konkreten Ermittlungsverfahrens. Diese Daten dürfen jedoch nicht dazu genutzt werden, gezielt personenbezogene Daten zur Erstellung von Persönlichkeitsprofilen zusammenzutragen.[238] Die Erhebung von Telekommunikationsinhalten nach § 100a StPO und von Verkehrsdaten nach § 100g

---

236 *Pieroth/Schlink/Kniesel* 2012, § 4, Rn. 1; ähnlich: *Thiel* 2014, § 4 Rn. 2; *Gusy* 2011, § 3, Rn. 101.

237 *BVerfGE* 120, 274 (344f.); *Schulz/Hoffmann*, DuD 2012, 7 (11).

238 *BVerfGE* 120, 274 (345).

StPO ist nur im Einzelfall beim Verdacht einer schweren Straftat aus einem abschließenden Straftatenkatalog zulässig. Auch die Vorgaben zur Strafverfolgung erlauben daher nicht die anlasslose Erhebung von Big Data zur künftigen Auswertung.

Personenbezogene Daten, die zur Gefahrenabwehr erhoben wurden, sind gemäß § 27 Abs. 2 HSOG zu löschen, wenn sie dafür nicht mehr erforderlich sind. Daten, die nach §§ 100a oder 100g StPO erhoben wurden, sind gemäß § 101 Abs. 8 Satz 1 StPO zu löschen, wenn sie nicht mehr für die Strafverfolgung oder eine gerichtliche Überprüfung der Maßnahme benötigt werden. Zufallsfunde für weitere Verfahren sind nicht zu löschen, dürfen aber nur für diese Verfahren verwendet werden.[239] Eine Bevorratung mit personenbezogenen Daten für die Auswertung mit Big Data-Verfahren zu noch unbestimmten Zwecken ist daher im Bereich der Gefahrenabwehr und der Strafverfolgung unzulässig.

Eine Auswertung von zulässigen Datenbeständen mit Hilfe von Big Data-Analysen könnte im Rahmen von Rasterfahndungen zulässig sein. Rasterfahndungen nach § 26 HSOG sind jedoch nur bei konkreten Gefahren für hochrangige Rechtsgüter wie den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib, Leben oder Freiheit einer Person zulässig, nicht bei allgemeinen Bedrohungslagen.[240] Rasterfahndungen nach § 98a StPO sind nur bei tatsächlichen Anhaltspunkten für eine Katalogstraftat von erheblicher Bedeutung zulässig. Selbst dann müssen weitere Schutzvorkehrungen eingehalten werden, wie die strenge Zweckbindung der Daten, die Löschung der Daten gemäß § 101 Abs. 8 Satz 1 StPO, sobald der Zweck erreicht ist, und die Benachrichtigung der Betroffenen gemäß § 101 Abs. 4 Nr. 4 ff. und Abs. 5 StPO, sobald der Ermittlungszweck hierdurch nicht mehr gefährdet wird.[241] Eine Auswertung aller der Polizei aufgrund ihrer Datenerhebungsbefugnisse zur Verfügung stehenden Daten zur per-

---

239 *Bruns*, in: Hannich 2013, § 101, Rn. 39.
240 *BVerfGE* 115, 320 (357).
241 S. hierzu *Greven*, in: Hannich 2013, § 98b StPO, Rn. 7 ff.

sonenbezogenen Rasterfahndung mit Big Data ist im Aufgabenbereich der Polizei damit nicht zulässig. Ungeklärt ist allerdings die Frage, wie die Polizei Merkmale für Rasterfahndungen festlegen darf. Hierzu könnten mit Big Data-Verfahren Datenbestände nach Mustern durchsucht werden, die keinen Personenbezug (mehr) aufweisen. So könnten Verhaltensweisen und Persönlichkeitsmerkmale aufgedeckt werden, die mittelbare statistische Hinweise auf strafbares Verhalten sein können. Würden nur anonyme Daten genutzt, fiele diese Merkmalserkennung nicht unter den Schutz personenbezogener Daten.

2.4.2.1.3 Gemeinsame Vorschriften für private und öffentliche Stellen

§ 15 Abs. 3 Satz 1 TMG erlaubt die Profilbildung aus Nutzungsdaten. Diese Profilbildung kann grundsätzlich auch mit Big Data durchgeführt werden. Allerdings verbietet § 15 Abs. 3 Satz 3 TMG, die erstellten Profile wieder mit den Identifizierungsdaten zusammenzuführen. Zwar würde ein Personenbezug des Big Data-Profils bestehen, weil der Diensteanbieter die Identifizierungsdaten nicht vernichten muss. Er darf jedoch den Personenbezug zum erstellten Profil nicht aktualisieren.[242] Daher erlaubt auch § 15 Abs. 3 TMG im Ergebnis keine personenbezogene Profilbildung mit Big Data.

§ 6a BDSG enthält das Verbot automatisierter Einzelentscheidungen. Die Norm beruht auf Art. 15 DSRL. Sie soll verhindern, dass Menschen zum Objekt reiner Datenverarbeitungsprozesse ihrer Datenprofile werden und dafür sorgen, dass in Entscheidungsverfahren Menschen als Entscheider eine Rolle spielen und die Betroffenen ihren individuellen Standpunkt einbringen können.[243] Damit berührt die Norm Big Data, denn Big Data verstärkt die Möglichkeiten der automatisierten Entscheidungsfindung, zum Beispiel für individuelle Vertragsschlüsse (Leistungsausfallrisiko eines Käufers oder Kreditnehmers, Zuverlässigkeit eines Arbeitnehmers) erheblich.

---

[242] S. hierzu *Dix/Schaar*, in: Roßnagel 2013, § 15 TMG, Rn. 61 ff.
[243] *Scholz*, in: Simitis 2014, § 6a BDSG, Rn. 3.

§ 6a Abs. 1 Satz BDSG schreibt vor, dass Entscheidungen, die für den Betroffenen eine rechtliche Folge nach sich ziehen oder ihn erheblich beeinträchtigen, nicht ausschließlich auf die automatisierte Verarbeitung personenbezogener Daten zu stützen sind, die der Bewertung einzelner Persönlichkeitsmerkmale dienen. Als rechtliche Folge kann insbesondere ein belastender Verwaltungsakt gelten. Entscheidungen im Zusammenhang mit einem Vertragsschluss, etwa die Ablehnung des Vertragsschlusses mit dem Betroffenen, stellen hingegen keine Rechtsfolge dar, sind aber als erhebliche Beeinträchtigung zu qualifizieren.[244] Gemäß Satz 2 liegt eine ausschließlich auf eine automatisierte Verarbeitung gestützte Entscheidung insbesondere dann vor, wenn eine inhaltliche Bewertung und auf diese Bewertung gestützte Entscheidung eines Menschen nicht stattfinden. Die Vorschrift ist grundsätzlich auf Big Data-Verfahren anwendbar. Big Data wird insbesondere eingesetzt, um Persönlichkeitsmerkmale zu prognostizieren. Die Vorschrift legt damit fest, dass Big Data-Profiling allein nicht die Grundlage für die Bewertung von Menschen sein darf, wenn für diese hieraus rechtliche Folgen oder erhebliche Beeinträchtigungen erwachsen. Um Entscheidungsvorschläge zu generieren, zum Beispiel eine Vorsortierung im Stellenbesetzungsverfahren zu treffen, darf es grundsätzlich eingesetzt werden.[245] Findet allerdings eine automatisierte Vorauswahl statt, in der Bewerber nicht nur in einer Rangliste strukturiert werden, sondern bestimmte Bewerber aufgrund der angelegten Kriterien aussortiert werden, liegt ein Anwendungsfall des § 6a Abs. 1 BDSG vor.[246] Solche Vorauswahlprozesse werden mit Big Data möglicherweise stark zunehmen. Sie sind nach § 6a Abs. 1 BDSG grundsätzlich nicht zulässig.

Abs. 2 erlaubt abweichend von Abs. 1 die rein automatisierte Entscheidung, wenn die Entscheidung im Rahmen des Abschlusses oder der Erfüllung eines Vertragsverhältnisses oder eines sonstigen Rechts-

---

244 *Kamlah*, in: Plath 2013, § 6a BDSG, Rn. 6f.; *Scholz*, in: Simitis 2014, § 6a BDSG, Rn. 27.
245 *Kamlah*, in: Plath 2013, § 6a BDSG, Rn. 5; BT-Drs. 14/4329.
246 *Scholz*, in: Simitis 2014, § 6a BDSG, Rn. 16.

verhältnisses ergeht und dem Begehren des Betroffenen stattgegeben wird oder wenn die Wahrung der berechtigten Interessen des Betroffenen durch geeignete Maßnahmen gewährleistet ist und die verantwortliche Stelle dem Betroffenen die Tatsache des Vorliegens einer automatischen Einzelentscheidung sowie auf Verlangen die wesentlichen Gründe dieser Entscheidung mittteilt und erläutert.

Als Maßnahme zur Wahrung der berechtigten Interessen der Betroffenen gilt gemäß Art. 15 Abs. 2 lit. a) DSRL insbesondere ein Verfahren, bei dem zwar eine rein automatisierte Entscheidung getroffen wird, der Betroffene aber die Möglichkeit hat, seinen Standpunkt einzubringen. Eine solche Überprüfung im Nachhinein hat in jedem Fall unter Beteiligung eines Menschen stattzufinden.[247]

Das in § 34 BDSG niedergelegte Auskunftsrecht des Betroffenen über den Umgang mit ihn betreffenden personenbezogenen Daten enthält in Abs. 2 Satz 1 besondere Anforderungen bezüglich einer Verarbeitung nach § 28b BDSG. In diesem Fall muss Auskunft erteilt werden über die innerhalb der letzten sechs Monate vor dem Zugang des Auskunftsverlangens erhobenen oder erstmalig gespeicherten Wahrscheinlichkeitswerte, über die zur Berechnung der Wahrscheinlichkeitswerte genutzten Datenarten sowie einzelfallbezogen und nachvollziehbar in allgemein verständlicher Form über das Zustandekommen und die Bedeutung der Wahrscheinlichkeitswerte.

Auch diese Anforderungen beziehen sich im Anwendungsbereich des § 28b BDSG auf Big Data-Verfahren und sind für sie passend, denn Big Data-Verfahren werden häufig eingesetzt, um statistisch begründete Wahrscheinlichkeitsprognosen abzugeben. Fraglich ist, was unter dem Tatbestandmerkmal „Zustandekommen" genau zu verstehen ist. Gemäß § 6a Abs. 3 BDSG schließt das Auskunftsrecht die Auskunft über den logischen Aufbau der automatisierten Datenverarbeitung ein. In Frage kommt dadurch grundsätzlich sowohl die Auskunft über die Gewichtung der verwendeten Daten als auch die Auskunft über die

[247] *Scholz*, in: Simitis 2014, § 6a BDSG, Rn. 32.

Rechenformel für den Score-Wert. An beidem haben aber die verarbeitenden Stellen ein Geheimhaltungsinteresse, da durch die Veröffentlichung Wettbewerbsvorteile gegenüber Konkurrenten verloren gehen könnten. Der Bundesgerichtshof hat Anfang 2014 beides mit Hinweis auf den Schutz von Geschäftsgeheimnissen dem Auskunftsanspruch entzogen.[248]

2.4.2.2 Big Data-Analysen ohne personenbezogenen Daten

Anonyme oder anonymisierte Datenverarbeitung wird vom Datenschutzrecht nicht reglementiert.

§ 30a BDSG ermöglicht, dass zunächst personenbezogene Daten in anonymisierter Form statistisch ausgewertet werden, um Merkmalserkennung zu betreiben. Diese anonymen Merkmale können unter Umständen sehr leicht wieder Personen zugeordnet werden. Dies ist bei äußerlichen Merkmalen auch durch Menschen möglich. Eine personenbezogene Anwendung von Merkmalen und Indikatoren aus Big Data durch Menschen ist für nicht-öffentliche Stellen gemäß § 1 Abs. 2 Nr. 2 BDSG aus dem Anwendungsbereich des BDSG ausgeschlossen und wäre auch kaum zu kontrollieren. Die anonyme Merkmalserkennung mit Big Data bildet hierfür die Grundlage und könnte dieses Risiko deutlich ausweiten und vertiefen. § 30a BDSG bildet die gesetzliche Grundlage hierfür.

Soweit Big Data ohne Personenbezug arbeitet, ist es derzeit grundsätzlich unbeschränkt möglich. Dabei ist aber zu bedenken, dass die faktischen Anforderungen an eine Anonymisierung im Sinne von § 3 Abs. 6 BDSG durch Big Data steigen und keinesfalls durch das bloße Entfernen von Namen und Adressen erfüllt sein dürften.

---

248 *BGH*, BKR 2014, 193.

3 Datenschutzrechtliche Regelungsdefizite

Nachdem im vorherigen Kapitel das geltende Datenschutzrecht und dessen Anwendung auf die „smarten" Informationstechniken im Alltag und auf die neuen technischen Auswertungsmöglichkeiten des Big Data vorgestellt wurden, werden in diesem Kapitel die Regelungsdefizite des geltenden Datenschutzrechts untersucht. Hierbei stehen sowohl die allgemeinen Regelungen zu Erlaubnistatbeständen und Datenschutzprinzipien als auch die nicht erfassten Grundrechtsrisiken in den Beispielsanwendungen des Smart Car, des Smart Home und des Smart Health sowie von Big Data-Anwendungen im Mittelpunkt.

3.1 Datenschutzrichtlinie

Das augenscheinlichste Defizit der Datenschutzrichtlinie liegt in ihrem Alter begründet. Die Richtlinie entstammt dem Jahr 1995 und damit einer Zeit, in der die technischen Möglichkeiten zur Erhebung und Verarbeitung personenbezogener Daten noch relativ überschaubar waren. Die konzeptionelle Basis der Richtlinie entstammt sogar im Wesentlichen den 1970er Jahren, als auf nationalstaatlicher Ebene erste Datenschutzgesetze verabschiedet wurden.[249] Geradezu explodiert sind seither nicht nur die Möglichkeiten zur Speicherung und Auswertung von Informationen, sondern auch die Möglichkeiten, über verschiedenste Sensoren und Erfassungssysteme[250] diese überhaupt erst zu gewinnen.[251] Eine weitere Entwicklung ist das zunehmende Bezahlen durch personenbezogene Daten. Ohne geldliche Gegenleistung angebotene Dienste dienen letztlich lediglich als Datensammelstelle. Sie nutzen alle erreichbaren Daten und nutzen sie für alle Zwecke, die einen die Gestehungskosten für den angebotenen Dienstes weit übersteigenden Gewinn versprechen.[252] Diese Entwicklungen konnten im Rahmen des Entstehungsverfahrens der Richtlinie nur in sehr begrenz-

[249] Den Anfang machte 1970 das Hessische Datenschutzgesetz.
[250] Wie z.B. Suchmaschinen, Netzwerke, Messenger u.a.
[251] S. hierzu Kap. 1.
[252] S. hierzu kritisch *Roßnagel* 2014b, 57 ff.

tem Maße antizipiert und berücksichtigt werden. Defizite ergeben sich bei der Richtlinie deshalb nicht nur in Detailfragen, sondern bereits auf konzeptioneller Ebene.

Insbesondere besteht bei den grundlegenden Datenschutzprinzipien der Transparenz, der Zweckbindung, der Erforderlichkeit und der Datensparsamkeit eine Inkompatibilität mit bestimmten bestehenden oder im Entstehen begriffenen Geschäftsmodellen.[253]

Ein weiteres strukturelles Problem besteht bei der Beschränkung des Anwendungsbereichs des Datenschutzrechts im Allgemeinen und der Richtlinie im Besonderen auf personenbezogene Daten (Art. 1 Abs. 1 DSRL). Eine Aufweichung dieses Prinzips etwa im Sinne einer Herausnahme bestimmter Datengruppen aus dem Anwendungsbereich ist nicht möglich; vielmehr stünden ihr in Deutschland verfassungsrechtliche Vorgaben, insbesondere die informationelle Selbstbestimmung, entgegen.[254] In der Beschränkung auf personenbezogene Daten ist ein Defizit zu sehen, denn sie bedeutet, dass Erfassung und Verarbeitung anonymer Informationen nicht in die Regelungsmaterie der Datenschutzrichtlinie fällt. Angesichts der Effekte, die auch der Umgang mit anonymen Daten haben kann, insbesondere in den Bereichen der Normung und Verhaltensprognose im Kontext von Big Data, stellt sich die Frage, ob nicht auch für solche Daten ein Schutzkonzept erstellt werden sollte.

Die Europäische Kommission nannte 2010 in einer Mitteilung neben der fortschreitenden technischen Entwicklung als Kernprobleme des geltenden europäischen Datenschutzrechts eine „unzureichende Harmonisierung", „Unklarheiten bezüglich des für die Verarbeitung geltenden Rechts und der Zuweisung der Verantwortung" bei Datenver-

253 S. ausführlich Kap. 3.2.2.
254 Ausführlich *Roßnagel*, digma 2011, 160.

arbeitung über die Grenzen der Europäischen Union hinweg sowie unzureichende Befugnisse der Datenschutzbehörden.[255]

Der Spielraum, der letztlich zu der gerügten unzureichenden Harmonisierung führte, war indes bei Erlass der Richtlinie durchaus gewollt. So heißt es in Erwägungsgrund 9 DSRL: „Die Mitgliedstaaten besitzen einen Spielraum, der im Rahmen der Durchführung der Richtlinie von den Wirtschafts- und Sozialpartnern genutzt werden kann. Sie können somit in ihrem einzelstaatlichen Recht allgemeine Bedingungen für die Rechtmäßigkeit der Verarbeitung festlegen. Hierbei streben sie eine Verbesserung des gegenwärtig durch ihre Rechtsvorschriften gewährten Schutzes an." Dieser Spielraum ergibt sich letztlich aus Art. 5 DSRL, wonach die Umsetzung der Richtlinie „nach Maßgabe" der Art. 6 bis 21 DSRL zu erfolgen hat. Der so ausformulierte Rahmen kann und muss – unter Beachtung der Tatsache, dass eine Vollharmonisierung durch die Richtlinie vorliegt – ausgefüllt werden. Die bezeichneten Artikel enthalten eine Reihe von raumlassenden Formulierungen, die schließlich zur Etablierung höchst unterschiedlicher Datenschutzniveaus in den der Richtlinie unterworfenen Staaten geführt haben. Die Richtlinie kann deshalb als insgesamt zu abstrakt bezeichnet werden. Gewollt war durch die Richtlinie ein Wettbewerb, bei dem die betroffenen Staaten mit durch den eingeräumten Spielraum ermöglichten unterschiedlichen Detailkonzepten um den bestmöglichen Datenschutzstandard konkurrieren. Stattdessen nutzten einzelne Staaten den Spielraum zur Etablierung niedriger Datenschutzstandards, um damit ihrer Wirtschaft einen Wettbewerbsvorteil zu ermöglichen.

Ein weiteres zentrales Defizit der Datenschutzrichtlinie ist ihr räumlich beschränkter Anwendungsbereich. Sie knüpft den Anwendungsbereich an das Niederlassungsprinzip und ist damit nicht auf Datenverarbeitungen anwendbar, die von Niederlassungen gesteuert wer-

[255] Mitteilung der Kommission zu einem Gesamtkonzept für den Datenschutz in der Europäischen Union, KOM(2010), 609, S. 4. Ein erster Bericht zur Umsetzung der Richtlinie war 2003 erschienen: Kommission, Erster Bericht über die Durchführung der Datenschutzrichtlinie (95/46/EG), KOM(2003), 265.

den, die außerhalb der 31 Staaten, in denen die Richtlinie gilt, liegen. Angesichts der Tatsache, dass die Mehrzahl der bedeutendsten datenverarbeitenden Unternehmen der Welt nicht in diesen Staaten niedergelassen sind und personenbezogene Daten regelmäßig über die Grenzen des EWR hinweg übermittelt werden, sind der Wirksamkeit der Richtlinie Grenzen gesetzt.

Zudem hat sich der Sanktionsmechanismus der Richtlinie weitgehend als stumpfes Schwert erwiesen. Nach Art. 24 DSRL ergreifen die Mitgliedstaaten „geeignete Maßnahmen, um die volle Anwendung der Bestimmungen dieser Richtlinie sicherzustellen, und legen insbesondere die Sanktionen fest, die bei Verstößen gegen die zur Umsetzung dieser Richtlinie erlassenen Vorschriften anzuwenden sind." In Deutschland kann der Verstoß gegen die Vorgaben des Bundesdatenschutzgesetzes als wesentlichem die Datenschutzrichtlinie umsetzenden Gesetz nach § 43 Abs. 3 BDSG mit einer Geldbuße von bis zu 300.000 Euro geahndet werden. Diese vergleichsweise niedrige Summe hat sich in der Vergangenheit als in der Praxis nicht ausreichend erwiesen, da sie aufgrund der Deckelung nur unzureichend mit der wirtschaftlichen Leistungsfähigkeit des Verstoßenden skaliert.

Insgesamt ist festzustellen, dass die Datenschutzrichtlinie den Herausforderungen allgegenwärtiger und potenziell alle Lebensbereiche durchdringender moderner Datenerfassung nicht gewachsen ist; ihre Vorgaben haben sich trotz angestrebter Technikneutralität als inflexibel erwiesen. Es droht „die Kapitulation des Datenschutzrechts vor der Komplexität des Internets".[256]

3.2 Spezifisches und allgemeines nationales Datenschutzrecht

Aufgrund der nationalen Systematik des Datenschutzrechts kann es aus verschiedenen Gründen zu datenschutzrechtlichen Regelungsdefiziten kommen. Auf der faktischen Ebene entstehen sie insbesondere aufgrund der Entwicklung einer neuen Technik mit Datenverarbei-

[256] So *Rogall-Grothe*, ZRP 2012, 193 (195).

tung und ihrer Integration in neue Einsatzbereiche, wie die in diesem Gutachten aufgegriffenen Bereiche verdeutlichen. Sofern personenbezogene Daten verarbeitet werden, besteht nicht die Gefahr, dass keine Datenschutzvorschriften zu beachten sind. Aber es kann sein, dass der Schutzbedarf für bestimmte Datenverarbeitungen in bestimmten Anwendungsbereichen höher ist als das Schutzniveau des allgemeinen Datenschutzrechts.[257]

Sofern spezifische Datenschutzvorschriften fehlen oder die anwendbaren Regelungen bezogen auf eine konkrete Technik nicht zu risikoadäquaten Lösungen führen, erfüllt das Datenschutzrecht die an es gestellten Erwartungen nicht. Gesetze sollen den Schutzbedarf für Grundrechte absichern und die aus ihm abgeleitete Schutzpflicht des Staates erfüllen. Im Vordergrund steht hier der Schutz der informationellen Selbstbestimmung. Es sind aber auch allgemein die Verhaltensfreiheit und der Gleichheitsgrundsatz zu berücksichtigen. Die Perspektive der datenverarbeitenden Stelle darf insofern nicht außer Betracht bleiben, als die Datenschutzvorschriften für sie als Garant für Rechts- und Innovationssicherheit fungieren sollen.

3.2.1 Erlaubnistatbestände

Das Datenschutzrecht sieht zwei Möglichkeiten zur Legitimierung des Umgangs mit personenbezogenen Daten vor – gesetzliche Erlaubnisvorschriften und die individuelle Einwilligung. Die datenschutzrechtlichen Erlaubnistatbestände erkennen den Umstand an, dass in einer modernen Gesellschaft in Verwaltung, Justiz, Unternehmen und im privaten Lebensbereich der Umgang mit personenbezogenen Daten notwendig und vorteilhaft ist. Ziel des Datenschutzrechts ist es nicht, jeglichen Umgang mit personenbezogenen Daten zu unterdrücken, sondern das Recht auf informationelle Selbstbestimmung der Betroffenen zu wahren und die sich häufig widersprechenden Interessen zwischen ihnen und den datenverarbeitenden Stellen in einen angemessenen Ausgleich zu bringen. Im öffentlichen Bereich könnten die

[257] S. zum Konzept des Regelungsdefizits das Vorwort.

gesetzlich zugewiesenen Aufgaben ohne den Umgang mit personenbezogenen Daten nicht erfüllt werden. Im privatrechtlichen Bereich setzen Unternehmen seit Jahrzehnten Datenverarbeitungssysteme zur Optimierung ihrer Prozessabläufe ein. Zahlreiche Unternehmensgründungen und Geschäftsmodelle basieren nahezu ausschließlich auf dem Umgang mit personenbezogenen Daten. Ist der Umgang mit personenbezogenen Daten in bestimmten Anwendungsbereichen und für eine Vielzahl gleichgelagerter Datenverarbeitungsvorgänge notwendig und sinnvoll, vereinfacht eine entsprechende gesetzliche Erlaubnisvorschrift den Weg zur datenschutzrechtlichen Zulässigkeit deutlich. Die Einwilligung übernimmt im Verhältnis zu den gesetzlichen Erlaubnistatbeständen eine Ausfüllungsfunktion. Über sie besteht immer noch die Möglichkeit, den Umgang mit personenbezogenen Daten zu legitimieren, die von den gesetzlichen Erlaubnisvorschriften nicht erfasst werden.

Für die datenschutzrechtlichen Erlaubnistatbestände können einige allgemeine Regelungsdefizite festgestellt werden. Aufgrund des enorm gestiegenen Umfangs an Datenverarbeitungsvorgängen, der verschwimmenden Grenzen zwischen personenbezogenen und nicht personenbezogenen Daten, der Anzahl der Beteiligten und insgesamt der hohen Komplexität der Strukturen wird der Erlass von gesetzlichen Erlaubnisvorschriften immer schwieriger. Diese können nur durch klare tatbestandliche Voraussetzungen neben der Legitimierungs- auch eine Begrenzungswirkung entfalten und gleichzeitig dem Bestimmtheitsgrundsatz genügen.

Entsprechend wird der Umgang mit personenbezogenen Daten faktisch immer häufiger über eine Einwilligung als über eine gesetzliche Erlaubnisvorschrift legitimiert. Hierdurch wird das grundsätzliche Verhältnis zwischen Erlaubnisvorschrift und Einwilligung umgekehrt. Der Gesetzgeber hat die gesetzlichen Erlaubnistatbestände als Regel-

fall und die Einwilligung als Ausnahme vorgesehen.[258] Dies kann insofern als Regelungsdefizit eingestuft werden, als der Staat seine ihm aus dem Grundrecht der informationellen Selbstbestimmung abgeleitete Schutzpflicht vernachlässigt. Gesetzliche Erlaubnistatbestände benennen klare Verantwortlichkeiten, Datenverarbeitungsumfang, zulässige Zwecke, das Korrektiv der Erforderlichkeit und sie können die Legitimierungswirkung von der Einhaltung zusätzlicher technisch-organisatorischer Anforderungen abhängig machen.[259]

Alle diese Einschränkungs- und Konkretisierungsmaßnahmen, durch die letztlich der grundrechtliche Interessenausgleich bewerkstelligt und die informationelle Selbstbestimmung gewährleistet wird, werden bei der datenschutzrechtlichen Einwilligung nur bedingt eingesetzt.[260] Insbesondere die Erforderlichkeit bleibt häufig im Unklaren oder liegt im alleinigen Interesse des Datenverwenders. Ausgleichende technisch-organisatorische Maßnahmen sind regelmäßig bei der Einwilligung ohne Bedeutung. Ursprünglich sollte gerade über die Einwilligungsmöglichkeit die Selbstbestimmung des Betroffenen gestärkt werden. Die Anzahl der Einwilligungen, ihre Bedeutung im Kontext kostenloser Dienstleistungen und schließlich auch die häufig von den Betroffenen nicht unmittelbar wahrnehmbaren Konsequenzen der Einwilligung führen jedoch eher zu einem „Abnicken" durch den Betroffenen, um der Überforderung aus dem Weg zu gehen.[261]

Grundsätzlich richten sich Erlaubnistatbestände an eine konkrete verantwortliche Stelle und nur von zwei Beteiligten aus – dem Verantwortlichen und dem Betroffener – und definieren somit deren Rechte und Pflichten in einem Zweipersonenverhältnis. Die Einbindung eines

---

[258] In der datenschutzrechtlichen Praxis wird dieses Verhältnis zwischen gesetzlichen Erlaubnistatbeständen und der Einwilligung schon seit langem häufig verkannt, in dem regelmäßig „aus Gründen der Rechtssicherheit" der verantwortlichen Stelle zur Einholung von Einwilligungen geraten wird, teilweise ohne das Vorliegen eines gesetzlichen Erlaubnistatbestands vorab zu prüfen oder nach datensparsamen Verarbeitungsalternativen, insbesondere hinsichtlich des Umfangs Daten, zu suchen.

[259] S. z.B. die Erlaubnisvorschrift für das Scoring gemäß § 28b BDSG.

[260] S. zur Einwilligung auch Kap. 3.2.2.2.

[261] S. *Roßnagel/Jandt/Müller/Gutscher/Heesen* 2006, 138.

Dritten kann systematisch nur über die Übermittlung der Daten an einen weiteren Verantwortlichen oder über die in § 11 BDSG normierte Auftragsdatenverarbeitung rechtskonform erfolgen. Bereits das Cloud Computing zeigt sehr deutlich die Anwendungsschwierigkeiten dieser Norm.[262] Der faktischen Komplexität von Datenverarbeitungsprozessen in allen Lebensbereichen zu allen denkbaren – auch sich ändernden und im vorhin nicht definierten Zwecken – mit einer Vielzahl von Beteiligten ist mit dieser Struktur der Erlaubnisvorschriften kaum noch in Einklang zu bringen. Dieses strukturelle Regelungsdefizit der Konstruktion von Erlaubnisvorschriften zeigt sich bereits deutlich im Bereich Smart Energy, wo der Datenschutz durch eine Vielzahl von Vorschriften in unterschiedlichen Gesetzen und durch zahlreiche technische Richtlinien gewährleistet werden soll.[263] Diese Komplexität wird in Zukunft zunehmen. Die datenschutzrechtlichen Erlaubnistatbestände sind bezogen auf die faktisch anzunehmenden Mehrpersonenverhältnisse bei Datenverarbeitungsprozessen defizitär.

3.2.2 Datenschutzprinzipien

Das geltende Datenschutzrecht ist weitgehend geeignet, adäquate Lösungen von Datenschutzkonflikten zu ermöglichen, wenn die Situationen übersichtlich, die Beteiligten auf zwei oder drei Rollen beschränkt und die Zwecke begrenzt sind. „Smarte" Informationstechnik im Alltag und Datenauswertung durch Big Data verändern jedoch die Verwirklichungsbedingungen für Datenschutz. Sie bieten dadurch aber nicht nur neue Handlungsmöglichkeiten zur besseren Durchsetzung der jeweils eigenen – in der Regel bereits mächtigen – Interessen. Sie verändern auch die Form der Interaktion des Menschen mit Infor-

---

[262] S. *Roßnagel* 2015, 21 sowie die „Orientierungshilfe – Cloud Computing" des Arbeitskreises Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Arbeitsgruppe Internationaler Datenverkehr des Düsseldorfer Kreises vom 9.10.2014 insbesondere zur Umsetzung der Kontrollpflicht gemäß § 11 Abs. 2 Satz 4 BDSG, 10f., https://www.datenschutz.rlp.de/downloads/oh/ak_oh_cloudcomputing.pdf.

[263] S. Kap. 2.4.1.2.

mationstechnik grundsätzlich und erzeugen dadurch Verhältnisse in denen

- viele Beteiligte mit ständig wechselnden Rollen beteiligt sind,
- der Personenbezug der Daten unklar ist,
- die Daten nicht in Dateien verarbeitet werden, sondern über viele Stellen verteilt und nur bei Bedarf genutzt werden,
- vielfältige Zwecke gleichzeitig verfolgt werden,
- Daten auch in privaten oder gemischt privaten und geschäftlichen Kontexten verwendet werden,
- die Datenverarbeitung spontan von den Techniksystemen selbst organisiert wird,
- die Datenverarbeitung für den Betroffenen unbemerkt erfolgt und in ihren Wirkungen undurchschaubar ist.

Auf diese neuen Verhältnisse sind die Grundsätze des datenschutzrechtlichen Schutzprogramms kaum anwendbar. Die Ziele, die mit dem Einsatz „smarter" Informationstechnik im Alltag und Big Data verfolgt werden, widersprechen den Zielen, die mit den Prinzipien des Datenschutzrechts verfolgt werden. In dem Konflikt zwischen beiden dürfte entscheidend sein, dass die Anwendungen der „smarten" Informationstechnik im Alltag den Betroffenen in den meisten Fällen nicht aufgedrängt – in diesem Fall dürften die Datenschutzprinzipien greifen –,[264] sondern von diesen gewollt werden. Sie wollen sich mit ihrer Hilfe die Träume erfüllen, die mit „smarter" Informationstechnik im Alltag und Big Data verbunden sind.[265] Sie werden dann als Konsequenz auch damit einverstanden sein müssen, dass die Hintergrundsysteme die notwendige Kenntnis über ihre Lebensweise, Gewohnheiten, Einstellungen und Präferenzen erhalten. Bei Datenauswertungen durch Big Data werden die Betroffenen die Datenverarbei-

[264] S. Kap. 2.4.1.
[265] S. zu diesen ausführlich *Roßnagel* 2007, 13 ff.

tung nur dann merken, wenn diese zu automatisierten Entscheidungen führen. Wenn Big Data-Auswertungen nur zu statistischen Mustern führen, werden sie zwar unter diese subsumiert, sie werden dies aber nicht als Wirkung von Big-Data-Auswertungen erfahren. In diesen neuen Verhältnissen wird das bisherige Schutzprogramm als solches in jedem seiner Bestandteile in Frage gestellt.[266] Dies soll am Beispiel der Prinzipien der Transparenz, der Einwilligung, der Zweckbindung und der Erforderlichkeit erläutert werden.

3.2.2.1 Transparenz

Der Grundsatz der Transparenz fordert, die Daten grundsätzlich bei dem Betroffenen zu erheben und ihn zuvor zu unterrichten. Bei jeder neuen Speicherung ist er zu benachrichtigen. Gegenüber der verantwortlichen Stelle hat er Auskunftsrechte.

Diese Instrumente der Transparenz stoßen künftig an subjektive Grenzen. Allein die zu erwartende Vervielfachung der Datenverarbeitungsvorgänge in allen Lebensbereichen übersteigt die mögliche Aufmerksamkeit um ein Vielfaches. Zudem soll die „smarte" Informationstechnik im Alltag gerade im Hintergrund und damit unmerklich den Menschen bei vielen Alltagshandlungen unterstützen. Niemand würde es akzeptieren, wenn er täglich hundertfach bei meist alltäglichen Verrichtungen Anzeigen, Unterrichtungen oder Hinweise zur Kenntnis nehmen müsste. Würde das Recht dennoch auf solchen Zwangsinformationen bestehen, würde es das Gegenteil von Aufmerksamkeit und Sensibilität erreichen. Und selbst wenn der Betroffene dies wollte, stehen für die Alltagsgegenstände meist keine oder keine adäquaten Ausgabemedien zur Verfügung.

Außerdem setzen hohe Komplexität und vielfältige Zwecke der möglichen Transparenz objektive Grenzen. Für viele Anwendungen wird bei der Datenerhebung unklar sein, ob die Daten personenbezogen sind. Sie erhalten den Personenbezug oft viel später. Eine einzelne Er-

[266] S. hierzu bezogen auf Ubiquitous Computing *Roßnagel* 2007, 128 ff. und in Bezug auf Internetdienste *Roßnagel* 2014b, 82 ff.

hebung mag irrelevant erscheinen, besondere Bedeutung wird sie oft erst dadurch erlangen, dass sie nachträglich mit vielen anderen Daten zusammengeführt wird. Dann besteht aber keine Möglichkeit mehr, den Betroffenen zu benachrichtigen. Für andere Anwendungen kann der Zweck der Datenverarbeitung mehrfach wechseln und sich auch unvorhergesehen einstellen. Vielfach wird eine unerwünschte (Mit-)Erhebung durch die mobilen Geräte anderer Kooperationspartner erfolgen. Viele Anwendungen werden ineinander greifen und verteilte Ressourcen nutzen (zum Beispiel Mitnutzung des Ausgabemediums eines anderen Gegenstands). Andere Anwendungen müssen zu ihrer Funktionserfüllung benötigte Daten austauschen (zum Beispiel braucht Ereignisdienst externe Information über einen Ereigniseintritt). Eine Erhebung beim Betroffenen und erst recht seine Unterrichtung über die zu erhebenden Daten und den Zweck ihrer Verarbeitung wird daher vielfach unmöglich oder sehr schwierig sein.

Bei einer Auskunft wird statt eines einfachen Datensatzes (zum Beispiel Postadresse), dem seine Bedeutung unmittelbar abzulesen ist, dem Betroffenen nur ein komplexes Destillat aus Sensordaten, statistischen Mustern oder anderen Rohdaten präsentiert, die ihre Bedeutung erst aus der konkreten Anwendung gewinnen. Oft wird nur eine Vermutung bestehen, dass dieser Datensatz den Betroffenen betrifft.[267] Wird die Auskunft zu einem Persönlichkeitsprofil erteilt, kann schlicht der Umfang der Auskunft den Betroffenen überfordern.[268]

Oft kann eine Auskunft nicht erfolgen, um nicht kontraproduktiv zu sein. So ermöglichen zum Beispiel Sensornetze, zu denen sich benachbarte Sensoren drahtlos spontan vernetzen, ihre Arbeit untereinander abstimmen und relevante Daten austauschen, eine flexible und nahezu unsichtbare Beobachtung der Umwelt.[269] Die einzelne Datenerhebung

---

[267] S. auch *Langheinrich* 2005, 340.

[268] *Max Schrems* erhielt von Facebook eine Auskunft zu seinem Account mit über 1.200 Seiten Länge. http://rtlnext.rtl.de/cms/wie-holt-man-sich-seine-facebook-daten-881716.html.

[269] S. z.B. *Mattern* 2005, 15.

ist weitgehend irrelevant, sie kann auch nicht im Einzelfall angezeigt werden. Eine nachträgliche Auskunft über alle verarbeiteten Daten ist prinzipiell möglich, würde aber eine Speicherung aller erhobenen und verarbeiteten Daten voraussetzen, um im Ausnahmefall eines Auskunftsbegehrens die Daten des Anfragenden herausdestillieren zu können.

3.2.2.2 Einwilligung

Ist „smarte" Informationstechnik in den Alltag eingedrungen und führen Sensoren, Lokalisatoren, biometrische Verfahren oder Kameras zu einer allgegenwärtigen Datenerfassung, würde die Forderung, für alle nicht durch Vertrag gedeckten Datenerfassungen, -verarbeitungen und -nutzungen jeweils eine Einwilligung zu erteilen, angesichts der Fülle und Vielfalt der Vorgänge und der Unzahl von verantwortlichen Stellen zu einer Überforderung aller Beteiligten führen.[270] Noch weniger umsetzbar wäre es, hierfür die geltenden Formvorschriften – Schriftform oder elektronische Form – zu fordern. Selbst eine Einwilligung in der für das Internet gedachten Form des § 13 Abs. 2 TMG dürfte unter diesen Umständen meist unpraktikabel sein. Angesichts der potentiell großen Zahl von impliziten (Mini-)Interaktionen und der ebenso großen Bandbreite an Nutzerschnittstellen scheint es nicht praktikabel, bekannte Verfahren, wie beispielsweise einen Bestätigungsknopf oder gar eine Einwilligung durch elektronische Signatur, allgemein einsetzen zu wollen.[271] Für Big Data-Analysen ist es ausgeschlossen, dass die vielen – oft Millionen Betroffenen – vorher um ihre Einwilligung gebeten werden. In der Regel dürften sie dem Big Data-Anwender auch gar nicht bekannt sein.

In dieser Welt wird die Einwilligung als Instrument des Datenschutzrechts in bisher bekannter Form nur in generalisierter Anwendung überleben können. Bei vorher bekannten Dienstleistungen werden die Betroffenen in Rahmenverträgen mit allgemeinen Zweckbestimmun-

---

[270] S. hierzu auch *Langheinrich* 2005, 338f.
[271] *Langheinrich* 2005, 339.

gen ihre Einwilligung erteilen. Damit wird die Steuerungskraft der Einwilligung für die Zulässigkeit der Datenverarbeitung noch weiter sinken. Für spontane Kommunikationen wird die Einwilligung ihre Bedeutung ganz verlieren.[272]

Vielfach handelt es sich bei den „smarten" Informationstechniken um informationstechnische Infrastrukturen (Plattformen, Netzwerke, Basisdienste), die ihrem Infrastrukturcharakter entsprechend für vielfältige Anwendungen gleichmäßig zur Verfügung gestellt werden. Deren Merkmale können nicht zur Auswahl der Nutzer gestellt werden. Den Nutzern bleibt nur die Entscheidung, sie zu nutzen oder nicht (take it or leave it). Wollen sie sie nutzen, ist dies nur zu den Bedingungen und mit den Merkmalen möglich, denen alle Infrastrukturnutzer unterliegen. In diesem Fall ist die individuelle Einwilligung ein inhaltsleerer Formalismus, da bei Nutzung der Infrastruktur keine Wahlmöglichkeit besteht.[273]

Das Gleiche gilt auch für Anwendungen, die keinen Infrastrukturcharakter haben, wenn zwischen dem Nutzer (meist als Verbraucher) und dem Anbieter große Informations- und Machtasymmetrien bestehen. In diesen Fällen ist bereits die Freiwilligkeit der Einwilligung fraglich. Freiwillig erfolgt die Einwilligung nur, wenn sie ohne Zwang abgegeben wird.[274] Die Freiwilligkeit wird grundsätzlich in einem Abhängigkeitsverhältnis in Frage gestellt, wie es zwischen Arbeitgeber und Arbeitnehmer oder bei der Inanspruchnahme von Leistungen besteht, auf welche die Betroffenen existenziell angewiesen sind. Datenschutzrechtlich ist die Einwilligung nur solange als Legitimierungsgrundlage zu akzeptieren, wie sich der Betroffene nicht in einer Situation befindet, die ihn faktisch dazu zwingt, sich mit dem Zugriff auf seine personenbezogenen Daten einverstanden zu erklären. Die technische Entwicklung wird dazu führen, dass der Einzelne immer mehr von unter-

---

272 S. *Roßnagel* 2008, 146.

273 Zur Kritik am Konzept der Einwilligung s. *Kamp/Rost*, DuD 2013, 80; *Gundermann*, VuR 2011, 74 (76).

274 *Simitis*, in: Simitis 2014, § 4a BDSG, Rn. 62.

stützenden Anwendungen abhängig sein wird, die für ihre Funktionalität den Umgang mit ihren Daten fordern.[275] Die Frage der Freiwilligkeit kann damit in einem neuen Kontext relevant werden. Nicht die datenverarbeitende Stelle übt auf den Betroffenen Zwang aus, sondern die Faktizität der Technik. Unterstützt wird dieser Zwang durch die Kostenlosigkeit zahlreicher Dienstleistungen und das gesellschaftliche Ausgrenzungsrisiko bei einem Technikverzicht.

3.2.2.3 Zweckbindung

Die Zweckbindung soll dem Betroffenen ermöglichen, die Preisgabe von Daten entsprechend seiner sozialen Rolle im jeweiligen sozialen Kontext selbst zu steuern. Mit ihr ist ein Zugriff Unberechtigter auf die Daten, eine Datenverarbeitung auf Vorrat und die Bildung umfassender Profile nicht zu vereinbaren.[276]

Bereits das Ziel, die Datenverarbeitung zu steuern und auf den festgelegten Zweck zu begrenzen, widerspricht sowohl der Idee einer unbemerkten, komplexen und spontanen technischen Unterstützung als auch dem Ziel, durch das Zusammenführen und Auswerten möglichst vieler Daten aus vielfältigen Quellen neue Erkenntnisse zu gewinnen. Je vielfältiger und umfassender die zu erfassenden Alltagshandlungen und je unterschiedlicher die Datenquellen sind, umso schwieriger wird es, den Zweck einzelner Datenverarbeitungen vorab festzulegen und zu begrenzen.[277]

Daher stellt sich die Frage, ob der bereichsspezifisch, klar und präzise festgelegte Zweck, den das Bundesverfassungsgericht fordert,[278] noch das angemessene Kriterium sein kann, um die zulässige Datenverarbeitung abzugrenzen.[279] Werden Daten für vielfältige und wechselnde Zwecke erhoben, sind eine an einem begrenzten Zweck orientierte Ab-

---

[275] Z.B. ersetzen Navigationsdienste Karten und Orientierungsvermögen der Nutzer.
[276] S. *BVerfGE* 65, 1 (49); *Scholz*, in: Roßnagel 2003, 1845 ff.
[277] S. hierzu auch *Langheinrich* 2005, 337.
[278] *BVerfGE* 65, 1 (44, 46).
[279] S. kritisch aus anderen Gründen *Roßnagel/Pfitzmann/Garstka* 2001, 29 ff.

schottung von Daten, ein daran anknüpfender Zugriffsschutz und eine auf der Zweckunterscheidung aufbauende informationelle Gewaltenteilung schwierig zu verwirklichen, vielfach sogar unpassend. Sollen „smarte" Informationstechniken die Sinne des Nutzers erweitern, können sie nicht nur für einen bestimmten Zweck Daten erheben. Sie müssen wie die Sinne des Nutzers die gesamte Umwelt wahrnehmen. Erst wenn diese Daten erhoben und gespeichert sind, kann nach und nach eine zweckorientierte Auswahl und Bewertung erfolgen. Erst danach können die Ergebnisse der „Sinneseindrücke" gelöscht werden – es sei denn sie sollen der Möglichkeit dienen, sich an etwas zu erinnern. Selbst wenn ein Zweck bestimmt wird, kann dieser so umfassend sein, dass er die Erhebung und Speicherung vielfältiger und umfassender Daten erfordert.[280]

Ähnlich verhält es sich mit dem Verbot einer Datenhaltung auf Vorrat und einer Profilbildung. Wenn viele Anwendungen ineinander greifen, Daten aus anderen Anwendungen übernehmen, für den Nutzer Erinnerungsfunktionen für künftige Zwecke erfüllen sollen, die noch nicht bestimmt werden können, sind Datenspeicherungen auf Vorrat nicht zu vermeiden.[281] Wenn die „smarten" Informationstechniken im Alltag kontextsensitiv und selbstlernend sein sollen, werden sie aus den vielfältigen Datenspuren, die der Nutzer bei seinen Alltagshandlungen hinterlässt, und seinen Präferenzen, die seinen Handlungen implizit entnommen werden können, vielfältige Profile erzeugen. Für Profile, die die informationelle Selbstbestimmung gefährden, und Profile, die eine optimale Befriedigung der Nutzerinteressen gewährleisten, bedarf es weiterer Unterscheidungskriterien, die nicht allein an der Tatsache einer Profilbildung anknüpfen können.[282]

Schließlich könnten sich faktisch mit der vielfältigen – oft unbewussten – Verfügbarkeit über personenbezogene Daten neue Offenbarungspflichten ergeben, die zu einer nachträglichen Zweckänderung

---

280 S. *Roßnagel* 2008, 147.
281 S. weitere Beispiele in *Roßnagel* 2008, 150.
282 S. hierzu bereits für Location Based Services *Jandt/Laue*, K&R 2006, 316 ff.

führen. Wenn die Dinge vieles um sich herum registrieren und speichern, könnte man durch Zusammenführung der gespeicherten Daten die Vergangenheit rekonstruieren und damit in vielen Fällen der Wahrheitsfindung dienen. Soll in der Familie, im Wohnumfeld, am Arbeitsplatz, im Rahmen der öffentlichen Sicherheit oder der gerichtlichen Beweisaufnahme geklärt werden, wie sich ein Ereignis zugetragen hat, könnte sich jeder verpflichtet fühlen oder verpflichtet werden, die Daten seiner Gegenstände zur Verfügung zu stellen.[283]

3.2.2.4 Erforderlichkeit und Datensparsamkeit

Da das Prinzip der Erforderlichkeit, das inhaltlich, modal und zeitlich die Datenverarbeitung begrenzen soll, am Zweck der Datenverarbeitung ausgerichtet ist, erleidet es die gleiche Schwächung wie das Prinzip der Zweckbindung. Soll die Datenverarbeitung im Hintergrund ablaufen, auf Daten zugreifen, die durch andere Anwendungen bereits generiert wurden, und gerade dadurch einen besonderen Mehrwert erzeugen, wird es schwierig sein, für jede einzelne Anwendung eine Begrenzung der zu erhebenden Daten oder deren frühzeitige Löschung durchzusetzen. Auch die Einbeziehung von Daten aus unterschiedlichsten Quellen in einer dynamischen, also laufend aktualisierenden Weise beschränkt zudem die Begrenzungsfunktion des Prinzips der Erforderlichkeit. Sensorbestückte Gegenstände und Umgebungen sind fast immer aktiv und erheben eine Unmenge Daten, um den Nutzern nach ihrem – sich ständig ändernden – Bedarf jederzeit ihre Dienste anbieten zu können.[284]

Das „Gedächtnis" der Gegenstände ermöglicht, eine Art „Fahrtenschreiber" der Dinge zu entwickeln und ihre „Lebensspur" zu rekonstruieren, immer zu wissen, wo sich ein Ding aufhält und verlorene Dinge immer wieder zu finden. Werden mehrere „Lebensspuren" mit einander abgeglichen, kann der gemeinsame Kontext verschiedener Dinge ermittelt werden – und damit zugleich auch der soziale Kontext

[283] S. *Roßnagel* 2008, 146.
[284] S. *Mattern* 2005, 18.

ihrer Besitzer. Nutzen die Betroffenen diese Gedächtnisfunktion der Gegenstände, um dadurch ihr eigenes löchriges Gedächtnis zu erweitern, lässt dies das Erforderlichkeitsprinzip gänzlich leer laufen. Für diese Funktion sind alle Daten für sehr lange Zeit erforderlich, weil niemand wissen kann, an was man sich irgendwann einmal erinnern möchte.[285]

Aus vergleichbaren Zwängen stößt auch der Grundsatz, möglichst keine oder wenige personenbezogene Daten zu erheben, zu speichern und zu verarbeiten,[286] an Grenzen. Oft kann erst eine Vielzahl langfristig gespeicherter Daten die gewünschte Unterstützungsleistung bieten. Auch die Verarbeitung anonymer und pseudonymer Daten kann ungeeignet sein, weil die Daten oftmals unmittelbar erhoben werden: Eine Kamera, ein Mikrofon oder ein Sensor nehmen anders als ein Webformular den Benutzer direkt wahr und können vielfach nicht ohne Offenlegung der Identität des Benutzers verwendet werden. Indirekte Sensoren, wie zum Beispiel druckempfindliche Bodenplatten, können auch ohne direkte Wahrnehmung durch Data-Mining-Techniken Menschen an ihrem Gang identifizieren. Die enge Verknüpfung der Sensorinformation mit Ereignissen der realen Welt erlaubt selbst bei konsequenter Verwendung von Pseudonymen in vielen Fällen eine einfache Personenidentifikation.[287]

3.2.3 Bereichsspezifische Regelungen

Für die spezifischen Risiken hält das geltende Datenschutzrecht nur wenige bereichsspezifische Vorschriften bereit, die für einzelne Spezialanwendungen geeignete Regelungen enthalten. Deren Reichweite und Grenzen werden im folgenden Kapitel näher beschrieben. Hier soll eine Übersicht gegeben und auf das Grundproblem aufmerksam gemacht werden.

---

285 S. *Roßnagel* 2008, 149.

286 S. § 3a BDSG; s. zu diesem Grundsatz ausführlich *Roßnagel* 2011, 41.

287 S. *Langheinrich* 2005, 339f.: So können z.B. bei einem Indoor-Lokalisierungssystem die pseudonymen Benutzer anhand ihres bevorzugten Aufenthaltsortes identifiziert werden.

Zum Umgang mit personenbezogene Daten im gesamten Themenbereich Smart Car gibt es nur zwei spezifische Regelungen, nämlich zum Zugriff auf die OBD-Schnittstelle und zur Nutzung des eCall.[288] Für alle anderen regelungsbedürftigen Themen zum Datenschutz in Smart Cars gibt es keine risikospezifischen Regelungen.

Im Themenfeld Smart Home gibt es spezifische Datenschutzregelungen zum Smart Metering für die Erfassung von präzisen Daten über den Stromverbrauch.[289] Alle anderen „smarten" Informationstechniken im Smart Home, etwa für die Versorgung mit anderen Energieträgern, für die Steuerung der Haustechnik, für die Gewährleistung von Sicherheit zum Beispiel gegen Einbrüche oder Brände, für die Versorgung mit Information und Unterhaltung und weitere Anwendungsbereiche fehlt es an risikospezifischen Regelungen.

Im Themenfeld Smart Health gibt es für den Umgang mit Gesundheitsdaten in der professionalisierten Gesundheitsversorgung differenzierte Regelungen zum Patienten- und zum Sozialgeheimnis, zu deren strafrechtlichem Schutz und zur beschränkten Zulässigkeit der Datenerhebung, -verarbeitung und -nutzung. Auch zu Sondersituationen in der Gesundheitstelematik und für den Einsatz der Gesundheitskarte bestehen risikobezogene Regelungen.[290] Dagegen fehlen risikobezogene Regelungen für den Umgang mit den oft gleichen Gesundheitsdaten im nichtprofessionellen Bereich durch Wearable Computing zu Zwecken der Fitnessmessung, der Leistungskontrolle im Sport, der Gesundheitsvorsorge und der Selbstdiagnose.

Für Big Data-Auswertungen gibt es Regelungen für Scoring und die Übermittlung von personenbezogenen Daten an Scoring-Ersteller sowie Regelungen für Marktforschung und für automatisierte Entscheidungen.[291] Big Data für alle anderen Zwecke, wie etwa die Erstellung von Profilen für die Personalisierung von Diensten, personalisierte

[288] S. hierzu Kap. 2.4.1.
[289] S. hierzu Kap. 2.4.2.
[290] S. hierzu Kap. 2.4.3.
[291] S. hierzu Kap. 2.4.4.

Werbung, Erkennen von Situations- und Verhaltensmustern Einzelner und Gruppen oder Erstellung von Statistiken wird von keiner Regelung speziell erfasst.

Zusammenfassend kann festgehalten werden, dass es zwar für wenige Einzelanwendungen oder Probleme für die neuen Herausforderungen durch die technische Entwicklung risikospezifische Regelungen gibt, dass aber für die meisten Anwendungsfelder und fasst alle Anwendungsprobleme auf die allgemeinen und abstrakten Datenschutzregelungen zurückgegriffen werden muss.

3.3 Feststellung konkreter Regelungsdefizite

Ob die speziellen Regeln und vor allem die allgemeinen und abstrakten Datenschutzregelungen ausreichende Vorgaben enthalten, um die Datenschutzkonflikte und Probleme mit diesen neuen technischen Herausforderungen lösen oder bewältigen zu können, wird im Folgenden im Detail untersucht.

3.3.1 Smart Car

Für den Datenschutz in Smart Cars gibt es kaum risikobezogene Regelungen. Nur für eCall und für die On-Board-Diagnose des Schadstoffausstoßes liegen spezifische Regelungen vor.[292] Für alle anderen Datenschutzfragen ist der Rückgriff auf die allgemeinen abstrakten Regelungen im Bundesdatenschutzgesetz und im Telemediengesetz erforderlich. Dies führt im Ergebnis in vielen Fällen zu defizitären oder zumindest zu unsicheren Ergebnissen. Da der Arbeitskreis VII des 52. Deutschen Verkehrsgerichtstags 2014 diese allgemeinen Regelungen für unzureichend hielt, hat er spezifische Regelungen zum Schutz der informationellen Selbstbestimmung empfohlen.[293]

Die allgemeinen Regelungen zur Unterrichtung bewirken nur eine unzureichende Transparenz bei Halter und Fahrer über die jeweils aktu-

[292] S. hierzu Kap. 2.4.1.

[293] S. Empfehlung Nr. 1 des Arbeitskreises VII des 52. Deutschen Verkehrsgerichtstags, in: 52. Deutscher Verkehrsgerichtstag, XV.

elle Datenerhebung und -verarbeitung. Meist werden die allgemeinen Unterrichtungspflichten durch den Hersteller durch Verweis auf allgemeine Erklärungen und Erläuterungen in Datenschutzerklärungen und Bedienungshinweisen in Handbüchern und Internetveröffentlichungen erfüllt. Diese überfordern den Halter oder Fahrer im Regelfall durch ihre Überfülle an Informationen. Diese Unterrichtung durch den Hersteller betrifft jedoch nur seine Dienste. Für alle anderen Dienste für Smart Cars erfolgen ebenso allenfalls nur allgemeine Unterrichtungen.

Eine ausreichende Kenntnis bei Halter oder Fahrer über die erfassten Daten, über den spezifischen Zweck der Datenverarbeitung, über die verschiedenen Phasen des Umgangs mit den Daten und über die Empfänger wird dadurch nicht erzeugt. Es bleibt vielmehr bei einer sehr hohen Informationsasymmetrie, da zwar Halter oder Fahrer für die Kontrolleure sehr transparent, dagegen die Kontrolleure, die Kontrollmöglichkeiten, die erfassten Daten und die Verwendungszwecke für Halter oder Fahrer völlig intransparent sind.

Die gebotene situationsgerechte Information über die Datenschutzeinstellungen und die aktuellen Datenerhebungen und –übermittlungen[294] findet im Regelfall nicht statt. Dadurch wird auch keine aktuelle Aufmerksamkeit, zum Beispiel für einen Datenzugriff oder eine Zweckänderung, erzeugt, die dann zu einer Aktion informationeller Selbstbestimmung führen könnte.

Einwilligungserklärungen oder Vertragsbedingungen fordern die Zustimmung zur Verarbeitung vieler personenbezogener Daten, ohne dass Halter oder Fahrer tatsächlich die Möglichkeit haben, darüber frei zu entscheiden. Die Nutzungsvorteile (teil-)automatisierten Fahrens können sie nur in Anspruch nehmen, wenn sie mit der Verarbeitung vieler Umgebungsdaten einverstanden sind. Die Kostenvorteile, die

---

294 S. Empfehlung Nr. 2 des Arbeitskreises VII des 52. Deutschen Verkehrsgerichtstags, in: 52. Deutscher Verkehrsgerichtstag, XV; zur Umsetzung s. z.B. *Bönninger*, DuD 2015, 388 ff.

ein Prämienrabatt kontrolliertem Fahren verspricht, können nur genutzt werden, wenn die dafür wesentlichen Fahrdaten übermittelt werden.[295] Die Servicevorteile durch Fernkontrolle und Fernwartung sind nur möglich, wenn dem Hersteller oder der Vertragswerkstatt der Fernzugriff auf die Betriebsdaten eingeräumt wird. Die Zeit- und Bequemlichkeitsvorteile durch die Unterstützung etwa durch Verkehrsdienste sind nur zu haben, wenn diese jeweils die Lokalisierungsdaten und Bewegungsmuster erfahren.

Das Erforderlichkeitsprinzip wird meist dadurch übergangen, dass die Dienste als „Bezahlung" für ihre Leistung mehr personenbezogene Daten erheben als erforderlich. Ein Kopplungsverbot, das verhindern würde, dass viele Leistungen von der Einwilligung in Datenverwendungen, die nicht für sie erforderlich sind, abhängig gemacht werden, fehlt.

Haltern und Fahrern fehlen vielfach Wahlmöglichkeiten bei Auswahl und Konfiguration vernetzter Dienste. Es fehlt eine Regelung, die sicherstellt, dass den Betroffenen keine Dienste aufgedrängt werden dürfen. Es fehlt an entsprechenden Anforderungen an Allgemeine Geschäftsbedingungen und Einwilligungsvordrucke.

Hinsichtlich der Gestaltung der Informationstechniksysteme fehlt es an Anforderungen für ein „Privacy by Design"[296] und ein „Privacy by Default"[297] sowie an Vorgaben zur Vermeidung personenbezogener Daten.[298] Vor allem fehlen Vorgaben zur Architektur der Datenverarbeitung, etwa dazu, ob bestimmte Daten im Auto oder in Hintergrundsystemen flüchtig oder persistent zu speichern sind und wie lange sie als erforderlich gelten oder zu löschen sind.

---

295 S. z.B. *Schwichtenberg*, DuD 2015, 378 ff.; *Weichert* 2014, 307f.

296 Datenschutz, der schon beim Design von Informationstechnik berücksichtigt wird, s. hierzu auch Kap. 5.2.5.

297 Datenschutz, der in den Voreinstellungen eines ausgelieferten Programms berücksichtigt wird, s. hierzu auch Kap. 5.2.5.

298 In Empfehlung Nr. 3 des Arbeitskreises VII des 52. Deutschen Verkehrsgerichtstags, in: 52. Deutscher Verkehrsgerichtstag, XV, ist die Forderung enthalten: „Das Prinzip der Datensparsamkeit ist sicherzustellen."

Probleme entstehen auch hinsichtlich der Verantwortlichkeit für die Einhaltung der Datenschutzvorschriften. Die Verantwortung für die Datenverarbeitung ist oft geteilt – wie zum Beispiel beim Bordsystem, Navigationssystem oder einer DashCam – oder wird kollektiv wahrgenommen. So bestimmt der Hersteller, welche Funktionen im Auto genutzt werden können, der Plattformanbieter, auf welche Dienste zugegriffen werden kann, der Diensteanbieter, welche Funktionen ein Dienst bietet und welche Daten er dafür benötigt, der Halter (Arbeitgeber, Autovermieter, Carsharing-Anbieter) sucht die genutzten Dienste aus und legt ihre Grundeinstellungen fest und der Fahrer legt möglicherweise fest, welche Dienste für die aktuelle Fahrt ausgestellt oder genutzt werden. Fahrer und Halter können vielfach ihre Rolle als Betroffene und verantwortliche Stelle wechseln oder gleichzeitig ausfüllen, wie das Beispiel DashCam deutlich macht. Die verantwortliche Stelle kann Aufgaben der Datenverarbeitung an Auftragnehmer auslagern, denen zwar Daten der Betroffenen übertragen werden, die diese aber nur unter Aufsicht und Verantwortung der verantwortlichen Stelle verarbeiten dürfen. Schließlich kann die verantwortliche Stelle die Datenverarbeitung auch an technische Systeme delegieren, die sie selbst oder ein Auftragnehmer nutzt. Für den jeweils Betroffenen kann die Feststellung der Verantwortung ohne klare Verantwortungszuteilungen sehr schwierig sein und ihn in der Wahrnehmung seiner Rechte behindern.

Solange die Generalklausel der Vertragsdatenverarbeitung nach § 28 Abs. 1 Satz 1 Nr. 1 BDSG zur Anwendung kommt, kann noch aus dem Vertragszweck einigermaßen präzis abgeleitet werden, welchem Zweck die Datenverarbeitung dienen darf und für welche Daten und welchen Zeitraum ihre Speicherung als erforderlich gilt. Dies ist bei Anwendung der Generalklausel der Datenverarbeitung für berechtigte Interessen nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG viel willkürlicher, weil der Datenverarbeitungsinteressent bestimmen kann, für welchen Zweck er die Daten verarbeiten möchte. Die notwendige Interessenabwägung wird immer wieder zu umstrittenen Ergebnissen führen.

Dies gilt auch für die Anwendung der Generalklausel auf Profiling. Grundsätzlich ist Profiling eine Zweckänderung, die nach der Interessenabwägung gemäß § 28 Abs. 1 Satz 1 Nr. 2 BDSG unzulässig ist. Nach dem Willen des Betroffenen kann sie aber nicht immer nur als verboten gelten. Vielmehr ist zwischen vom Betroffenen gewünschten Profilen (zum Beispiel für die Adaption der Bordsysteme an seine Bedürfnisse und Gewohnheiten) und unerwünschten Profilen, von denen der Betroffene nichts weiß, die ohne seine Einwilligung erfolgen oder einen anderen als den vereinbarten Zweck der Datenverarbeitung verfolgen, zu unterscheiden.[299] Geeignete Regelungen, die zulässige von unzulässigen Profilen unterscheiden, fehlen aber.

Ungeklärt ist auch, welche Interessenten auf die im Smart Car erzeugten Daten zugreifen können sollen oder wem sie übermittelt werden dürfen. Allein die Anwendung der Generalklausel für die Datenübermittlung nach § 28 Abs. 2 BDSG wird wegen der notwendigen Interessenabwägung zu großer Rechtsunsicherheit führen. Völlig ungeklärt ist, wie die entstehenden Smart Data verteilt und verwendet werden sollen und wer an der Wertschöpfung durch diese wie zu beteiligen ist.

Diese Regelungsdefizite führen im Ergebnis auf Seiten der Betroffenen zu einem unzureichenden Schutz ihrer Grundrechte und auf Seiten der Hersteller von Smart Cars und der Anbieter von geeigneten Diensten zu einer hohen Rechts- und damit auch Innovationsunsicherheit.

3.3.2 Smart Home

Solange „lediglich Daten mit punktuellem Bezug zu einem bestimmten Lebensbereich des Betroffenen“[300] verarbeitet werden, ist davon auszugehen, dass der Schutz des geltenden Datenschutzrechts grundsätzlich ausreichend ist. Dies ist jedoch dann nicht mehr der Fall, wenn Qualität und Quantität der Datenverarbeitung im Smart Home ansteigen, insbesondere wenn die gewonnenen Daten die Erstellung umfas-

[299] S. z.B. *Roßnagel* 2007, 96 ff.
[300] *BVerfGE* 120, 274 (313 f.).

sender Profile über die Lebensgewohnheiten der Bewohner oder sogar Dritter zulassen. Gerade in diese Richtung bewegt sich jedoch der aktuelle Trend zur Vernetzung von immer mehr Haushaltsgeräten und Hausteilen miteinander und mit dem Internet. In welche Richtung sich Markt und Technik aller Voraussicht nach bewegen werden, lassen Produkte wie Amazon Echo und erste, noch recht simple Haushaltsroboter bereits erahnen. Während aktuell noch die Automatisierung etwa der Heizungssteuerung oder der Lüftung und damit Aspekte des Energiemanagements im Vordergrund stehen, wird sich das Smart Home immer mehr zu einem umfassenden Assistenzsystem entwickeln, das letztlich die Funktionen von Concierge, Haushälter, Butler, Personal Assistant, Putzkraft und mehr in sich vereint. Dennoch ist zu betonen, dass auch die Auswertung ausschließlich von Energiedaten bereits tiefe Einblicke in die private Lebensgestaltung ermöglicht.

Deutlichstes Regelungsdefizit ist das Fehlen von bereichsspezifischen Vorschriften zur Datenverarbeitung im Smart Home. Lediglich der Bereich des Smart Metering ist geregelt.[301] Die entsprechenden Regelungen greifen indes nur solange, wie die anfallenden Daten den geregelten Bereich nicht verlassen. Die durch das Smart Home entstandenen und durch den technischen Fortschritt im Entstehen befindlichen Risiken müssen durch die allgemeinen Vorschriften des geltenden Datenschutzrechts aufgefangen werden. Dessen Grundprinzipien geraten im Kontext des Smart Home jedoch unter erheblichen Druck.

Die Vernetzung von immer mehr Geräten in der Wohnung mit dem Internet und untereinander verstärkt den ohnehin moderne Informationstechnik kennzeichnenden Hang zur Intransparenz. Transparenz ist jedoch notwendig für eine informierte Einwilligung sowie für die Wahrnehmung von Betroffenenrechten. Die Herstellung von Transparenz scheitert nicht nur mit Blick auf die Komplexität der eingesetzten Technik in der Praxis immer häufiger, sie ist auch mit dem Ziel der unbemerkten Assistenz der Nutzer durch die Technik nicht zu verein-

[301] S. Kap. 2.5.1.2.

baren. Eine Kennzeichnungspflicht, die Dritte vor Betreten des durch die Sensoren des Smart Home erfassten Bereichs informiert, existiert nicht. Ihr wären in der Praxis aber auch deutliche Grenzen gesetzt, da genaue Angaben zur Datenverarbeitung im Geflecht der Systeme des Smart Home schwierig sind.

Im Smart Home werden bei den Anbietern der einzelnen Komponenten des Smart Home immense Datenmengen anfallen. Dies macht es für die Betroffenen unmöglich, zu überblicken, „wer was wann und bei welcher Gelegenheit über sie weiß".[302] Hier stößt auch das Auskunftsrecht nach § 34 Abs. 1 Satz 1 Nr. 1 BDSG an seine Grenzen, denn ihm nachzukommen, wird in der Praxis möglicherweise die Grenze des faktisch Zumutbaren überschreiten.

Die Assistenz der Nutzer eines Smart Home-Systems kollidiert ferner mit Datensparsamkeit, Erforderlichkeit und Zweckbindung. Zum einen erlaubt eine möglichst große Datenbasis gekoppelt mit einer hohen Qualität der Daten genauere technische Vorhersagen und Verhaltensantizipationen. Zum anderen wird es mit dem Anspruch an umfassende Assistenz durch Technik immer schwerer, vorab konkrete Zwecke für einzelne Datenverarbeitungsvorgänge zu bestimmen und die Nutzung der Daten auf diese Zwecke zu beschränken. Vielmehr wird es technikbedingt zu spontanen Zweckänderungen kommen und eine Vielzahl von Zwecken wird mitunter auch parallel verfolgt. Das Ziel der genannten Prinzipien, Datenverarbeitung zu begrenzen, steht mithin in direktem Konflikt zu den Aufgaben und Zielsetzungen der Technik.

Das Zusammenwirken einer Vielzahl von Anwendungen auch unterschiedlicher Anbieter ist ein zentrales Merkmal des Smart Home, aber auch von „smarten" Geräten und Systemen im Allgemeinen. Zusammen mit der Vielzahl der potentiell betroffenen Personen, von den Bewohnern und Gästen über den Postboten bis hin zum Vermieter und Mitarbeitern von Wartungsfirmen, ergeben sich Probleme für ein

[302] *BVerfGE* 65, 1 (43).

Datenschutzrecht, das von einer eindeutigen Rollenverteilung ausgeht, in der Praxis des Smart Home aber mit vielen und unklar verteilten Rollen konfrontiert wird. Daten können neben den Anbietern auch von Auftragnehmern gespeichert und ausgewertet werden, wodurch sich das Geflecht weiter verdichtet. Tritt an einem oder durch ein System des Smart Home ein Schaden auf, kommen zusätzlich noch Versicherer ins Spiel. Wird demgegenüber auf Basis von Art. 2 lit. d) DSRL eine kollektive Verantwortlichkeit angenommen, so ergeben sich Probleme bei der Pflichtenzuweisung innerhalb dieses Kollektivs.[303]

Des Weiteren fehlt ein adäquates Modell zur Einwilligung in die Datenverarbeitung. Dieses müsste einerseits so gestaltet sein, dass es den Betrieb eines umfassenden Assistenzsystems ermöglicht. Das bedeutet vor allem einen Bruch mit der Zweckbindung, bei der jede Zweckänderung eine erneute Einwilligung erfordert. Dies ist beim Smart Home aber gerade nicht gewollt. Vielmehr soll es die Bewohner so unmerklich wie möglich unterstützen und entlasten. Andererseits muss das Modell zur Einwilligung so gestaltet sein, dass es der Tatsache gerecht wird, dass auch von Hausgästen und sonstigen Personen, die mit dem Haussystem in Kontakt treten, wie zum Beispiel den Angestellten von Lieferdiensten oder Haushaltshilfen, eine Einwilligung eingeholt werden kann. Es muss ferner die Abgabe einer informierten Einwilligung ermöglicht werden. Dabei ist insbesondere an diejenigen Personen zu denken, die nicht in die Einrichtung des Haussystems involviert sind. Hierbei können Parallelen zur Situation der Beifahrer und der Fahrer, die nicht auch Halter sind, im Smart Car gezogen werden. All dies leistet das derzeit geltende Datenschutzrecht nicht. Eine entsprechende technikneutral formulierte Regelung zur Einwilligung im elektronischen Verfahren findet sich lediglich in § 94 TKG und § 13 Abs. 2 TMG. Voraussetzung ist hier, dass die Einwilligung durch den Diensteanbieter protokolliert wird. Aber auch diese Form der Einwilligung wird dem praktischen Problem der Überforderung der Betroffenen im Smart Home, wo sie ständig vielfältigen einwilligungs-

[303] *Jandt/Roßnagel*, ZD 2011, 160 (165); *Kroschwald*, ZD 2013, 388.

bedürftigen Formen der Datenverarbeitung ausgesetzt sind, nicht gerecht.

Ferner ist nach der Freiwilligkeit der Einwilligung zu fragen. Auch diese dürfte in der Praxis des Smart Home nicht immer gegeben sein. Dies soll ein Beispiel illustrieren: Ein Arbeitnehmer, der von seinem Vorgesetzten privat zum Abendessen in dessen Smart Home eingeladen ist, wird sich vermutlich für das Betreten des Smart Home und die damit verbundenen Datenverarbeitungsvorgänge entscheiden, auch wenn er die Technik eigentlich ablehnt. Es sind im Bereich des Smart Home also vor allem soziale Zwänge, die Druck auf den Einzelnen ausüben.

§ 1 Abs. 2 Nr. 3 BDSG nimmt die Verarbeitung personenbezogener Daten für persönliche oder familiäre Tätigkeiten vom Anwendungsbereich des Bundesdatenschutzgesetzes aus. Der Umfang der Datenverarbeitung ist dabei nicht von Relevanz.[304] Dies ist dort problematisch, wo auch Gäste, Zusteller, Handwerker und andere Dritte mit dem Smart Home in Kontakt treten und ihre Daten verarbeitet werden.[305] Werden im Smart Home Tätigkeiten beispielsweise im Rahmen von freien Berufen ausgeübt, so entfällt die Privilegierung durch § 1 Abs. 2 Nr. 3 BDSG. Zudem dürften mit dem anhaltenden Trend hin zum Cloud-Computing die lokale Verarbeitung und Speicherung von personenbezogenen Daten im Smart Home in der Zukunft eher die Ausnahme sein. Dafür spricht die cloud-basierte Struktur technischer Wegbereiter des Smart Home wie Amazon Echo.

Für den Teilbereich des Smart Metering ist die Neuregelung durch das Gesetz zur Digitalisierung der Energiewende aus datenschutzrechtlicher Sicht grundsätzlich zu begrüßen. Bestimmte Mängel bezüglich der datenschutzrechtlichen Ausgestaltung sollten jedoch adressiert werden. So sieht § 60 Abs. 5 MsbG zwar vor, dass „Berechtigte vom Messstellenbetreiber jede von Absatz 3 abweichende datensparsamere

[304] *Plath*, in: ders. 2013, § 1 BDSG, Rn. 30.
[305] S. hierzu ausführlich *Skistims* 2016, 393 ff.

Konfiguration des Smart-Meter-Gateways verlangen“ können, nicht aber, dass bereits die datensparsamste Konfiguration vorgewählt ist.[306] Zu beachten ist auch, dass das Messstellenbetriebsgesetz – wie auch der wegfallende § 21g EnWG – keine eigenen Bußgeldvorschriften für Verstöße gegen datenschutzrechtliche Vorschriften enthält.[307]

Zusammenfassend ist dem geltenden Datenschutzrecht eine fehlende Adäquanz bezüglich der Risiken und Problemstellungen der Datenverarbeitung im Smart Home zu attestieren. Hier lassen sich an vielen Stellen Parallelen zur Datenverarbeitung im Smart Car ziehen. Im Vergleich zum Smart Car als „private-in-public place“[308] und bereits hochkritischem Bereich ist mit der Wohnung als letztem Rückzugsort jedoch ein noch sensiblerer Bereich betroffen. Dieser Tatsache muss das Datenschutzrecht Rechnung tragen. Insbesondere das Schutzinteresse von Mitbewohnern und Gästen muss adressiert werden.

Darüber hinaus sind auch in anderen Rechtsgebieten viele Fragen im Zusammenhang mit dem Smart Home bis dato ungeklärt, insbesondere im allgemeinen bürgerlichen Recht, im Haftungsrecht und im Versicherungsrecht. Dies betrifft etwa die Frage nach der Schadensliquidation und der Haftung bei durch ein System des Smart Home verursachten Schäden; zum Beispiel ein durch das Herunterfahren der Heizung im Winter infolge eines Softwarefehlers verursachter Wasserrohrbruch. Auch hier ergeben sich viele Parallelen zum Betrieb von vernetzten und autonomen Kraftfahrzeugen. Darüber hinaus stellen sich praktische Fragen etwa zur Wirksamkeit von Kaufverträgen, die durch autonome Geräte abgeschlossen werden.

---

306 So auch die Kritik des Verbraucherzentrale Bundesverbandes 2015, 9.

307 In Fällen der Delegation der Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten auf einen Dienstleister im Auftrag der berechtigten Stelle verweist § 49 Abs. 3 MsbG auf § 43 BDSG.

308 S. hierzu *Urry*, The Sociological Review 54, 2006, Issue Supplement s1, 17.

3.3.3 Smart Health

Das Bundesverfassungsgericht hat im Volkszählungsurteil betont, dass es kein „belangloses Datum" gäbe.[309] Aus dieser Feststellung folgte die Schlussfolgerung, dass das Datenschutzrecht für jegliche personenbezogenen Daten gleichermaßen greifen müsse. Dennoch differenziert das Bundesdatenschutzgesetz zwischen personenbezogenen und besonderen Arten personenbezogener Daten und ordnet für die zweite Kategorien ein höheres Schutzniveau an. Im Ergebnis ist die höhere Schutzbedürftigkeit insbesondere von Gesundheitsdaten in keiner Weise anzuzweifeln. Allerdings führen die Smart Health-Entwicklungen dazu, dass sich die Gesundheitsdaten aufgrund der faktischen Veränderungen quasi eigenständig aus dieser besonderen Schutzzone hinausbewegen, indem sie immer häufiger vom Betroffenen selbst erhoben werden. Dadurch wird die als am risikoreichsten bewertete Phase der Datenerhebung nicht durch das Datenschutzrecht abgesichert.

Die einschlägigen Vertraulichkeits- und Datenschutzvorschriften unterstellen, dass Gesundheitsdaten überwiegend von Schweigepflichtigen und besonders sensibilisierten Personen sowie in geschützten Umgebungen erhoben werden. Zu nennen sind insbesondere Ärzte, Arzthelfer, Krankenschwestern und Pfleger in Krankenhäusern, Seniorenheimen und Arztpraxen, von Gesundheits- und Pflegediensten, in Apotheken sowie Kranken- und Lebensversicherungen.[310] Die Weitergabe dieser Informationen wird über die Parallelgeltung von Geheimnispflichten und Datenschutzrecht zweifach abgesichert.

Der originäre Vertraulichkeitsschutz wird nach und nach verloren gehen. E- und insbesondere Mobile Health sind gerade auf die Patientenbetreuung auf Distanz ausgerichtet und nur durch eine intensive Erfassung und Übermittlung von Gesundheitsdaten möglich. Die Geräte zur Datenerfassung werden sich am Körper oder beim Patienten

---

309 *BVerfGE* 65, 1 (45).

310 S. auch *Schaffland/Wiltfang* 2015, § 3 BDSG, Rn. 107.

befinden und mit einer Kommunikationsschnittstelle versehen sein. Nicht nur die medizinische Verantwortung für korrekte Messvorgänge wird dem Patienten, sondern auch die datenschutzrechtliche Verantwortung weitgehend dem Betroffenen übertragen.

Bewahrheitet hat sich dieses Risiko bereits bei Wearables, Gesundheits- und Fitness-Apps. In diesem Bereich werden die Vitaldaten- und Gesundheitsdaten ebenfalls von den Betroffenen bei bestimmten Freizeitaktivitäten oder während des ganzen Tages, zum Beispiel bei einem Schrittzähler, selbst erhoben und gespeichert. Gerade bei den Apps ist den Nutzern häufig nicht einmal bekannt oder zumindest nicht bewusst, ob eine lokale Speicherung auf dem eigenen Endgerät erfolgt oder die Daten an den Dienstanbieter übermittelt und auf dessen Speichern abgelegt werden. Zwar mag argumentiert werden, dass es in der Situation der Datenerhebung mangels Kenntnis eines Dritten des Daten- und Vertraulichkeitsschutzes nicht bedürfe, allerdings greift dies aus zwei Gründen zu kurz. Zum einen wird erstmals allein dem Patienten die Verantwortlichkeit für die auf ihn bezogenen Gesundheitsdaten aufgebürdet, obwohl er diese Informationen nicht im gleichen Umfang wie die im medizinischen Bereich tätigen Personen verstehen, deuten und bewerten kann. Zum anderen tritt die Technik als weiteres risikobegründendes Element hinzu. Der Patient muss nicht nur in der Lage sein, die eingesetzte Technik korrekt zu bedienen, sondern er müsste theoretisch auch selbst die datenschutzrechtlichen Risiken einschätzen und entsprechende technische und organisatorische Sicherheitsmaßnahmen ergreifen. Dies setzt zur Gewährleistung der Vertraulichkeit zum Beispiel voraus, dass er die Speicherorte der Daten kennt – lokal oder dezentral sowie Haupt- und Nebenspeicher zum Beispiel zum Caching –, alle Übermittlungs- und Zugriffsprozesse kennt und steuern kann sowie die Anwendung gegen gezielte Angriffe von außen abgesichert hat.

Der Weg bis zur Einführung der elektronischen Gesundheitskarte war auch deshalb so lang, weil intensiv um ein angemessenes Datenschutzkonzept gerungen wurde. Dieses findet sich nun in den diffe-

renzierten Vorgaben des § 291a SGB V.[311] Bei dem Einsatz von Informationstechniken im Gesundheitsbereich werden jedoch bei beiden beschriebenen Entwicklungsbereichen Gesundheitsdaten, wie sie sich auch auf der elektronischen Gesundheitskarte befinden, in anderen technischen und potentiell unsicheren Umgebungen abgelegt. Insbesondere für die Wearables, Fitness- und Gesundheits-Apps auf dem Smartphone existiert kein spezifisches Datenschutzkonzept, obwohl es sich bei beiden Anwendungsbereichen – elektronische Gesundheitskarte und Wearables, Fitness- und Gesundheits-Apps – qualitativ um die gleichen Daten handelt. Insofern ist eine deutliche Diskrepanz zur datenschutzrechtlichen Regulierung der elektronischen Gesundheitskarte festzustellen. Daraus lässt sich ein datenschutzrechtliches Regelungsdefizit für den Umgang mit Gesundheitsdaten feststellen, die aus Anwendungen jenseits der elektronischen Gesundheitskarten resultieren.

Bereits in der Vergangenheit trat in unterschiedlichen Zusammenhängen das Problem der Auftragsdatenverarbeitung von Gesundheitsdaten auf.[312] Zum Beispiel erfolgt bei Arztpraxen und Krankenhäusern die Rechnungserstellung teilweise durch externe Dienstleister,[313] immer mehr Krankenhäuser stellen auf elektronische Patientenakten um und lassen Papierakten, für die regelmäßig sehr lange Aufbewahrungsfristen bestehen, von externen Dienstleistern durch Scannen digitalisieren[314] oder nehmen Cloud Computing-Dienste in Anspruch.[315] Umso mehr hochkomplizierte Daten verarbeitende Technik im Gesundheitsbereich eingesetzt wird, umso unumgänglicher wird zudem die IT-Administration. Diese kann nicht mehr von den Ärzten selbst umgesetzt werden, sondern erfordert entsprechende Fachkräfte, die meist als externe Dienstleister agieren. Alle diese Tätigkeiten bedingen

311 S. hierzu Kap. 2.4.1.3.1.
312 *Seiler,* DSRITB 2015, 69.
313 *BSGE* 102, 134.
314 Die gleiche Problematik ergibt sich für Anwaltskanzleien, s. *Jandt/Nebel,* NJW 2013, 1570.
315 *Kroschwald/Wicker* 2012, 733; *Becker* 2013, 343.

oder führen zwangsläufig zu einem umfassenden Zugriff auf Gesundheitsdaten. Keiner dieser Dienstleister unterliegt einer gesetzlichen oder berufsständischen Schweigepflicht und schon gar nicht den strafrechtlichen Konsequenzen aus § 203 StGB. Diese Beispiele zeigen, dass durch die Integration von Informationstechniken das Schutzkonzept für Gesundheitsdaten aufgrund dieser faktischen Notwendigkeiten immer lückenhafter wird. Insofern sind Regelungsansätze zu finden, durch die auch zukünftig ein umfassend hohes Schutzniveau für Gesundheitsdaten erreicht wird, um die Vorteile von Smart Health realisieren zu können.

3.3.4 Big Data-Analysen

Nicht nur die „smarten" Informationstechniken im Alltag bewirken Regelungsdefizite des Datenschutzrechts, sondern auch die Auswertungsverfahren, die Big Data-Techniken anbieten. Dies gilt sowohl für die Anwendungen, die personenbezogene Daten verarbeiten, als auch für Anwendungen, die sich auf statistische Muster beschränken.

3.3.4.1 Big Data-Analysen mit Personenbezug

Soweit mit Big Data personenbezogene Daten verarbeitet werden, entweder weil personenbezogene Profile erstellt oder weil anonyme statistische Typenprofile auf individuelle Personen angewendet werden, sind diese Anwendungen zumeist als datenschutzwidrig zu bewerten. Im Hinblick auf Big Data ergibt sich also zunächst in weiten Teilen kein Regelungsdefizit, sondern ein Durchsetzungsdefizit. Zum Problem wird aber auch der politische Druck gegen die Aufrechterhaltung zentraler Bestandteile des datenschutzrechtlichen Schutzkonzepts.

Zunächst steht Big Data in teilweise scharfem Kontrast zu den geltenden Datenschutzprinzipien. Der Grundsatz der Zweckbindung bedeutet, dass personenbezogene Daten nur zu bestimmten vorab festgelegten Zwecken erhoben und verwendet werden dürfen. Das Konzept von Big Data ist es hingegen, Daten für unbestimmte Zwecke auf Vor-

rat zu halten und immer wieder frei kombinieren zu können. Der Grundsatz der Erforderlichkeit des Umgangs mit personenbezogenen Daten für bestimmte Zwecke läuft ohne die Bestimmung von Zwecken aber leer. Wenn Daten für beliebige Zwecke ausgewertet werden sollen, sind sie immer erforderlich. Die gesetzlichen Erlaubnistatbestände und die datenschutzrechtliche Einwilligung der Betroffenen sollen die Datenverarbeitung auf bestimmte Zwecke begrenzen. Sie erlauben daher nicht die freie Verwendung personenbezogener Daten für Big Data-Analysen. Das Zweckbindungsprinzip steht damit in scharfem Kontrast zu allen Datenverarbeitungskonzepten, die einmal erhobene Daten für neue Zwecke – meist ohne Wissen des Betroffenen – weiterverarbeiten wollen, wie etwa Suchdienste, Social Media und Werberinge. In besonderer Weise gilt dies für Big Data-Analysen. Zentrales Merkmal von Big Data ist es, die Datenverarbeitung gerade nicht an bestimmte Zwecke zu binden, sondern Daten auf Vorrat zu sammeln und anhand der Analyseergebnisse immer neue Zwecke zu erschließen.[316] Im krassesten Gegensatz steht Big Data schon wörtlich zum Grundsatz der Datenvermeidung und Datensparsamkeit.

Die Transparenz der Datenverarbeitung für die Betroffenen, die sich in den Informationspflichten und Auskunftsansprüchen konkretisiert, kann bei Big Data ebenfalls nur schwer umgesetzt werden, da die Datenmengen zu groß und unstrukturiert sind und selbst die Anwender der Analysetools häufig nicht überblicken können, welche Daten jeweils konkret verwendet werden.

Big Data eröffnet wie keine andere Technik zuvor die Möglichkeit, persönliche Merkmale zu prognostizieren, die gar nicht offenbart wurden, bis hin zu politischen Einstellungen und aktuellen Gemütszuständen. Dies steht in Konflikt mit dem Verbot der Bildung von Persönlichkeitsprofilen. Überdies wird die Möglichkeit untergraben, über den eigenen Datenstrom durch bewusste Auswahl von publizierten Daten selbst zu bestimmen. Big Data umgeht die individuelle Daten-

316 *Weichert*, ZD 2013, 251 (255 f.); *Roßnagel*, ZD 2013, 562 (564).

askese, indem aus den Daten ähnlicher Personen, auf durchschnittliche oder individuelle Verhaltensweisen geschlossen wird. Selbst wenn ein Betroffener keine Daten zur Verfügung stellt, können über Durchschnittswerte von anderen Personen, die diese Daten preisgeben, die fehlenden Merkmale des Betroffenen prognostiziert werden. Überdies wird das Recht der Betroffenen auf Korrektur falscher Angaben konterkariert, denn die in den Big Data-Profilen vorherrschenden Wahrscheinlichkeitswerte können nicht als falsch eingeordnet werden, solange sie anhand korrekter Daten errechnet wurden.

Big Data erleichtert erheblich die Prognose von unbekannten Persönlichkeitsmerkmalen durch den statistischen Vergleich mit ansonsten ähnlichen Personen, so dass Persönlichkeitsprofile umfassender und intrusiver werden können. Die freiwillig offenbarten Daten des einen werden durch die Möglichkeit, mit statistischen Inferenzen unbekannte Merkmale vergleichend zu prognostizieren, zum Datenschutzrisiko für andere. Diese Prognosen werden aber, soweit sie nicht auf Einwilligungen der Betroffenen beruhen, häufig einen eindeutigen Verstoß gegen bestehendes Datenschutzrecht darstellen.

Außerhalb von § 28b BDSG, also außerhalb des Vertrags-Scorings, bestehen keine qualitativen Anforderungen an Scoringverfahren. Sie fehlen zum Beispiel für die Personalisierung von Internetdiensten und Geräten, für den Sicherheitsbereich, also für Predictive Policing und Rasterfahndungen, aber auch für Big Data-Verfahren, die für die Infrastrukturplanung eingesetzt werden sollen.

§ 6a Abs. 1 BDSG schreibt nicht konkret vor, wie die Bewertung der automatisierten Entscheidung durchgeführt werden muss. Daher besteht das Risiko, dass sie in der Realität zum bloßen Formalismus gerät, bei dem die automatisierte Verarbeitung die eigentliche Entscheidung trifft und der eingebundene Mensch diese einfach abzeichnet. Überdies besteht das Risiko, dass nur wenige Menschen die komplexen Big Data-Analysen überhaupt nachvollziehen und hinterfragen

können.[317] Hierbei kann keineswegs davon ausgegangen werden, dass überall dort, wo Big Data eingesetzt wird, Big Data-Analyseexperten vorhanden sein werden, die die Ergebnisse kritisch hinterfragen. Vielmehr sollen die Verfahren es technischen und mathematischen Laien ermöglichen, Entscheidungen auf einer mathematischen Grundlage zu treffen. Angesichts der Bedeutung, die die Prognose von Persönlichkeitsmerkmalen mit Big Data in Zukunft erreichen könnte, von der Polizeiarbeit bis zum Bewerbungsgespräch, erscheint es fraglich, ob die Norm noch ein adäquates Schutzniveau bietet oder ob sie nicht fortentwickelt werden müsste.

3.3.4.2 Big Data-Analysen ohne Personenbezug

Big Data-Analysen mit nicht personenbezogenen oder anonymisierten Daten sind vom Datenschutzrecht nicht erfasst.

Da Big Data-Verfahren die Fähigkeiten von Datenverarbeitern zur Deanonymisierung deutlich erhöhen, ist aber fraglich, inwiefern das in § 3 Abs. 6 BDSG etablierte Konzept der praktischen Anonymität noch passend ist. Durch Big Data könnte das zur Deanonymisierung erforderliche Zusatzwissen für viele Datenverarbeiter zur Verfügung stehen. Das Risiko der Deanonymisierung von umfassenden Profilen, die als anonym gelten, würde deutlich steigen. Vorsorgeregelungen für diesen Fall finden sich im Datenschutzrecht bisher kaum.

§ 30a BDSG ist generell so konzipiert, dass die Ergebnisse der Markt- und Meinungsforschung nur anonym übermittelt werden. Die Vorschrift soll so vor personenbezogenen Auswirkungen dieser Forschung schützen. Allerdings können solche anonymen Ergebnisse mitunter anhand von wenigen, leicht erkennbaren Merkmalen auf individuelle Personen übertragen werden, so dass durch sie das Risiko personenbezogenen Profilings deutlich wächst.

Durch das Risiko, des plötzlichen Umschlagens anonymer Statistik in personenbezogene Profilbildung und Verhaltensprognosen, können

[317] S. *Wolfangel*, Technology Review (dt. Ausgabe) 1/2016, 59 (60).

auch bereits anonyme Statistiken einen Konformitätsdruck auslösen. Sie führen den Menschen vor, welche Indikatoren zu bestimmten Wertungen führen, so dass diese darum bemüht sein werden, die Merkmalsindikatoren für unerwünschte Schlussfolgerungen an sich selbst zu tilgen, bevor sie überhaupt jemand mit ihnen in Verbindung bringt. Die durch Big Data gesteigerte Verfügbarkeit von Statistik für immer mehr menschliche Merkmale kann damit die Normativität der Normalität deutlich verschärfen.

Das Regelungskonzept des Datenschutzrechts, das fundamental zwischen personenbezogenen und anonymen Daten unterscheidet und nur den Umgang mit personenbezogenen Daten reguliert, ist vor diesem Hintergrund nicht mehr ausreichend für den Schutz von Persönlichkeitsrechten, Willens- und Handlungsfreiheit.

3.3.4.3 Übergreifende Defizite

Datenverarbeitung kann auf anonymer Big Data-Statistik beruhen, der Personenbezug wird aber häufig nur im menschlichen Gehirn hergestellt werden.[318] Personenbezogene Datenverarbeitung, die nur im menschlichen Gehirn abläuft, steht aus zwei Gründen bisher nicht im Fokus des Datenschutzrechts. Erstens begründet sie viel geringere Risiken für die Persönlichkeitsrechte. Ohne Einsatz von Medien, in denen sich die Datenverarbeitung verkörpert, hat der einzelne Mensch nur einen Zugriff auf sehr wenige zusätzliche Informationen, er kann seine eigenen Informationen nur sehr mühsam mit denen anderer verknüpfen und er vergisst viele der Informationen, die er sammelt, wenn er nicht aufwendige Memorisierungstechniken verwendet. Kaum ein Mensch kann wohl im Kopf Wahrscheinlichkeitsprognosen über Verhalten und Merkmale errechnen. Zweitens, und dies ist vielleicht der ausschlaggebende Grund, können Datenverarbeitungen im Kopf häufig nicht bewiesen oder überhaupt bemerkt werden. Sie können festgestellt werden, wenn zum Beispiel ein Polizeibeamter einen Bürger

[318] S. Kap. 1.2.4.

ausdrücklich nach seinem Namen fragt und eine Antwort erhält.[319] Überhaupt nicht zu bemerken und damit auch nicht anhand von Rechtsnormen zu kontrollieren, ist aber die rein menschliche Anwendung statistisch errechneter Merkmale auf Menschen in Auswahlprozessen, wie zum Beispiel einem Bewerbungsgespräch.

Big Data verändert die erste Prämisse. Statistisch errechnet werden Merkmale als Indikatoren für erwünschtes und unerwünschtes Verhalten, die auf den ersten Blick oder auf einfache Nachfragen hin erkennbar sind. So werden Menschen mit Informationen versorgt, die ihre rein organische, medienfreie Datenverarbeitung mit einem gesteigerten Risiko für die Betroffenen versieht. Die zweite Prämisse bleibt aber unverändert. Diese medienfreien Datenverarbeitungen bleiben häufig strukturell völlig im Verborgenen (des menschlichen Gehirns). Rein menschliche medienfreie Datenerhebungen, wie das mündliche Erfragen und Sichmerken oder auch das reine Beobachten und Sichmerken, sind nicht grundsätzlich von der Anwendbarkeit des Datenschutzrechts ausgeschlossen.[320] Allerdings sind sie gemäß § 1 Abs. 2 Nr. 3 BDSG bei der Datenverarbeitung durch private Stellen gerade nicht erfasst. Überdies entziehen sie sich der Kontrolle, soweit sie nicht protokolliert werden, so dass an dieser Stelle eine konzeptionelle Schutzlücke des Datenschutzrechts bezüglich der Risiken von Big Data besteht. Die Anwendbarkeit von § 30a BDSG ist zwar, insbesondere durch das Tatbestandsmerkmal „Forschung", auf solche Verfahren beschränkt, die anerkannte wissenschaftliche Methoden der empirischen Sozialforschung einsetzen.[321] Die Branchenverbände haben einen Verhaltenskodex erarbeitet, der entsprechende Standards enthält.[322] Damit können gerade nicht alle Big Data-Analysen auf § 30a BDSG gestützt werden. § 30a BDSG enthält aber weder eine Einschränkung be-

---

319 Z.B. gemäß § 13 Abs. 3 HSOG geht davon aus, dass eine Befragung die Erhebung personenbezogener Daten darstellt, ohne hierfür zu verlangen, dass die Antworten niedergeschrieben werden.

320 *Schild*, in: Roßnagel 2003, 510.

321 *Hornung/Hofmann*, WRP 2015, 776 (784).

322 *ADM/ASI/BVM/DGOF* 2008; *ICC/ESOMAR* 2007.

züglich der Stellen, die Markt- und Meinungsforschung betreiben dürfen, noch eine Einschränkung der zulässigen Fragestellungen dieser Forschung. Dies erscheint angesichts der Risiken für die individuelle und demokratische Willensbildung, die mit der Erforschung bestimmter Bereiche menschlichen Denkens und Fühlens mit Hilfe von Big Data einhergehen, nicht mehr risikoangemessen. Die Beschränkung auf wissenschaftliche Methoden bietet bezüglich dieses Risikos keinerlei Schutz. Wissenschaftliche Verfahren sind im Gegenteil sogar besser dazu geeignet, wirkungsvolle Einwirkungsstrategien zu erforschen und zu entwickeln.

4 Vorschläge zur Novellierung des Datenschutzrechts

Die im Rahmen dieser Studie behandelten „smarten" Informationstechniken im Alltag und die Datenauswertung durch Big Data führen deutlich vor Augen, dass Informationstechnik in naher Zukunft weite Bereiche des alltäglichen Lebens der Menschen durchziehen und das gesellschaftliche Leben prägen werden. Diese tiefgreifenden Veränderungen in der Informationstechnik und ihren Anwendungen fordern neue Ansätze zur Gewährleistung von informationeller Selbstbestimmung, die die bestehenden Konzepte ergänzen oder ersetzen. Wenn die Informationstechnik und ihre Anwendungen so gravierende Auswirkungen haben, liegt es nahe zu versuchen, vor allem diese Technik als Ursache oder Auslöser der Veränderungen so zu gestalten, dass die positiven Wirkungen der Informationstechnik gewahrt und die negativen vermieden werden. Daher ist die rechtsverträgliche, in diesem Fall datenschutzrechtsverträgliche, Gestaltung dieser Technik eine zutiefst politische Angelegenheit, deren Erfolg über die zukünftigen Verwirklichungsbedingungen grundrechtlicher Freiheiten, sozialen Lebens und demokratischer Willensbildung mitentscheidet.

Im Folgenden werden allgemeine Erwägungen vorgestellt, welche Konzepte, Instrumente und Regelungen die festgestellten Defizite beseitigen und mindern könnten (4.1). Danach werden die vier beispielhaften Technikanwendungen daraufhin untersucht, welche Vorschläge bei ihnen konkret in Betracht kommen, um die Defizite in dem jeweils spezifischen Anwendungsfeld anzugehen (4.2).

4.1 Regelungsvorschläge zur Stärkung des Datenschutzes

Regelungsvorschläge, die über das Anwendungsfeld einer bestimmten smarten Informationstechnik hinausgehen, können verschiedene Regelungsthemen betreffen. Sie beziehen sich auf die Erlaubnistatbestände, auf die Datenschutzprinzipien, auf die technische Gestaltung der Informationstechnik, auf ergänzende Instrumente zur Verbesserung der Information, zur Aktivierung der Datenverarbeiter und zur Stärkung der Kontrolle.

4.1.1 Anpassungen und Ergänzungen der Erlaubnistatbestände

Als ein Hauptdefizit der Erlaubnistatbestände wurde festgestellt, dass sie aufgrund ihrer Struktur kaum noch geeignet sind, die Komplexität von Datenverarbeitungsprozessen zu erfassen und zu regulieren. Eine alternative Struktur für ergänzende Erlaubnistatbestände könnte sich aus einem risikoorientierten Regelungsansatz ergeben, der nicht primär verantwortliche Stelle, Betroffener und Zweck der Datenverarbeitung festlegt. Stattdessen sollten der Einsatz einer bestimmten Technik und die damit verbundenen datenschutzrechtlichen Risiken adressiert werden, wie dies zum Beispiel bei den §§ 6a, 6b und 6c BDSG oder Art. 6 eCall-Verordnung (EU) 2015/758 der Fall ist. Vergleichbare Regelungen wären zum Beispiel für das Cloud Computing, Smart Cars, Big Data-Anwendungen, Wearables oder auch insgesamt für datengetriebene Geschäftsmodelle denkbar.[323]

Lösen die Techniken besondere datenschutzrechtliche Risiken aus, sollte die Zulässigkeit der Datenverarbeitung von entsprechend hohen technisch-organisatorischen Maßnahmen der Datensicherheit abhängig gemacht werden. Diese sollten in einem umfassenden Datenschutzkonzept dargelegt werden. Seine Umsetzung sollte nachzuweisen sein. Dies kann durch eine Fremdkontrolle mit Zertifizierung erleichtert werden.[324] Das Konzept sollte veröffentlicht und seine Umsetzung gegenüber dem Betroffenen auf Antrag erläutert werden. Die Umsetzung kann durch die Aufsichtsbehörden überprüft werden.

4.1.2 Beschränkung der Einwilligung

Zur Erfüllung der Schutzpflicht des Staates für die informationelle Selbstbestimmung sollte die Bedeutung gesetzlicher Erlaubnistatbestände durch eine Einschränkung der Einwilligung gestärkt werden. Dies kann dadurch erreicht werden, dass für besondere Kategorien

---

[323] S. auch *Roßnagel*, Schriftliche Stellungnahme zum öffentlichen Fachgespräch zur Datenschutz-Grundverordnung am 24.2.2016 im Ausschuss Digitale Agenda des Deutschen Bundestags, vom 19.2.2016, 2.

[324] S. hierzu Kap. 4.1.9.

von Daten oder auch in besonderen Verarbeitungskonstellationen, wie zum Beispiel im Beschäftigungsverhältnis, die Einwilligung grundsätzlich als Legitimationsmöglichkeit ausgeschlossen wird. Denkbar wäre auch, in bestimmten Anwendungsbereichen nur befristete Einwilligungen zuzulassen. Zudem können die Voraussetzungen einer wirksamen Einwilligung ebenfalls risikoorientiert angehoben werden. Um die Sensibilität der Betroffenen für den Wert ihrer Daten zu erhöhen, wäre es zum Beispiel sinnvoll, wenn die Anbieter datengetriebener Geschäftsmodelle ihre Vermarktungsstrategie hinsichtlich der personenbezogenen Daten vor der Einwilligung offenlegen müssten.

Soweit der Betroffene keine Wahlmöglichkeiten hinsichtlich der Verarbeitung seiner Daten hat, sondern nur die Allgemeinen Geschäftsbedingungen akzeptieren oder die Einwilligungserklärungen erteilen kann oder ansonsten auf die Leistung verzichten muss, ist der Betroffene nicht in der Lage, frei zu entscheiden. Diese Texte sollten daher einer objektiven Kontrolle zugeführt werden. Hierzu sollten sie zum Gegenstand des Wettbewerbsrechts werden. Die vorformulierten Texte sollten als wettbewerbswidrig angesehen werden, wenn sie Zwecke verfolgen, die keinen Bezug zu den versprochenen Leistungen des Datenverarbeiters haben oder die Interessen des Betroffenen in anderer Weise unzureichend berücksichtigen. Dabei könnte der Marktanteil des Anbieters und damit die Abhängigkeit des Betroffenen in der Nutzung dieses Angebots berücksichtigt werden. Mit dem Marktanteil würde damit auch die Verantwortung für faire Vertragsbedingungen steigen.

4.1.3 Gestaltungs- und Verarbeitungsregeln

Die Zulassungsregeln müssen durch Gestaltungs- und Verarbeitungsregeln ergänzt werden. Statt das Schwergewicht auf eine einmalige, lange vor der Datenverarbeitung liegende Zulassungsentscheidung durch Zwecksetzung des Gesetzgebers oder des Betroffenen zu legen, sollte Datenschutz künftig vorrangig durch Gestaltungs- und Verar-

beitungsregeln bewirkt werden, die permanent zu beachten sind.[325] So könnte zum Beispiel Transparenz statt auf einzelne Daten stärker auf Strukturinformationen bezogen sein und das Informationsinteresse des Betroffenen dann befriedigen, wenn er dies wünscht.[326] Statt durch eine einmalige Unterrichtung könnte dies durch eine ständig einsehbare Datenschutzerklärung im Internet gewährleistet werden. Eine andere Transparenzforderung könnte sein, von allen Alltagsgegenständen eine technisch auswertbare Signalisierung zu fordern, wenn sie Daten erheben. Statt einer Einwilligung könnte als Opt-in auch anzusehen sein, wenn der Betroffene freiwillig seine individuellen Fähigkeiten unterstützende und verstärkende Techniksysteme und Dienste nutzt. Zum Ausgleich müssten diese so gestaltet sein, dass sie über Datenschutzfunktionen verfügen, die er auswählen und für sich konfigurieren kann.

4.1.4 Neufassung der Zweckbindung

Die Zweckbindung ist ein zentrales Steuerungsinstrument des Datenschutzes und der Gewährleistung der informationellen Selbstbestimmung. Daher sollte sie auf keinen Fall generell aufgeweicht werden. Soweit die Zweckbindung durch einen notwendig weiten Zeck der spezifischen IT-Anwendung unter Druck gerät,[327] könnte der Gesetzgeber, soweit er diese IT-Anwendung mit diesem weiten Zweck zulassen will, eine bereichsspezifische Ausnahme von der engen Zweckbindung vorsehen und für diese Anwendung den Zweck entsprechend weit festlegen. Es besteht jedenfalls kein Grund, nur weil der Zweck für einige IT-Anwendungen schwer festzulegen ist, auf die Zweckbindung insgesamt zu verzichten oder diese für herkömmliche Datenverarbeitungen zu relativieren. Die Ausnahmen von der Zweckbindung müssen vom Gesetzgeber durch andere Schutzvorkehrungen – wie etwa erweiterte Transparenzansprüche, eine wirksame Wider-

---

325 S. *Roßnagel/Pfitzmann/Garstka* 2001, 70 ff.
326 S. *Roßnagel* 2008, 145.
327 S. Kap. 3.2.2.3.

spruchsmöglichkeit oder spezifische technische Sicherungen – ausgeglichen werden.

Vereinfacht und effektiviert würde der Datenschutz für viele Anwendungen smarter Informationstechnik, wenn als zulässiger Zweck relativ weit die Erbringung einer rein technischen Funktion anerkannt, dafür aber als Ersatz die Verwendung der Daten strikt auf diese Funktion begrenzt würde. Dies könnte erreicht werden, wenn zwischen Datenverarbeitungen mit und ohne gezielten Personenbezug unterschieden würde.[328] Eine Datenverarbeitung ohne gezielten Personenbezug betrifft die Verarbeitung personenbezogener Daten, die zur Erfüllung – vor allem technischer – Dienstleistungen technisch notwendig ist, ohne dass es dem Verarbeiter auf den Personenbezug ankommt. Dies wird bei allgegenwärtiger Datenverarbeitung sehr oft der Fall sein. Sensoren erheben alle Veränderungen, die sie nach ihrer Fähigkeit erfassen können. Diese Daten werden nach der Erhebung in der Form weiterverarbeitet, dass sie mit anderen Sensordaten kombiniert und analysiert werden. Danach dürfte sich nur ein Bruchteil als interessant herausstellen. Die anderen Daten wurden nicht erhoben, um für sie einen Personenbezug herzustellen. Ähnlich verhält es sich mit dem Auslesen von RFID-Chips. Bei einer automatischen Erhebung werden unvermeidlich alle RFID-Chips in der Reichweite des Lesegeräts erfasst. Auch hier werden in einem weiteren Verarbeitungsschritt die relevanten von den nicht relevanten Daten getrennt. In Ad-hoc-Netzen bilden sich die Kommunikationsverbindungen durch Peer-to-Peer-Kontakte zufällig Beteiligter. Um Telekommunikation zu ermöglichen, verarbeitet jeder personenbeziehbare Verkehrs-, Nutzungs- und Inhaltsdaten. Diese könnte er zwar zur Kenntnis nehmen, an ihnen hat er aber kein Interesse, weil er sie nur verarbeitet, um die Funktionen des Ad-hoc-Netzes zu ermöglichen.

Die Anforderungen für diese Art der Datenverarbeitung sollten risikoadäquat und effizienzsteigernd spezifiziert werden. Sie sollten inso-

---

328 S. näher *Roßnagel/Pfitzmann/Garstka* 2001, 68 ff., 113 ff.

fern verschärft werden, als die Daten auf das erforderliche Minimum begrenzt, während ihrer Verarbeitung gegen Zweckentfremdung geschützt und nach der Verarbeitung sofort gelöscht werden müssen. Die Daten sollten außerdem einer strengen Zweckbindung, wie nach § 31 BDSG, unterliegen und durch ein Verwertungsverbot geschützt sein. Werden diese Anforderungen nicht erfüllt, wird vor allem ein weitergehender Zweck mit diesen Daten verfolgt, gelten für sie von Anfang an alle Anforderungen für die Datenverarbeitung mit gezieltem Personenbezug. Erleichterungen sollten insoweit vorgesehen werden, als auf eine vorherige Unterrichtung der betroffenen Personen verzichtet wird und ein Anspruch auf Auskunft über einzelne Daten für die kurze Zeit ihrer Speicherung nicht besteht, um kontraproduktive Protokollverfahren zu vermeiden. Die notwendige Transparenz sollte vielmehr durch eine veröffentlichte Datenschutzerklärung über die Struktur des Datenverarbeitungsverfahrens hergestellt werden.[329]

4.1.5 Datenschutz durch Technikgestaltung

Die Durchsetzung von Zulassungs- und Verarbeitungsregeln und auch Betroffenenrechten muss im Regelfall durch Technik und nicht durch persönliches Handeln des Betroffenen erreicht werden. Diese Regeln sind auf eine technische Umsetzung angewiesen. Selbstbestimmung muss durch Infrastrukturen unterstützt werden, die ermöglichen, auf Gefährdungen automatisch zu reagieren, ohne dass dies aufdringlich oder belästigend wirkt. Ein Beispiel: Die Einhaltung von Verarbeitungsregeln zu kontrollieren, darf nicht die permanente persönliche Aufmerksamkeit erfordern, sondern muss automatisiert erfolgen. Wenn die datenverarbeitenden Alltagsgegenstände ein Signal aussenden, kann dies von einem Endgerät des Betroffenen erkannt werden und zu einer automatisierten Auswertung der zugehörigen Datenschutzerklärung führen. Entsprechend der voreingestellten Datenschutzpräferenzen kann ein Alter Ego, ein technisches System des

[329] S. z.B. *Roßnagel* 2008, 154f.

Betroffenen, dem dieser vertraut, eine Einwilligung erteilen oder ablehnen.[330] In Zweifelsfällen kann das Gerät je nach Voreinstellung den Betroffenen warnen und ihm die Erklärung in der von ihm gewählten Sprache anzeigen oder akustisch ausgeben. Die Hinweis- und Warndichte muss einstellbar sein. Aber auch andere Betroffenenrechte müssen an die modernen Technikanwendungen angepasst werden. Der Alter Ego sollte in der Lage sein, Datenverarbeitungen zu kontrollieren und Widerspruchs- und Löschungsrechte nach Voreinstellungen der Nutzer ausüben.

Die technische Unterstützung des Betroffenen setzt aber die Standardisierung und Offenlegung von Datenformaten und Schnittstellen voraus. Nur unter dieser Voraussetzung können technische Instrumente entwickelt und angeboten werden, die eine automatische Unterstützung betroffener Personen ermöglichen. Daher sollten Anbieter von Diensten und die Hersteller von Systemen verpflichtet werden, gängige oder einheitliche Schnittstellen und Funktionen ihrer Systeme anzubieten und offenzulegen, um die Entwicklung und Nutzung von Softwareagenten zur Ausübung von Betroffenenrechten zu ermöglichen. Die Konkretisierung sollte den Entwicklern, Herstellern und Anbietern im Wege der Selbstregulierung ermöglicht werden.[331]

Die Durchsetzung von Verarbeitungsregeln muss im Regelfall durch Technik und nicht durch persönliches Handeln des Betroffenen erreicht werden. Technischer Datenschutz hat gegenüber rein rechtlichem Datenschutz Effektivitätsvorteile: Was technisch verhindert wird, muss nicht mehr verboten werden. Gegen Verhaltensregeln kann verstoßen werden, gegen technische Begrenzungen nicht. Datenschutztechnik kann so Kontrollen und Strafen überflüssig machen.

---

330 Einen solchen Alter Ego zur technischen Unterstützung des Datenschutzes untersucht z.B. das DFG-Graduiertenkolleg 2050 „Privatheit und Vertrauen für mobile Nutzer" an den Universitäten Darmstadt und Kassel.

331 S. z.B. *Roßnagel/Richter/Nebel*, ZD 2013, 107.

4.1.6 Freiheitsfördernde Architekturen

Die Möglichkeiten der Überwachung und Kontrolle steigen, wenn Daten aus vielen verschiedenen Lebensbereichen zusammengeführt werden können. Dies ist leicht möglich, wenn die Organisation der Datenverarbeitung zentral oder abgestimmt erfolgt. Sie fällt schwer, wenn die Datenverarbeitung dezentral und spontan erfolgt. Entscheidend ist also, wie die Architektur smarter Informationstechnik im Alltag oder für Big Data-Analysen gestaltet und wie die Datenflüsse und Zugriffsmöglichkeiten organisiert sind.[332]

Rechtlich müsste sichergestellt werden, dass es für Ubiquitous Computing-Anwendungen keinen „Anschluss- und Benutzungszwang" gibt, der zu einer zentralen Datenhaltung führt und einen zentralen Zugriff auf alle erhobenen personenbezogenen Daten ermöglicht. Auch muss ein Kopplungsverbot sicherstellen, dass bestimmte wichtige Infrastrukturleistungen nicht davon abhängig gemacht werden dürfen, dass der Betroffene in die Erhebung von Daten, die nicht unbedingt erforderlich sind, einwilligt. Schließlich müsste die Aufgabe der datensparsamen oder datenvermeidenden Systemgestaltung nach § 3a BDSG aufgewertet und ihre Berücksichtigung bei der Gestaltung von IT-Architekturen überprüfbar werden.[333]

4.1.7 Technikgestalter als Regelungsadressaten

Regelungen, die sich nur an Datenverarbeiter richten, dürften viele Gestaltungsziele nicht erreichen. Statt Regelungsadressaten ohne Einfluss zu wählen, sollten diejenigen verpflichtet werden, die auch die entsprechenden Handlungsmöglichkeiten haben. In viel stärkerem Maß sind daher die Technikgestalter anzusprechen. Diese sollten vor allem Prüfpflichten für eine datenschutzkonforme Gestaltung ihrer Produkte, eine Pflicht zur Dokumentation dieser Prüfungen für bestimmte Systeme und Hinweispflichten für verbleibende Risiken tref-

[332] S. näher *Roßnagel* 2007, 188 ff.
[333] S. *Roßnagel* 2008, 157f.

fen.[334] Vor allem die Hersteller nicht nur die Datenverarbeiter sollten verpflichtet werden, ihre Produkte und Systeme nach dem Konzept des „Privacy by Design" zu gestalten. Auch sollten sie verpflichtet werden, ihre Produkte mit datenschutzkonformen Default-Einstellungen auszuliefern. Die Anbieter von Diensten sollten die gleichen Pflichten hinsichtlich der Organisation ihrer Dienstleistungen treffen.

4.1.8 Vorsorge für informationelle Selbstbestimmung

Wie auch in anderen Rechtsbereichen muss im Datenschutzrecht Vorsorge die Gefahrenabwehr ergänzen, zum einen durch die Reduzierung von Risiken und zum anderen durch präventive Folgenbegrenzungen potenzieller Schäden. Die Risiken für die informationelle Selbstbestimmung sind in einer Welt „smarter" Informationstechnik im Alltag und Big Data nicht mehr ausreichend zu bewältigen, wenn nur auf die Verarbeitung personenbezogener Daten abgestellt wird. Vielmehr sind im Sinn vorgreifender Folgenbegrenzung auch Situationen zu regeln, in denen noch keine personenbezogenen Daten entstanden sind, aber damit gerechnet werden muss. So bedürfen zum Beispiel die Sammlungen von Sensorinformationen, Umgebungsdaten oder von pseudonymen Präferenzen einer vorsorgenden Regelung, wenn die Möglichkeit oder gar die Absicht besteht, sie irgendwann einmal mit einem Personenbezug zu versehen.[335] Auch sind zur Risikobegrenzung Anforderungen an eine transparente, datensparsame, kontrollierbare und missbrauchsvermeidende Technikgestaltung zu formulieren. Ebenso entspricht es dem Vorsorgegedanken, die einzusetzenden Techniksysteme präventiven (freiwilligen) Prüfungen ihrer Datenschutzkonformität zu unterziehen und die Prüfungsergebnisse zu dokumentieren.[336]

---

334 S. näher *Roßnagel/Pfitzmann/Garstka* 2001, 143 ff.
335 S. *Roßnagel/Scholz*, MMR 2000, 728 ff.
336 S. hierzu ausführlich *Roßnagel* 2007, 185 ff.

4.1.9 Anreize und Belohnungen

Die datenschutzgerechte Gestaltung der künftigen Welt allgegenwärtiger Datenverarbeitung fordert die aktive Mitwirkung der Entwickler, Gestalter und Anwender. Sie werden hierfür aber nur zu gewinnen sein, wenn sie davon einen Vorteil haben. Daher sollte die Verfolgung legitimen Eigennutzes in einer Form ermöglicht werden, die zugleich auch Gemeinwohlbelangen dient. Datenschutz muss daher zu einem Werbeargument und Wettbewerbsvorteil werden. Dies ist möglich durch die freiwillige Auditierung von Anwendungen, die Zertifizierung von Produkten und die Präsentation von Datenschutzerklärungen. Werden diese von Datenschutzempfehlungen a la „Stiftung Warentest", von Datenschutzrankings oder durch die Berücksichtigung bei öffentlichen Auftragsvergaben begleitet, kann ein Wettbewerb um den besseren Datenschutz entstehen. Dann werden die Gestaltungsziele beinahe von selbst erreicht.[337] Dies kann unterstützt werden, wenn öffentliche Stellen verpflichtet sind, zertifizierte Produkte bei öffentlichen Ausschreibungen zu bevorzugen und selbst möglichst weitgehend zertifizierte Produkte zu verwenden.[338]

4.1.10 Institutionalisierte Grundrechtskontrolle

Der Schutz der informationellen Selbstbestimmung bedarf schließlich einer objektiven Ordnung, die in der Praxis mehr und mehr an die Stelle individueller Rechtewahrnehmung tritt. Die Einhaltung von Datenschutzvorgaben kann künftig immer weniger von der individuellen Kontrolle des Betroffenen abhängig gemacht werden. Sie muss in noch viel stärkerem Maß stellvertretend Aufsichtsverfahren und Aufsichtsstellen übertragen werden, die das Vertrauen der Betroffenen genießen. Gegenstand der Kontrolle müssen Systeme mit ihren Funktionen und Strukturen sein, nicht so sehr die individuellen Daten. Ziel der Aufsicht muss es sein, die individuellen und gesellschaftlichen Wirkungen der technischen Systeme zu überprüfen und diese daten-

---

337 *Roßnagel,* in: ders. 2003, 439 ff.

338 *Roßnagel/Pfitzmann/Garstka* 2001, 143 ff.

schutzgerecht zu gestalten. Neben der behördlichen Kontrolle sollten auch Kontrollen durch Verbände[339] und durch Institutionen erfolgen können, die an der Einhaltung eines lauteren Wettbewerbs interessiert sind.

4.2 Konkrete Regelungsvorschläge

Diese allgemeinen Erwägungen zu einer Verbesserung des Datenschutzes angesichts der Herausforderungen moderner Informationstechniken werden in diesem Kapitel bezogen auf die beispielhaft herangezogenen Technikanwendungen konkretisiert.

4.2.1 Smart Car

Der Datenschutz bei Smart Cars bedarf einer spezifischen Regelung, weil nur so die besonderen Risiken durch die Verarbeitung von personenbezogenen Daten aus dem vernetzten und künftig selbständig fahrenden Auto adäquat erfasst und allen Beteiligten eine entsprechende Rechts- und Innovationssicherheit geboten werden können. Auch der 52. Deutsche Verkehrsgerichtstags 2014 empfiehlt, den „Austausch von Daten und Informationen aus dem Fahrzeug Regeln (zu unterwerfen) …, die das informationelle Selbstbestimmungsrecht durch Transparenz und Wahlfreiheit der Betroffenen (zum Beispiel Fahrzeughalter und Fahrer) sichern".[340]

Hinsichtlich der Transparenz für Betroffene hält der 52. Deutschen Verkehrsgerichtstag eine umfassende und verständliche Information für erforderlich, bei welchem Dienst „welche Daten generiert und verarbeitet werden sowie welche Daten auf welchen Wegen und zu welchen Zwecken übermittelt werden. Änderungen dieser Inhalte sind rechtzeitig anzuzeigen."[341] Diese Anforderung kann nicht nur für die

---

339 Zur Erweiterung des § 2 Abs. 2 Nr. 11 UKlaG um Datenschutznormen s. *Spindler*, ZD 2016, 114 ff.

340 S. Empfehlung Nr. 1 des Arbeitskreises VII des 52. Deutschen Verkehrsgerichtstags, in: 52. Deutscher Verkehrsgerichtstag, XV.

341 S. Empfehlung Nr. 2 des Arbeitskreises VII des 52. Deutschen Verkehrsgerichtstags, in: 52. Deutscher Verkehrsgerichtstag, XV.

Auto-Hersteller gelten, sondern ist auch für alle anderen Anbieter von Diensten für Smart Cars anzuwenden. Auch sie müssen verständliche Informationen vor Abschluss des Vertrags bieten und situationsgerechte Anzeigen ermöglichen.[342] Notwendig wäre eine situationsangepasste Information, die mindestens drei Ebenen umfasst: Allgemeine Strukturinformationen sollten ständig – auf einer Website – bereit gehalten werden, auf die mit dem Kaufvertrag und in Allgemeinen Geschäftsbedingungen aufmerksam gemacht wird. Mit der Inbetriebnahme der jeweiligen Funktion muss im Auto eine technische Anzeige erfolgen, dass diese Funktion eingeschaltet ist, und schließlich muss bei der aktuellen Nutzung des Autos auf dem Armaturenbrett auf die derzeit genutzten Dienste hingewiesen werden. Bei einer Aktivierung der Anzeige können weitere Informationen zum Datenschutz abgerufen werden.

Weil die Rollen nicht eindeutig festliegen und vielfach ein Rollenwechsel erfolgt, müssen die Informationspflichten dem angepasst werden. Aufklärungspflichten über die Verarbeitung personenbezogener Daten dürfen daher nicht nur für den Verkäufer gegenüber dem Käufer und dem Diensteanbieter gegenüber dem Nutzer bestehen, sondern sind auch erforderlich für den Halter gegenüber dem Fahrer und für den Fahrer gegenüber Mitfahrern. Diese Aufklärungspflichten müssen sich vor allem auf die für einen Dienst vorgesehenen Möglichkeiten der Datenerhebung und -verwendung (Strukturinformationen) erstrecken.

Informationelle Selbstbestimmung kann nur bestehen, wenn Halter oder Fahrer Wahlmöglichkeiten hinsichtlich der verschiedenen Dienste und ihrer Konfiguration haben.[343] „Bei der freiwilligen oder vertraglich vereinbarten Datenübermittlung an Dritte sind Fahrzeughal-

---

342 S. z.B. auch der Vorschlag eines "Security and Privacy in your Car Act" der Senatoren *Markey* und *Blumenthal* vom 21.7.2015; s. hierzu auch *Keppeler*, RDV 2015, 299 ff.

343 S. hierzu auch den Vorschlag eines "Security and Privacy in your Car Act" der Senatoren *Markey* und *Blumenthal* vom 21.7.2015; s. auch *Keppeler*, RDV 2015, 299 ff.

ter und Fahrer technisch und rechtlich in die Lage zu versetzen, diese zu kontrollieren und gegebenenfalls zu unterbinden."[344]

Für die Gestaltung des Smart Car und die angebotenen Dienste sollte es risikoadäquate Vorgaben für „Privacy by Design" und „Privacy by Default" geben.[345] Diese sollten auch die Architektur der Datenverarbeitung betreffen: So sollten personenbezogene Daten prinzipiell im Auto selbst verbleiben und nur anonymisierte oder pseudonymisierte Daten im Backend der Hersteller oder Diensteanbieter verarbeitet werden. Die Anforderungen an den Datenschutz gegenüber Herstellern sollten – wie beim eCall[346] – bei der Zulassung der Automobile geprüft werden. Die Umsetzung der Anforderungen gegenüber Diensteanbietern sollten diese durch ein Audit oder eine Zertifizierung der Datenschutzanstrengungen nachweisen.[347] Sie sollten dazu durch die Bundesregierung angehalten werden.

Gegenstand der spezifischen gesetzlichen Regelungen zu Smart Cars müssen auch die Zweckbestimmung und die Absicherung von Zweckbindungen sein. So sollte zum Beispiel festgelegt werden, welche Datenkategorien nur flüchtig und welche für einen gewissen Zeitraum, welche anonym, pseudonym und personenbezogen gespeichert werden dürfen. Aus diesen Festlegungen müssen sich Begrenzungen für Einwilligungserklärungen und Allgemeine Geschäftsbedingungen ergeben.

Zulässige Zweckänderungen sollten spezifisch und bestimmt geregelt werden. Eine solche Zweckänderung könnte sich für die Aufklärung von Verkehrsunfällen ab einer bestimmten Schwere ergeben. Hier könnte auf bestimmte Speicherungen von Fahrzeugzuständen direkt vor dem Unfallgeschehen zurückgegriffen werden. Um dies zu erleichtern, empfiehlt der 52. Deutsche Verkehrsgerichtstag: „Für Un-

344 S. Empfehlung Nr. 3 des Arbeitskreises VII des 52. Deutschen Verkehrsgerichtstags, in: 52. Deutscher Verkehrsgerichtstag, XV.
345 S. hierzu beispielhaft *Rieß/Gress*, DuD 2015, 402 ff.
346 S. Kap. 2.4.1.
347 S. zu diesen *Roßnagel* 2010, 263 ff.

falldatenspeicher, Event Data Recorder usw. ist ein Standard vorzuschreiben."[348] Er empfiehlt weiter: „Bei Daten, die aufgrund gesetzlicher Regelungen erhoben, gespeichert oder übermittelt werden sollen, sind verfahrensrechtliche und technische Schutzvorkehrungen genau zu bestimmen."[349] Auch für den Zweck der Strafverfolgung sind Zweckänderungen vorzusehen: „Zugriffsrechte der Strafverfolgungsbehörden und Gerichte sind unter konsequenter Beachtung grundrechtlicher und strafprozessualer Schutzziele spezifisch zu regeln."[350]

Schließlich sollte sichergestellt werden, dass der Halter die in seinem Auto erzeugten Daten auch selbst nutzen kann. Der Zugang zu diesen Daten sollte nicht als Markthindernis für die Wartung und Reparatur des Autos genutzt werden können. Daher sollte dem Halter oder seinem Beauftragten der Zugang zu den Daten in seinem Auto technisch ermöglicht werden, die für ein Marktangebot wesentlich sind, soweit der Halter seine Erlaubnis zum Umgang mit den personenbezogenen Daten gegeben hat.[351]

4.2.2 Smart Home

Vorschläge zur Regelung des Smart Home sind notwendigerweise stark abhängig davon, welche Ausprägung des Smart Home letztlich zugrunde gelegt wird. Ein Regelungsmodell, das zukunftsfest sein und dabei einerseits den Schutz der Betroffenen, andererseits aber auch die wirtschaftlichen Interessen der Hersteller im Blick haben soll, die auf Rechts- und Investitionssicherheit angewiesen sind, darf nicht lediglich den heute üblichen und noch relativ geringen Stand der Vernetzung und Digitalisierung von Haustechnik zugrunde legen, sondern muss bereits jetzt auf die technischen Visionen zur Zukunft des Smart Home reagieren. Dieses Regelungsmodell muss – ganz allge-

---

348 S. Empfehlung Nr. 3 des Arbeitskreises VII des 52. Deutschen Verkehrsgerichtstags, in: 52. Deutscher Verkehrsgerichtstag, XV.

349 S. Empfehlung Nr. 4 des Arbeitskreises VII des 52. Deutschen Verkehrsgerichtstags, in: 52. Deutscher Verkehrsgerichtstag, XV.

350 S. Empfehlung Nr. 5 des Arbeitskreises VII des 52. Deutschen Verkehrsgerichtstags, in: 52. Deutscher Verkehrsgerichtstag, XV.

351 S. *Roßnagel* 2014a, 275 ff.

mein gesprochen – risikoadäquat sein.[352] Das bedeutet vor allem, dass berücksichtigt werden muss, dass es sich bei der eigenen Wohnung um einen rechtlich besonders geschützten Rückzugsort handelt.

Insgesamt lässt sich die Herstellung von Transparenz bezüglich Art und Umfang der Datenverarbeitung als zentrale Herausforderung des Smart Home und von Assistenzsystemen im Allgemeinen beschreiben.[353] Hierzu gehört auch eine verständliche Aufklärung der Betroffenen über die Auswertungsmöglichkeiten. Das oben angeführte Beispiel der Ableitung der Erkennbarkeit etwa des betrachteten Fernsehprogramms aus Stromdaten bei der Wahl kurzer Ableseintervalle[354] zeigt, dass sich Auswertungsmöglichkeiten ergeben können, die selbst für den technisch versierten Verbraucher nur schwer oder gar nicht antizipierbar sind.

Eng verbunden mit der Herstellung von Transparenz ist die individuelle Kontrolle des Betroffenen als zentrales datenschutzrechtliches Prinzip. Die rechtliche Verankerung von Privacy by Design für Systeme des Smart Home, bei direkter Adressierung der Hersteller dieser Systeme, könnte hier den Betroffenen helfen, die Hoheit über die eigenen Daten zurückzuerlangen. Eine datenschutzfreundliche Ausgestaltung verringert ferner die Attraktivität des Systems für Datendiebe und mindert zugleich die kommerzielle Ausbeutbarkeit des Systems durch die Auswertung gesammelter Daten. Jedoch stößt der Ansatz dort an Grenzen, wo ein Haussystem funktionsbedingt auf umfassende Datenerhebung und -verarbeitung angewiesen ist, sowie dort, wo Dienstleistungen – vordergründig kostenlos – im Tausch gegen Daten angeboten werden.

Der Herstellung von Transparenz dienlich wären auch an die Anbieter adressierte Pflichten zur Bereitstellung von Informationen, die über die Funktionalitäten und Risiken des Smart Home aufklären. Solche

---

352 S. hierzu auch *Skistims* 2016, 534 ff.
353 S. hierzu auch Skistims 2016, 541f.
354 S. Kap. 1.1.2.

Informationen müssten nicht nur dem Eigentümer des Smart Home bereitgestellt werden, sondern auch Mietern, Bewohnern, die nicht in die Einrichtung des Systems involviert sind, und Gästen. Fraglich ist, welche Inhalte genau bereitgestellt werden sollten. Die Bereitstellung in Form von langen und komplex formulierten Texten ist jedenfalls nicht zielführend. Es muss aber die Logik der Datenverarbeitungsstruktur des Smart Home dargestellt werden und dies nicht fortlaufend bei jedem relevanten Vorgang, sondern situationsgerecht, etwa wenn neue Personen mit den Systemen des Smart Home in Kontakt kommen oder sich Änderungen in der Funktionalität ergeben. Hier bietet sich die Vereinfachung der Komplexität des Systems durch konkrete und einfach zu fassende Beispiele an. Der Betroffene darf durch die bereitgestellten Informationen nicht überfordert und auch nicht ungebührlich gestört werden, schon um ein Abstumpfen gegenüber den Informationen zu verhindern. Besonders relevante, weil besonders invasive Praktiken betreffende Informationen sind zu priorisieren. Dies könnte beispielsweise der prominent präsentierte Hinweis sein, dass Daten ins außereuropäische Ausland fließen.

Gemeinsame technische Standards, die die Kommunikation von Geräten innerhalb des Smart Home ermöglichen, existieren derzeit noch nicht. Sollten sich hier Standards durchsetzen, die nach dem Stand von Wissenschaft und Technik als unsicher bezeichnet werden müssen, oder aber Monopolbildungen befördern, so ist gegebenenfalls der Gesetzgeber gefordert.

Im Bereich des Smart Metering sollte vor allem § 60 Abs. 5 MsbG so angepasst werden, dass Messstellenbetreiber bereits die datensparsamste Konfiguration vorwählen müssen, anstatt die Verantwortung hierfür auf den Berechtigten zu verlagern. Von dieser könnte der Berechtigte dann durch informierte Einwilligung im Sinne von weniger datensparsameren Einstellungen abweichen; nicht umgekehrt. Zu verhindern ist ferner, dass sich Geschäftsmodelle herausbilden, bei denen Verbilligungen an die Wahl weniger datensparsamer Voreinstellungen geknüpft werden. Zudem sollten wirksame Bußgeldvorschriften für

Verstöße gegen die Regelungen des Messstellenbetriebsgesetzes geschaffen werden. Die Pflicht zur Installation eines entsprechenden Messgeräts ist ebenfalls kritisch zu hinterfragen und kann nur dann gerechtfertigt sein, wenn ihr hohe Standards zu Datenschutz und Datensicherheit gegenüber gestellt werden.

Insgesamt ist aufgrund der potentiellen Aussagekraft von Energieverbrauchsdaten ein hohes Schutzniveau bei der Erhebung, wie auch bei der Übertragung und Verarbeitung dieser Daten zwingend notwendig. Das geplante Messstellenbetriebsgesetz ist hier grundsätzlich ein Schritt in die richtige Richtung. Allerdings müssten bis zum Abschluss des Gesetzgebungsverfahrens die aufgezählten Defizite beseitigt werden.

Zusammenfassend ist im Bereich des Smart Home die Adressierung der besonderen Risiken umfassender Datenverarbeitung im privatesten Bereich durch bereichsspezifische Regelungen angezeigt, die einerseits in der Bildung extensiver Profile, andererseits in den vielfältigen Möglichkeiten der Einwirkung auf die Bewohner des Smart Home und des Missbrauchs begründet sind.[355] Vorbildcharakter könnten hier die geplanten gesetzlichen Vorgaben zu Smart Metering haben, insbesondere die dort vorgesehene Zertifizierungspflicht. Hierdurch würde die Kontrolllast vom Betroffenen auf eine Vorabkontrolle durch Experten verlagert. Dabei ist darauf zu achten, dass nicht einzelne Aspekte des Systems mit Verweis auf das Geschäftsgeheimnis der Hersteller von der Kontrolle ausgenommen werden dürfen.

Eine ausreichende Rechtfertigung für die Installation von Ereignisschreibern, wie sie im Zusammenhang mit Smart Cars zur Aufklärung von Unfällen gefordert werden,[356] ist im Falle des Smart Home nicht ersichtlich. Zwar könnten solche Schreiber zur Aufklärung schwerer Straftaten beitragen, indem etwa die Anwesenheit einer bestimmten Person in der Wohnung zur Tatzeit im Falle eines Tötungsdelikts mit-

[355] S. hierzu auch *Skistims* 2016, 530 ff.
[356] S. Kap. 4.2.1.

tels der aufgezeichneten Daten belegt wird, der Eingriff durch das ständige Mitlaufen eines Ereignisprotokolls im intimsten Rückzugsraum des Menschen wiegt aufgrund seiner besonderen Breiten- und Tiefenwirkung auch in diesem Fall jedoch schwerer als das Aufklärungsinteresse.[357] So müssten in diesem Fall deutlich längere Zeiträume aufgezeichnet werden, als im Falle des Unfalldatenschreibers im Smart Car, und eine Vermeidung der Erfassung durch die Sensorik etwa durch das Tragen einer Gesichtsmaske zur Umgehung der Gesichtserfassung ist leicht möglich. Die bereits bestehenden polizeilichen Zugriffsrechte[358] sind vielmehr grundsätzlich ausreichend.

4.2.3 Smart Health

Das bisherige datenschutzrechtliche Konzept zum Umgang mit Gesundheitsdaten fußt im Wesentlichen darauf, dass die Daten durch besonders qualifiziertes und in Bezug auf die Datenschutzrisiken sensibilisiertes medizinisches Personal insbesondere Ärzte erfolgt, die der strafrechtlichen Geheimhaltungspflicht unterliegen. Zudem wird für den Umgang mit Gesundheitsdaten eine strenge Zweckbindung angeordnet. Entsprechend sind die Erlaubnistatbestände ausgestaltet. Die Datenerhebung und anschließende Übermittlung durch den Betroffenen wird nicht datenschutzrechtlich erfasst. Dies ist zwar bezogen auf die informationelle Selbstbestimmung, die auch die freie Entscheidung über die Weitergabe der Daten umfasst, grundsätzlich konsequent. Es stellt sich allerdings die Frage, ob dies im Hinblick auf die Begehrlichkeiten an den Gesundheitsdaten noch risikoadäquat ist. Versicherungen haben bereits Interesse geäußert und auch für Arbeitgeber, Forschungseinrichtungen und Unternehmen der Gesundheitsbranche ist das Potential dieser Daten beachtlich. Elektronische Patientenakten und medizinische Identitäten sind zudem zunehmend Angriffsziel von Hackern und Kriminellen, die diese Informationen für weitere Straftaten wie Versicherungsbetrug, Identitätsdiebstahl oder Erpres-

---

[357] Man vergleiche hierzu die Vorgaben aus *BVerfGE* 125, 260 und *EuGH*, Urt. v. 8.4.2014, C-293/12, C-594/12.

[358] S. Kap. 2.4.1.2.

sung der Krankenhäuser einsetzen.[359] Gesetzliche Erlaubnistatbestände für den Umgang mit den eigenen personenbezogenen Daten sind kaum vorstellbar. Die daraus resultierende gesetzliche Pflicht zum Selbstschutz wäre wohl nicht mit der informationellen Selbstbestimmung in Einklang zu bringen – auch nicht unter Berufung auf die grundrechtliche Schutzpflicht des Staates.[360] Diese könnte aber zum Beispiel durch gesetzliche Informations- oder sogar Warnpflichten gegenüber dem Betroffenen erreicht werden. Es wäre denkbar, für jegliche Hard- und Software, die auf den Umgang mit Gesundheitsdaten abzielt, eine verbindliche Risikoaufklärung einzuführen, die insbesondere von den Herstellern zu erfüllen wäre.

Werden Gesundheitsdaten immer häufiger durch Hard- und Softwaretechniken, die vom Betroffenen bedient werden, und in nahezu jedem Lebensbereich erzeugt, wächst die Bedeutung der Datensicherheit im Sinne des technischen Datenschutzes. Bisher basiert der zusätzliche Schutz für besondere Kategorien von Daten primär auf spezifischen Erlaubnisvorschriften und einigen weiteren Sonderregelungen.[361] Ein gegenüber der Anlage zu § 9 BDSG höherer Sicherheitsstandard ist für diese Datenkategorien erstaunlicherweise nicht vorgesehen.[362] Es sollte einerseits ein dem höheren Schutzbedarf der besonderen Datenkategorien entsprechendes Schutzkonzept aus technischen und organisatorischen Maßnahmen entwickelt werden, auf dessen Einhaltung die datenverarbeitenden Stellen zu verpflichten sind. Andererseits sollten Maßnahmen zum technischen Selbstdatenschutz durch den Betroffenen entwickelt und deren Integration in die Technik verbindlich gefordert werden.

---

359 S. *Hulverscheidt,* Plötzlich drogensüchtig, Süddeutsche Zeitung vom 25.2.2016; *Finsterbusch,* Hacker erbeuten Patientenakten Schaden von 20 Milliarden Dollar / Der Schwarzmarkt blüht, Frankfurter Allgemeine Zeitung vom 25.2.2016.

360 Davon zu differenzieren sind datenschutzrechtliche Beschränkungen z.B. bezogen auf den gesetzlichen Ausschluss einer Einwilligung zum Schutz Dritter.

361 S. Kap. 2.4.1.3.1.

362 *Jandt/Steidle*, CR 2013, 338.

Gesundheitsdaten werden neben dem Datenschutzrecht regelmäßig ergänzend durch die ärztliche Schweigepflicht und damit durch zwei parallele Regelungsansätze geschützt. Dieser doppelte Schutz entfällt im Bereich Smart Health häufig, so dass ein adäquates Schutzinstrument gefunden werden sollte, um den Wegfall des originären Vertraulichkeitsschutzes zu kompensieren. Dies könnte grundsätzlich entweder durch eine Änderung des Datenschutz- oder des Strafrechts erfolgen. Aufgrund der Entwicklung der elektronischen Datenverarbeitung wurde § 203 Abs. 2a StGB im Jahr 2006 eingeführt. Danach macht sich ein Beauftragter für den Datenschutz entsprechend den Absätzen 1 und 2 der Vorschrift strafbar, wenn er unbefugt ein fremdes Geheimnis im Sinne dieser Vorschriften offenbart, das ihm in seiner beruflichen Eigenschaft anvertraut worden oder sonst bekannt geworden ist und von dem er bei der Erfüllung seiner Aufgaben als Beauftragter für den Datenschutz Kenntnis erlangt hat. Eine vergleichbare Ergänzung könnte für Anbieter von Hard- und Software, die auf den Umgang mit Gesundheitsdaten abzielen, eingeführt werden, sofern sie den originären Zugriff auf die Gesundheitsdaten erhalten. Das Bundesdatenschutzgesetz enthält mit § 44 in Verbindung mit § 43 BDSG bereichsspezifische Strafvorschriften. Der rechtswidrige Umgang mit Gesundheitsdaten oder allgemein besonderen Arten personenbezogener Daten wird in § 43 BDSG weder isoliert noch unter Bezugnahme auf die Erlaubnisvorschriften gemäß §§ 13 Abs. 2, 14 Abs. 6 und 28 Abs. 6 bis 8 BDSG als Ordnungswidrigkeit eingestuft und kann infolge dessen auch keine Straftat gemäß § 44 BDSG darstellen. Um bei einem rechtswidrigen Umgang mit Gesundheitsdaten zumindest auch die Möglichkeit zu haben, diese strafrechtlich zu sanktionieren, wäre eine entsprechende Ergänzung der §§ 43 und 44 BDSG sinnvoll.

Bei den Regelungsdefiziten wurde auf das strafrechtliche Problem der externen Datenverarbeitung im Gesundheitsbereich hingewiesen. Dies könnte ebenfalls durch eine Änderung von § 203 StGB bezogen auf externe IT-Dienstleister gelöst werden, sofern es rechtspolitisch gewollt ist. Alternativ könnte auf den Regelungsansatz zurückgegriffen wer-

den, der in einigen Krankenhausgesetzen der Länder verfolgt wird.[363] Gemäß § 48 LKHG BW ist die Auftragsdatenverarbeitung von Patientendaten nur zulässig, wenn sie gemäß Abs. 1 durch ein anderes Krankenhaus erfolgt oder gemäß Abs. 2 durch ein Rechenzentrum erbracht wird, sofern die zuständige Datenschutzaufsichtsbehörde benachrichtigt, den Mitarbeitern des Auftragsnehmers eine § 203 StGB entsprechende Schweigeplicht auferlegt und die erforderlichen technischen und organisatorischen Maßnahmen schriftlich festgelegt werden.

Die strafprozessualen Zugriffsbefugnisse und auch deren Einschränkungen durch das Zeugnisverweigerungsrecht sind noch vor dem Hintergrund erlassen worden, dass vertrauliche Gesundheitsinformationen vornehmlich im Behandlungsverhältnis zwischen Arzt und Patienten in einer Art und Weise dokumentiert worden sind, die einen Zugriff durch die Sicherheitsbehörden ermöglichen. Da diese Konstellation bei Wearables nicht gegeben ist, gibt es für die Sicherheitsbehörden eine neue Quelle, um Gesundheitsdaten von Beschuldigten zu erheben. In die Diskussion um eine Erweiterung der beruflichen Schweigepflichten gemäß § 203 StGB für Anbieter von Hard- und Software, die auf den Umgang mit Gesundheitsdaten abzielen, ist entsprechend die Erweiterung des Zeugnisverweigerungsrechts zu berücksichtigen. Zugunsten von Beschuldigten eines Strafverfahrens greift zwar der in § 136 Abs. 1 Satz 2 StPO normierte Grundsatz der Aussagefreiheit, doch folgt aus diesem keine Begrenzung bei den staatlichen Zugriffsbefugnissen. Anderenfalls hätten die Strafverfolgungsbehörden kaum Möglichkeiten, Straftaten aufzuklären und durch die Sammlung von Beweismitteln die Justiziabilität herzustellen. Der Beschuldigte kennt in der Regel das Material, das ihn belastet, und kann dieses rechtzeitig vernichten. Diese Überlegungen können auch auf die mittels Wearables erlangten Gesundheitsdaten übertragen werden.

[363] Im hessischen Krankenhausgesetz (HKHG) findet sich keine entsprechende Regelung.

Es bleibt zu beobachten, ob Wearables und deren umfangreiche Datenerhebung das Risiko begründen, die strengen Voraussetzungen von § 81a StPO zu unterlaufen. Nach dieser Vorschrift sind körperliche Untersuchungen des Beschuldigten nur sehr eingeschränkt zulässig. Sollten aus den Datenspeicherungen bei Wearables die gleichen Erkenntnisse gezogen werden können, die bisher nur durch eine körperliche Untersuchung erlangt worden sind, wäre dies gegebenenfalls als weiteres Regelungsdefizit einzustufen.

4.2.4 Big Data

Für die Auswertung personenbezogener Daten durch Big Data-Anwendungen sind bereichsspezifische Regelungen notwendig, die mit den spezifischen Regelungen des Anwendungsbereichs harmonieren. Die folgenden Empfehlungen beschränken sich auf allgemeine Vorgaben, die bereichsspezifisch und risikoadäquat konkretisiert werden müssten.

4.2.4.1 Big Data-Analysen mit personenbezogenen Daten

Im Hinblick auf die personenbezogene Profilbildung mit Hilfe von Big Data sollten die Regelungen zum Scoring in § 28b BDSG und zur automatisierten Einzelentscheidung in § 6a BDSDG aufgegriffen und insbesondere bezüglich der Transparenz der Score-Verfahren und der Beschränkung diskriminierender Merkmale weiterentwickelt werden.[364] Sie könnten durch den statistischen Ansatz von Big Data und die Überzeugungskraft der gewonnenen Ergebnisse zu zwei der wichtigsten Datenschutzregeln der Zukunft werden. Diesbezüglich ist der Gesetzentwurf der Bundestagsfraktion von Bündnis90/Die Grünen aus dem Mai 2015 zur „Verbesserung der Transparenz und der Bedingungen beim Scoring" beachtenswert.[365] Mit dem Gesetzentwurf soll unter anderem in § 28b Abs. 1 BDSG geregelt werden, dass Anschriftendaten, Daten aus sozialen Netzwerken, Daten aus Internetforen,

[364] *Weichert*, ZRP 2014, 168.
[365] BT-Drs. 18/864.

Angaben zur Staatsangehörigkeit, zum Geschlecht, zu einer Behinderung oder Daten nach § 3 Abs. 9 BDSG für die Berechnung des Wahrscheinlichkeitswerts für die Prüfung der Bonität nicht genutzt werden dürfen. Da diese Daten nicht direkt das Zahlungsverhalten der Betroffenen betreffen und leicht diskriminierende Wirkung entfalten können, wäre eine solche Regelung zu begrüßen.[366] Der Gesetzentwurf schlägt außerdem vor, in den Auskunftsanspruch nach § 34 Abs. 2 Satz 1 BDSG ausdrücklich die Gewichtung der Datenkategorien aufzunehmen, nicht aber die Rechenformel, weil diese als Geschäftsgeheimnis gilt.[367] Eine entsprechende Vorschrift wäre aus Sicht der Betroffenen ein deutlicher Fortschritt beim Grundrechtsschutz.

Der Gesetzentwurf zum Beschäftigtendatenschutz aus dem Jahr 2010[368] enthielt in § 32 Abs. 6 Satz 3 BDSG-E eine Regelung, die für das Bewerbungsverfahren die Erhebung von Daten aus sozialen Netzwerken einschränkt. Solche aus eindeutig berufsbezogenen sozialen Netzwerken (wie zum Beispiel Xing) sollten erhoben werden dürfen, solche aus Netzwerken mit „privater" Ausrichtung (wie zum Beispiel Facebook) nicht. Eine Big Data-Analyse dürfte danach im Bewerbungsverfahren also nicht mit den personenbezogenen Daten aus Facebook abgeglichen werden. Dies würde einen Schutz der Betroffenen vor den Risiken von Big Data im Bewerbungsverfahren bedeuten und wäre daher zu begrüßen.

4.2.4.2 Big Data-Analysen ohne personenbezogene Daten

Werden Daten ohne Personenbezug verarbeitet, entweder weil sie bisher noch nicht personenbezogen waren (zum Beispiel reine Wetterdaten) oder weil sie anonymisiert wurden, greift das Datenschutzrecht nicht. Big Data bietet aber besonders effiziente Mittel, um Daten zu deanonymisieren.[369] Dadurch können Daten lange anonym und daher ohne datenschutzrechtlichen Schutz verarbeitet werden und dann

366 *Roßnagel*, 2015.
367 S. *Roßnagel* 2015, 5f.
368 BT-Drs. 17/4230; hierzu *Seifert*, in: Simitis 2014, § 32 BDSG, Rn. 51.
369 *Roßnagel*, ZD 2013, 562.

durch Big Data-Analysen plötzlich einen Personenbezug erlangen. Der Schutz der informationellen Selbstbestimmung ist dann nachträglich kaum noch möglich. Außerdem können statistische Erkenntnisse aus Big Data-Analysen über menschliches Verhalten und menschliche Merkmale leicht personenbezogen werden, insbesondere wenn es sich um leicht erkennbare äußere Merkmale oder um leicht zu erfragende Indikatoren handelt.[370]

Vor diesem Hintergrund sollte für anonyme Daten ein adäquater Vorsorgeschutz eingerichtet werden. Zum Beispiel könnten die Datenverarbeiter dazu verpflichtet werden zu überprüfen, wie hoch das Risiko einer Deanonymisierung bestimmter anonymisierter Daten einzuschätzen ist. Für Daten mit einem hohen Risiko der Deanonymisierung könnten einzelne Vorschriften des Datenschutzrechts trotz aktuell fehlendem Personenbezug präventiv angewendet werden.[371] Problematisch hieran ist aber, dass die Überprüfung durch die verantwortlichen Stellen selbst zu Interessenkonflikten führen dürfte. Eine zumindest grundsätzliche gesetzliche Typisierung risikoreicher Datenbestände sollte daher in Erwägung gezogen werden.

4.2.4.3 Übergreifende Vorschläge

Sowohl für die personenbezogene als auch für die anonyme Anwendung von Big Data wären gesetzliche Regelungen notwendig, die eine diskriminierungsfreie und transparente Verwertung von Daten vorschreiben. Hierzu sollten insbesondere Verfahren der Auditierung oder Zertifizierung gefördert und mit Blick auf die spezifischen Risiken von Big Data ausgebaut werden.[372] Für Bereiche, in denen die eigene freiwillige Offenbarung von Lebenssachverhalten aufgrund statistischer Datenauswertung negative Konsequenzen für andere Bürger haben kann, sollte eine Beschränkung der datenschutzrechtlichen Einwilligung erwogen werden.[373] Ein Komplex der Regulierung von

---

370 S. Kap. 1.2.4.
371 *Roßnagel/Pfitzmann /Garstka* 2001, S. 61.
372 *Roßnagel*, ZD 2013, 562
373 *Roßnagel*, ZD 2013, 562 (566).

Big Data bestünde dann darin, Daten zu typisieren, in deren (personenbezogene oder anonyme) Verarbeitung aufgrund des Risikos für andere Personen nicht wirksam eingewilligt werden kann. Weiterhin sollte festgelegt werden, welche Datentypen in statistische Analysen, auch anonym, nicht einfließen dürfen und welche Fragestellungen nicht statistisch behandelt werden dürfen.

Die Verarbeitung dieser Daten durch Erlaubnistatbestände müsste nicht vollkommen ausgeschlossen sein, da in Erlaubnistatbeständen weitere drittschützende Voraussetzungen festgelegt werden können. Möglicherweise wäre eine solche Regelung in verallgemeinerter Form auch eine Alternative zur Beschränkung von Einwilligungen. Unabhängig von der genauen Implementierung müsste in jedem Fall diskutiert werden, welche Daten nicht in statistische Auswertungen einfließen dürfen. Die Diskussion kann insofern an die Diskussion um Scoring anknüpfen. Sie reicht jedoch weiter, da über die Kreditwürdigkeit hinaus ständig neue relevante Eigenschaften in den Blickwinkel von Analysen geraten können.

Die in § 30a BDSG geregelte Markt- und Meinungsforschung durch Private sollte stärker reguliert werden. Die Branchenverbände sollten verpflichtet werden, ihren bereits bestehenden Verhaltenskodex dahingehend zu überarbeiten, dass dieser Themenbereiche nennt, die aus Gründen der Wahrung der freien Willensbildung und zum Schutz vor Diskriminierung nicht statistisch untersucht werden dürfen. Hierzu zählen in erster Linie Fragestellungen, die den menschlichen Willensbildungsprozess für immer genauere automatisierbare Einwirkungsstrategien öffnen und die eine Selektion anhand diskriminierender Kriterien ermöglichen oder faktisch herbeiführen. Auch sollten die Markt- und Meinungsforschungsinstitute verpflichtet werden, Beiräte für ihre Forschungsprojekte einzurichten, die eine unabhängige Kontrolle der Qualität der Forschungsprojekte und -ergebnisse gewährleisten.

Big Data-Analysen bei Polizei und Geheimdiensten sind nach geltendem Recht nur sehr eingeschränkt möglich, weil die Verwendung

großer Mengen personenbezogener Daten aus unterschiedlichen Quellen an deren Zweckbegrenzung scheitert. Sollen Big Data-Analysen erlaubt werden, um die Arbeit der Sicherheitsbehörden zu verbessern, müssten für diesen Bereich neue Schutzkonzepte implementiert werden, die die erheblichen Risiken für die Bürger adäquat adressieren. Die dargestellte freiheitsbegrenzende Macht der Statistik kann in der Anwendung durch Sicherheitsbehörden besonders scharfe Wirkung entfalten. Zwar sind staatliche Behörden an klare und strenge Erlaubnistatbestände gebunden und es darf davon ausgegangen werden, dass sie in der Regel rechtskonform handeln. Allerdings können Maßnahmen der Sicherheitsbehörden für die betroffenen Bürger im Vergleich zur Privatwirtschaft sehr empfindliche Freiheitseingriffe bedeuten. Die Diskussion, welches Wissen Strafverfolgung, Gefahrenabwehr und Geheimdienste mit Big Data-Statistik generieren und nutzen sollen, muss daher unter diesen Aspekten und unter Beachtung der besonderen Aufgaben der Sicherheitsbehörden gesondert geführt werden.

5 Datenschutz-Grundverordnung und „smarte“ Informationstechnik

In dem letzten inhaltlichen Kapitel wird untersucht, inwieweit die rechtspolitischen Vorschläge von der Datenschutz-Grundverordnung aufgenommen werden, inwieweit ihre Regelungen diese verfehlen und inwieweit ihre Vorgaben für einen verbesserten Grundrechtsschutz angesichts der neuen Herausforderungen durch „smarte“ Informationstechnik im Alltag und Big Data sogar kontraproduktiv sind. Im ersten Schritt werden die Datenschutz-Grundverordnung kurz vorgestellt und einige allgemeine Regelungen erläutert, die positiv zu bewerten sind (5.1). Im zweiten Schritt werden wichtige allgemeine Regelungen untersucht, die für die Bewältigung der Risiken durch „smarte“ Informationstechnik im Alltag und Big Data von besonderem Interesse sind (5.2). Im dritten Schritt werden die Defizite der allgemeinen Regelungen der Datenschutz-Grundverordnung analysiert (5.3) und im vierten Schritt Vorschläge entwickelt, wie diesen begegnet werden müsste, um den Datenschutz bezogen auf die permanente technische Dynamik zukunftsfähig zu machen (5.4).

5.1 Europäische Datenschutz-Grundverordnung

Nach einem Entwurf der Kommission am 25. Januar 2012, einer Stellungnahme des Parlaments am 12. März 2014 und einer Stellungnahme des Rats am 11. Juni 2015[374] haben sich Rat und Parlament auf eine gemeinsame Fassung geeinigt. Die „Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)“ wurde am 4. Mai 2016 verkündet[375] und trat am 25. Mai 2016 in Kraft. Sie gilt ab dem 25. Mai 2018 in allen Mitgliedstaaten.

---

374 S. zu den drei Entwürfen die Synopse des Bayrischen Landesamts für Datenschutzaufsicht, www.lda.bayern.de.

375 EU ABl. L 119 vom 4.5.2016, 1.

Die Verordnung verfolgt drei Zielsetzungen: Zum einen will sie den Datenschutz angesichts der Herausforderungen der technischen Entwicklung modernisieren und den Schutz der Grundrechte verbessern.[376] Zum anderen will sie das Datenschutzrecht unionsweit harmonisieren und einen soliden, „kohärenten und durchsetzbaren Rechtsrahmen im Bereich des Datenschutzes in der Union" schaffen.[377] Schließlich will sie einheitliche Vorgaben für gleiche wirtschaftliche Bedingungen in der Union bieten und damit den Binnenmarkt stärken.[378]

Die Datenschutz-Grundverordnung enthält 50 Artikel, die das Datenschutzrecht materiell regeln und 49 Artikel, die überwiegend organisatorische Fragen der Datenschutzaufsicht, der Regelungskompetenzen und weitere formelle Themen regeln.

Eine wichtige Änderung bringt die Datenschutz-Grundverordnung in Art. 3 Abs. 2 in der Ausweitung des räumlichen Anwendungsbereichs durch das Marktortprinzip. Danach soll nicht mehr der Ort, an dem der Datenverarbeiter niedergelassen ist, für die Anwendung des Datenschutzrechts entscheidend sein, sondern ob personenbezogene Daten von Personen verarbeitet werden, die sich in der Union aufhalten. Voraussetzung ist hierfür, dass der Verarbeiter entweder der betroffenen Person Waren oder Dienstleistungen anbietet oder die Datenverarbeitung der Beobachtung ihres Verhaltens in der Europäischen Union dient. Damit gilt die Datenschutz-Grundverordnung auch gegenüber den vielen geldfreien Internetdienstleistungen, die Anbieter außerhalb der Union anbieten. Diese Erweiterung sorgt auf dem europäischen Markt für Wettbewerbsgleichheit zwischen Anbietern in der Union und Anbietern außerhalb der Union und vereinfacht die Wahrnehmung von Betroffenenrechten.

---

376 S. hierzu Erwägungsgrund 1, 2, 4 und 6 DSGVO.
377 S. hierzu Erwägungsgrund 3 und 9 DSGVO.
378 S. Erwägungsgrund 5 und 10 DSGVO.

Eine auffällige Veränderung bringt auch Art. 83 DSGVO, der sich mit Sanktionen von Verstößen gegen Vorgaben der Datenschutz-Grundverordnung befasst. Art. 83 Abs. 5 DSGVO bestimmt, dass bei Verstößen gegen die dort aufgelisteten Bestimmungen Geldbußen von bis zu 20 Mio. Euro oder im Fall eines Unternehmens von bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt werden können, je nachdem, welcher der Beträge höher ist. Solche drastischen Strafandrohungen dürften die Beachtung der Vorgaben der Verordnung sicher unterstützen.

5.2 Anwendbarkeit allgemeiner Vorschriften der Datenschutz-Grundverordnung

Die Datenschutz-Grundverordnung enthält bewusst keine Vorschriften für die als Beispiele untersuchten „smarten“ Informationstechniken im Alltag und Big Data-Anwendungen. Daher werden im Folgenden die allgemeinen Datenschutzregelungen näher untersucht, in denen vorrangig Vorgaben für die Bewältigung der Risiken für Grundrechte enthalten sind, die von diesen Beispielen ausgehen können. Untersucht wird, welche Antworten sie für die analysierten Regelungsdefizite bieten.

5.2.1 Zweckbindung und Erforderlichkeit

Die Datenschutz-Grundverordnung stand seit dem Ratsentwurf[379] in der medialen Berichterstattung unter dem Eindruck, er würde das datenschutzrechtliche Prinzip der Zweckbindung aufweichen.[380] Eine Aufweichung des Zweckbindungsprinzips hätte grundlegende Auswirkungen auf die Stabilität des datenschutzrechtlichen Regulierungskonzepts allgemein und insbesondere im Hinblick auf die hier behandelten Anwendungsfelder „smarter“ Informationstechnik.

Art. 5 Abs. 1 lit. b) DSGVO fordert, dass personenbezogene Daten nur für genau festgelegte, eindeutige und rechtmäßige Zwecke erhoben

379 Rat der Europäische Union, 9565/15.
380 *Bergemann* 2015; *Schulzki-Haddouti* 2015; *Krempel* 2015.

und nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden dürfen. Der Verordnungsgeber fordert damit ausdrücklich eine Zweckbindung der Datenverarbeitung. In den Erlaubnistatbeständen des Art. 6 Abs. 1 DSGVO ist überdies das Erforderlichkeitsprinzip ausdrücklich als zentrales Tatbestandsmerkmal verankert, das nur in Verbindung mit der Zweckbindung sinnvoll angewendet werden kann.

Die Weiterverarbeitung einmal erhobener personenbezogener Daten bedarf aber nur dann einer gesonderten Erlaubnis, wenn sie mit dem Erhebungszweck nicht vereinbar ist. Die Zweckbindung ist nicht schon bei jedem formalen Unterschied vom Erhebungszweck und nicht nur deshalb, weil ein neuer Verarbeitungsschritt vorliegt, verletzt.[381] Auch die Datenschutzrichtlinie verlangte „nur" Vereinbarkeit mit dem Erhebungszweck. Allerdings entschied über diese Vereinbarkeit bisher der Gesetzgeber, indem er vorschrieb, für welche Weiterverarbeitungen eine gesonderte Erlaubnis nötig war. Die Entscheidung obliegt durch die direkte Anwendbarkeit der Verordnung nun in erster Linie den Datenverarbeitern und kontrollierend den Gerichten. Um genauer zu bestimmen, wann eine Verarbeitung vorliegt, die mit dem Erhebungszweck vereinbar ist, sieht der Verordnungsgeber mehrere Konkretisierungen vor:[382]

Erstens enthält Art. 5 Abs. 1 lit. b) DSGVO, wie auch schon Art. 6 Abs. 1 lit. b) DSRL, die Feststellung, dass „eine Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke oder für wissenschaftliche, statistische oder historische Zwecke gemäß Art. 89Abs. 1 nicht als unvereinbar mit den ursprünglichen Zwecken" gilt. Diesbezüglich ist entscheidend, wie „wissenschaftliche, statistische oder historische Zwecke" zu verstehen ist. Würde darunter jede wissenschaftliche, statistische oder historische Methode zu beliebigen Zielen verstanden, wäre die Zweckbindung abgeschafft. Dann könnten alle Profiling- und Scoring-Verfahren für Werbemaßnahmen oder für die Kre-

381 S. Erwägungsgrund 50 DSGVO.
382 S. ausführlich *Richter,* DuD 2015, 735.

ditvergabe als „Statistik" gelten. Da die Grundverordnung aber ausdrücklich an der Zweckbindung festhält, wäre diese Auslegung systemwidrig. Statistische Verfahren – insbesondere auch Big Data-Analysen, deren Ergebnis für Entscheidungen gegenüber Individuen verwendet werden sollen – können daher nicht mit statistischen Zwecken im Sinn des Art. 5 Abs. 1 lit. b) DSGVO gleichgesetzt werden.[383]

Zweitens nennt Art. 6 Abs. 4 DSGVO fünf abstrakte Kriterien, nach denen zu bestimmen ist, ob sie mit dem festgelegten Erhebungszweck vereinbar sind. Zu „berücksichtigen" sind für diese Bewertung „jede Verbindung“ zwischen dem Erhebungszweck und der weiteren Verarbeitung, der „Zusammenhang, in dem die Daten erhoben wurden“, ob „besondere Kategorien personenbezogener Daten verarbeitet“ werden, die „möglichen Folgen“ der weiteren Verarbeitung und das Vorhandensein „angemessener Garantien“ für die Rechte der betroffenen Personen.[384]

Solche Orientierungen für Datenverarbeiter und Gerichte, um im Einzelfall bestimmen zu können, ob eine Weiterverarbeitung mit dem Erhebungszweck vereinbar ist, sind sehr zu begrüßen. Sie sind auch notwendig, um zu einer einheitlichen Anwendung der Verordnung in den Mitgliedstaaten zu kommen. Die zu beachtenden Faktoren sind allerdings sehr breit formuliert und es ist nicht klar, wie viele der Merkmale und wie intensiv sie vorliegen müssen oder nicht. Die Vorschrift bildet für den für die Verarbeitung Verantwortlichen keine klare Grundlage anhand der er abschätzen könnte, welche Weiterverarbeitungen mit dem Erhebungszweck vereinbar sind und welche nicht. Die aufgeführten Faktoren könnten aufgrund ihrer Breite dazu genutzt werden, jegliche Weiterverarbeitung als vereinbar zu begründen. Ohne weitere Konkretisierung bilden sie jedenfalls keinen Ersatz für ein ausdifferenziertes System von Erlaubnistatbeständen. Der Verordnungsgeber verkennt völlig die legislative Aufgabe, die die nationalen Gesetzgeber an dieser Stelle bisher erfüllten. Bisher war es eine

[383] S. auch Erwägungsgrund 29 DSRL; Art. 29-Datenschutzgruppe 2013, 28.
[384] Diese Kriterien gehen auf einen Vorschlag in Art. 29-Datenschutzgruppe 2013 zurück.

politische Entscheidung, welche Zwecke als vereinbar mit den Erhebungszwecken galten. Indem der Verordnungsgeber von der Datenschutzrichtlinie auf das Instrument der Verordnung umschwenkt und dabei aber den Inhalt der Richtlinie beibehält, entmachtet er die nationalen Gesetzgeber ohne für Ersatz zu sorgen. Er verlagert damit eine wichtige politische Frage auf die Schultern privater Datenverarbeiter.

Entscheidend wird als Ausgangspunkt einer Konkretisierung insbesondere sein, was unter „eindeutigem" Zweck zu verstehen ist, an dem die Vereinbarkeit zu messen ist. Wird der Zweck im Einzelfall ausreichend eng festgelegt, könnten die Kriterien aus Art. 6 Abs. 4 DSGVO einen substantiellen Gehalt bekommen. Wird der Zweck im Einzelfall aber mit den höchst abstrakten Erlaubnistatbeständen des Art. 6 Abs. 1 DSGVO gleichgesetzt, bleiben auch die Kriterien des Art. 6 Abs. 4 DSGVO inhaltsleer. Da die Zweckfestlegung in erster Linie von dem für die Verarbeitung Verantwortlichen abhängt, weil keine spezifischen Zweckfestlegungen durch den Verordnungsgeber erfolgen, ist zu befürchten, dass die Zwecke äußerst breit festgelegt werden, da dies den Datenverarbeitern erhebliche Spielräume für die Weiterverarbeitung eröffnet.

Die verbindliche Konkretisierung von Fallgruppen und Verarbeitungsformen, die als vereinbar oder unvereinbar mit bestimmten Erhebungszwecken gelten, ist nun Fall einer langwierigen Einzelfallaufgabe für die Rechtsprechung. Dass sich schnell (oder überhaupt) eine europaweit kongruente Rechtsprechung herausbildet, ist kaum zu erwarten. Da die Art. 29-Gruppe das „Compatibility Assessment", das in Art. 6 Abs. 4 DSGVO umgesetzt wurde, vorgeschlagen hat, erscheint es sinnvoll, dass sie auch in ihrer neuen Form als Europäischer Datenschutz-Ausschuss hieran weiterarbeitet und Fallgruppen für vereinbare und unvereinbare Weiterverarbeitungen erarbeitet, um den für die Verarbeitung Verantwortlichen (und den Gerichten) eine Orientierungshilfe zu bieten.[385]

[385] Erste Vorschläge bereits in Art. 29-Datenschutzgruppe 2013, 56 ff.; darauf Bezug nehmend *Helbing*, K&R 2015, 148 ff.

Ist die Weiterverarbeitung nach diesen Kriterien mit dem Erhebungszweck unvereinbar, bedarf sie einer eigenen datenschutzrechtlichen Erlaubnis.

Im Hinblick auf die „smarte“ Informationstechnik im Alltag stellen die Neuerungen bei der Zweckbindung eine aus Sicht der Betroffenen sehr unvorteilhafte Entwicklung dar. Über die in Art. 6 Abs. 4 DSGVO niedergelegten Kriterien für eine Vereinbarkeitsprüfung ist einer möglichst weitgehenden Weiterverwendung von personenbezogenen Daten für verschiedenste Zwecke Tür und Tor geöffnet. Die zusätzliche Möglichkeit, trotz Unvereinbarkeit mit dem Erhebungszweck für die Weiterverarbeitung ohne irgendwelche zusätzlichen Anforderungen auf alle vorhandenen extrem abstrakten Erlaubnistatbestände zurückgreifen zu können, entzieht dem Zweckbindungsprinzip praktisch die beschränkende Wirkung. Dies erleichtert die Datenverarbeitung in Smart Car, Smart Home und Smart Health, insbesondere mit Big Data, ungemein. Für die Betroffenen gibt es aber kaum noch Sicherheit, was mit den Daten, die immer weitere Teile ihres Lebens abdecken, vom Verhalten in der Wohnung über das Fahrverhalten, über den Puls und individuelle Gesundheitsrisiken bis hin zu politischen Einstellungen und emotionalen Zuständen, geschehen darf und was nicht.

5.2.2 Transparenz und Betroffenenrechte

Regelungen, die der Herstellung von Transparenz im Rahmen der Erhebung und Verarbeitung von personenbezogenen Daten dienen, finden sich an vielen Stellen der Verordnung.[386] Die folgende Darstellung beschränkt sich auf die zentralen Vorgaben.

Art. 13 und 14 DSGVO enthalten die zentralen Informationspflichten des für die Verarbeitung Verantwortlichen gegenüber der betroffenen Person dahingehend differenziert, ob personenbezogene Daten bei ihr oder bei anderen erhoben werden. Mitzuteilen sind etwa der Name und die Kontaktdaten des für die Verarbeitung Verantwortlichen so-

[386] Der Herstellung von Transparenz dienen zusätzlich zu den im Text genannten letztlich etwa auch die Art. 12, 19, 26, 27 und 31 DSGVO.

wie die Zwecke der Verarbeitung zusammen mit der Rechtsgrundlage der Verarbeitung. Erwähnenswert ist insbesondere die jeweils aus Art. 13 Abs. 2 lit. f) und Art. 14 Abs. 2 lit. g) DSGVO resultierende Pflicht, zur Bereitstellung von „aussagekräftige[n] Informationen über die verwendete Logik" im Falle automatisierter Entscheidungsfindung „sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person".[387] Erwägungsgrund 63 DSGVO relativiert die Informationspflicht dahingehend, dass „die Rechte und Grundfreiheiten anderer Personen, etwa Geschäftsgeheimnisse oder Rechte des geistigen Eigentums und insbesondere das Urheberrecht an Software, nicht angetastet werden". Hoffnungen auf eine Aufdeckung der im Bereich des Scorings verwendeten Algorithmen, die der Bundesgerichtshof noch mit Verweis auf das Geschäftsgeheimnis verneint hatte,[388] müssen angesichts dessen gedämpft werden. Immerhin dürfe die Berücksichtigung der Rechte anderer „nicht dazu führen, dass der betroffenen Person jegliche Auskunft verweigert wird".[389]

Wesentlicher Unterschied von Art. 13 im Vergleich zu Art. 14 DSGVO ist neben dem konkreten Inhalt der Informationspflicht der Zeitpunkt, an dem die Informationspflicht ansetzt. Werden die Daten beim Betroffenen erhoben, so sind die Informationen direkt zum Zeitpunkt der Erhebung zu geben,[390] andernfalls innerhalb einer angemessenen Frist, spätestens aber nach Ablauf eines Monats.[391] Eine Ausnahme von der Informationspflicht liegt nur dann vor, wenn der Betroffene bereits über die Informationen verfügt. Den Direkterhebungsgrundsatz,[392] der

---

387 Zum Profiling s. Kap. 5.2.3.

388 *BGH*, BKR 2014, 193.

389 Erwägungsgrund 51 DSGVO.

390 Art. 13 Abs. 1 und 2 DSGVO.

391 Art. 14 Abs. 3 lit. a) DSGVO. Sollen die Daten zur Kommunikation mit dem Betroffenen genutzt werden, sind die Informationen spätestens zum Zeitpunkt der ersten Kommunikation zu erteilen. Soll eine Weitergabe an einen anderen Empfänger stattfinden, so ist der Zeitpunkt der ersten Weitergabe maßgeblich, s. Art. 14 Abs. 3 lit. b) und c) DSGVO.

392 S. zu diesem § 4 Abs. 2 Satz 1 BDSG.

die beste Sicherung der Transparenz ist, kennt die Verordnung nicht mehr.

Die konkreten Probleme bei der Gewährleistung von Transparenz im Falle von Big Data, Smart Car und Smart Home[393] werden durch diese Informationspflichten der Verordnung nicht adressiert. Es bleibt vielmehr das praktische Problem der Durchführbarkeit, gerade im Kontext von Big Data. Zudem ist keine situationsgerechte Bereitstellung der Informationen vorgesehen; es bleibt unklar, was im laufenden Betrieb passiert. Dies ist aber im Smart Car und im Smart Home von größter Bedeutung. Es müsste verständlich mitgeteilt werden, wo welche Daten erhoben werden. Diesen Anforderungen werden die Art. 13 und 14 DSGVO nicht gerecht.

Nach Art. 30 Abs. 1 DSGVO treffen den für die Verarbeitung Verantwortlichen umfangreiche Dokumentationspflichten, unter anderem zu den Zwecken der Verarbeitung, den Kategorien der verarbeiteten personenbezogenen Daten, gegebenenfalls der Übermittlung an ein Drittland und, wenn möglich, den vorgesehenen Löschfristen. Der Auftragsdatenverarbeiter ist nach Art. 28 Abs. 2 DSGVO mit ähnlichen Pflichten belegt. Die Dokumentation soll „schriftlich“ erfolgen, was ausdrücklich auch die elektronische Dokumentation mit einschließt.[394] Die Einschränkung in Art. 28 Abs. 5 DSGVO, wonach die in Abs. 1 und 2 enthaltenen Pflichten nicht für Unternehmen und Organisationen mit weniger als 250 Angestellten gelten sollen,[395] hat indes das Ziel, kleine und mittelständische Unternehmen zu entlasten.[396] Die Dokumentation ist auf Anforderung der Aufsichtsbehörde zur Verfügung zu stellen.[397]

---

393 S. Kap. 3.3.

394 Art. 28 Abs. 3 DSGVO.

395 Es sei denn, dass die Verarbeitung in dem Unternehmen oder in der Organisation voraussichtlich ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen birgt, die Verarbeitung nicht nur gelegentlich stattfindet oder besondere Kategorien personenbezogener Daten verarbeitet werden.

396 Europäische Kommission, Pressemitteilung 2015, IP/15/5176.

397 Art. 28 Abs. 4 DSGVO.

Art. 33 und 34 DSGVO belegen den für die Verarbeitung Verantwortlichen mit einer Pflicht zur Meldung von Verletzungen des Schutzes personenbezogener Daten. Nach Art. 33 DSGVO ist die Aufsichtsbehörde „ohne unangemessene Verzögerung“[398] von einer solchen Verletzung in Kenntnis zu setzen, es sei denn, es ist unwahrscheinlich, dass die Verletzung ein Risiko für Rechte und Freiheiten des Einzelnen bedeutet. Der Auftragsdatenverarbeiter wiederum hat den für die Verarbeitung Verantwortlichen über jede Verletzung zu informieren und zwar in jedem Fall ohne ungebührliche Verzögerung.[399] Auch nicht meldungspflichtige Verletzungen sind vom für die Verarbeitung Verantwortlichen zu dokumentieren.[400] Die Meldung an die Aufsichtsbehörde hat unter anderem die wahrscheinlichen Konsequenzen der Verletzung und die getroffenen Gegenmaßnahmen zu enthalten.[401] Nach Art 34 Abs. 1 DSGVO ist in bestimmten Fällen auch der Betroffene ohne ungebührliche Verzögerung von einer Verletzung zu unterrichten, die gleichsam der Pflicht zur Unterrichtung der Aufsichtsbehörde an die Wahrscheinlichkeit der Verletzung von Rechten und Freiheiten gekoppelt ist.[402] Art. 34 Abs. 3 DSGVO sieht jedoch eine Reihe von Ausnahmen von dieser Unterrichtungspflicht gegenüber der betroffenen Person vor.[403] Die in der Verordnung enthaltenen Meldepflichten dürften sich gerade mit Blick auf die hohen Risiken bei Zugriffen Unbefugter auf die im Kontext von Smart Car, Smart Home und Smart Health erhobenen Daten positiv auf die Datensicherheit auswirken. Dies wird durch die Bußgeldregelungen in Art. 83 DSGVO, die auch bei Verstößen gegen die Meldepflichten greifen, unterstützt.

---

[398] Oder nicht später als 72 Stunden nach Kenntniserlangung der für die Verarbeitung Verantwortlichen von der Verletzung. Erfolgt die Meldung später als nach 72 Stunden, so ist die Verzögerung zu begründen.

[399] Art. 33 Abs. 2 DSGVO.

[400] Art. 33 Abs. 4 DSGVO.

[401] Art. 33 Abs. 3 DSGVO. Zum Zeitpunkt der Meldung nicht verfügbare Informationen sind nach Art. 33 Abs. 4 DSGVO nachzureichen.

[402] Art. 34 Abs. 2 DSGVO.

[403] Art. 34 Abs. 3 DSGVO.

Als eines ihrer Ziele nennt die Verordnung die „Stärkung und Präzisierung der Rechte der betroffenen Personen“.[404] Die zentralen Rechte des Betroffenen finden sich in Art. 15 bis 21 DSGVO. Es handelt sich konkret um ein Recht auf Auskunft, ein Recht auf Berichtigung, ein Recht auf Löschung,[405] ein Recht auf Einschränkung der Verarbeitung, ein Recht auf Datenübertragbarkeit und ein Recht auf Widerspruch.[406]

Die in Art. 12 bis 22, 34 und teilweise auch die in Art. 5 DSGVO enthaltenen Rechte können nach Maßgabe von Art. 23 DSGVO beschränkt werden, „sofern eine solche Beschränkung den Wesensgehalt der Grundrechte und Grundfreiheiten achtet und in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme darstellt“ bezogen auf zehn näher beschriebene Zwecke und Bereiche, die von der Landesverteidigung bis hin zur Durchsetzung zivilrechtlicher Ansprüche reichen.[407] Jede legislative Maßnahme, die eine solche Beschränkung vorsieht, muss zudem den formellen Anforderungen des Art. 23 Abs. 2 DSGVO entsprechen und etwa den Umfang der vorgenommenen Beschränkungen und die Speicherfristen enthalten. Es ist davon auszugehen, dass die Mitgliedstaaten von den ihnen durch Art. 23 DSGVO eingeräumten Möglichkeiten der Beschränkung regen Gebrauch machen werden. Dadurch könnten die dargestellten Betroffenenrechte erheblich relativiert werden.

Neu ist das Recht auf Datenübertragbarkeit, das in Art. 20 DSGVO geregelt ist. Art. 20 Abs. 1 DSGVO gibt der betroffenen Person das „Recht, die sie betreffenden personenbezogenen Daten, die sie einem für die Verarbeitung Verantwortlichen bereitgestellt hat, in einem strukturierten, gängigen und maschinenlesbaren Format (zurück) zu erhalten“. Sie hat „das Recht, diese Daten einem anderen für die Verarbeitung Verantwortlichen ohne Behinderung durch den für die Bearbeitung Verantwortlichen, dem die Daten bereitgestellt wurden, zu

404 Erwägungsgrund 11 DSGVO.
405 Zum „Recht auf Vergessenwerden“ s. Kap. 5.2.4.
406 S. hierzu auch Erwägungsgrund 63 DSGVO.
407 Art. 23 Abs. 1 DSGVO.

übermitteln". Das Recht greift jedoch nur in den Fällen, in denen die Bereitstellung der Daten aufgrund einer Einwilligung des Betroffenen erfolgt[408] oder die Verarbeitung für die Erfüllung eines Vertrags oder zur Durchführung vorvertraglicher Maßnahmen erforderlich ist[409] und die Verarbeitung mit automatischen Mitteln erfolgt.[410] Explizit ausgeschlossen ist das Recht „für eine Verarbeitung, die für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem für die Verarbeitung Verantwortlichen übertragen wurde".[411]

Wo dies technisch möglich ist, sollen Daten auch auf Verlangen des Betroffenen direkt von einem für die Verarbeitung Verantwortlichen zum anderen übertragen werden. Hintergrund ist hier vornehmlich der Umzug des Betroffenen von einem sozialen Netzwerk in ein anders. Ob diese konkrete Vorschrift in der Praxis große Relevanz entfalten wird, darf aufgrund des Verweises auf die technische Durchführbarkeit und zwischen Anbietern mitunter stark divergierender Standards gerade bezüglich Datenformate bezweifelt werden. Hier ist letztlich abzuwarten, wie eng oder weit diese Einschränkung ausgelegt werden wird.[412]

Besondere risikobezogene Recht der betroffenen Person, die den besonderen Risiken in den Anwendungsbereichen Smart Car, Smart Home, Smart Health und Big Data gerecht werden, enthält die Verordnung nicht.

5.2.3 Profiling

Zu den Vorschriften der Verordnung zu Profiling ist festzustellen, dass an den Grundsätzen des Art. 15 DSRL weitestgehend festgehalten wird. So räumt auch Art. 15 Abs. 1 DSRL dem Betroffenen ein fast

---

408 Art. 6 Abs. 1 lit. a) und Art. 9 Abs. 2 lit. a) DSGVO.
409 Art. 6 Abs. 1 lit. b) DSGVO.
410 Art. 20 Abs. 2 DSGVO.
411 Art. 20 Abs. 3 DSGVO.
412 S. hierzu *Roßnagel/Richter/Nebel*, ZD 2013, 107.

gleichlautendes Recht ein, „keiner für sie rechtliche Folgen nach sich ziehenden und keiner sie erheblich beeinträchtigenden Entscheidung unterworfen zu werden, die ausschließlich aufgrund einer automatisierten Verarbeitung von Daten zum Zwecke der Bewertung einzelner Aspekte ihrer Person ergeht“. Auch bezüglich der Ausnahmen von der Geltung dieses Rechts sowie der Verarbeitung besonderer Kategorien personenbezogener Daten ergeben sich keine substantiellen Unterschiede. Anknüpfungspunkt bleibt die Entscheidung und nicht schon die Profilbildung selbst.

Profiling ist in Art. 4 Nr. 4 DSGVO definiert als „jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren und vorherzusagen“.

Konkret geregelt ist die „automatisierte Generierung von Einzelentscheidungen, einschließlich Profiling“ in Art. 22 der Verordnung. Es handelt sich um eine der wenigen risikobezogenen Regelungen der Verordnung. Nach Art. 22 Abs. 1 DSGVO hat die betroffene Person das Recht, nicht einer solchen Entscheidung unterworfen zu werden, „die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt“. Dabei greift Art. 22 Abs. 1 DSGVO nur, wenn eine Entscheidung „ausschließlich auf einer automatisierten Verarbeitung“ beruht. Die Verordnung nimmt vielfach auch an anderer Stelle ausdrücklich Bezug auf Profiling, so etwa bei den Informationspflichten, bei den Auskunftsrechten und bei der Datenfolgenabschätzung.

Ausnahmen von der Geltung des Art. 22 Abs. 1 DSGVO sieht die Verordnung dann vor, wenn „die Entscheidung für den Abschluss oder die Erfüllung eines Vertrages“ erforderlich ist, sie aufgrund von Rechtsvorschriften zulässig ist oder „mit ausdrücklicher Einwilligung

der betroffenen Person erfolgt".[413] Außer im Falle der Zulässigkeit der Entscheidung aufgrund einer Rechtsvorschrift hat der für die Verarbeitung Verantwortliche „geeignete Maßnahmen" zu treffen, „um die Rechte und Freiheiten sowie die berechtigten Interessen der betroffenen Person zu wahren". Art. 22 Abs. 3 DSGVO präzisiert den Begriff der „geeigneten Maßnahmen" mit der Etablierung eines Mindeststandards, wonach hierzu „mindestens das Recht auf Erwirkung des Eingreifens einer Person seitens des für die Verarbeitung Verantwortlichen, auf Darlegung des eigenen Standpunkts und auf Anfechtung der Entscheidung gehört". Die Nutzung besonderer Kategorien personenbezogener Daten ist zulässig, sofern der Betroffene ausdrücklich zugestimmt hat, die Verarbeitung aus Gründen eines erheblichen öffentlichen Interesses erforderlich ist oder sie aufgrund einer Rechtsvorschrift erfolgt.

Die Vorschriften zum Profiling folgen in ihrer Struktur dem datenschutzrechtlichen Grundsatz, dass im Sinne eines Regel-Ausnahme-Verhältnisses die Verarbeitung personenbezogener Daten verboten ist, wenn nicht ein gesetzlicher Erlaubnistatbestand oder eine Einwilligung des Betroffenen vorliegt.

Zusammenfassend ist festzustellen, dass die Regelung der Datenschutzrichtlinie aus dem Jahr 1995 weitestgehend fortgeführt wird. Die Verordnung umfasst mit ihrem Art. 22 letztlich nur einen kleinen Teil der bereits heute täglich stattfindenden Profilbildungen und lässt etwa die Profilbildung für individualisierte Dienste bei den Internetgiganten Google, Amazon und Facebook außen vor. Auf Ubiquitous Computing ist sie ebenso wenig anwendbar wie auf Smart Car, Smart Home und Smart Health. Auf Big Data-Anwendungen findet sie nur Anwendung, wenn Scoring betrieben wird.

[413] Art. 22 Abs. 2 lit. a) bis c) DSGVO.

5.2.4 „Recht auf Vergessenwerden“

Art. 17 DSGVO trägt die Überschrift „Recht auf Löschung (‚Recht auf Vergessenwerden‘)“. Die Ergänzung in Klammern kann vielleicht schon als Hinweis darauf gewertet werden, dass der Verordnungsgeber selbst Zweifel hinsichtlich eines neu geschaffenen datenschutzrechtlichen Anspruchs hegt. Ein „Recht auf Vergessen“ ist im Entwicklungsprozess der Datenschutz-Grundverordnung immer wieder werbewirksam als Lösung für das faktische Problem angepriesen worden, dass das Internet nichts vergisst. Dennoch ist es verwirrend, dass im Titel der Vorschrift immer noch ein Versprechen gemacht wird, das der darunter stehende Text weder einhält noch einhalten kann.

Art. 17 Abs. 1 DSGVO regelt neben dem Löschungsanspruch des Betroffenen, eine ausdrückliche Löschungspflicht der verantwortlichen Stellen. Sofern einer der sechs aufgelisteten Gründe vorliegt, hat die verantwortliche Stelle die personenbezogenen Daten ohne unangemessene Verzögerung zu löschen. Die schriftliche Fixierung der Löschungspflicht der verantwortlichen Stelle stellt eine Neuerung gegenüber der Datenschutzrichtlinie dar, die in Art. 12 DSRL zugunsten der Betroffenen nur ein Auskunftsrecht explizit vorgesehen hat. In Deutschland sind in § 35 BDSG die Löschung, Sperrung und Berichtung als weitere Rechte der Betroffenen gesetzlich festgeschrieben. § 35 Abs. 2 Satz 2 Nr. 1 bis 4 BDSG definiert vier verschiedene Anwendungsfälle, bei deren Vorliegen personenbezogene Daten zu löschen sind. Dieses Verständnis entspricht auch der Konzeption des Datenschutzrechts. Da gemäß § 4 Abs. 1 BDSG eine Datenverarbeitung nur zulässig ist, wenn eine gesetzliche Erlaubnis oder eine Einwilligung vorliegt, sind unzulässige Datenverarbeitungen rechtswidrig, so dass die personenbezogenen Daten gelöscht werden müssen. Für die systematische Prüfung kann diese Ergänzung durchaus als Fortschritt gewertet werden, obwohl durch sie in Deutschland keine zusätzliche Rechtspflicht begründet wird.

Ergänzend wird in Art. 17 Abs. 2 DSGVO vorgesehen, dass ein zur Löschung verpflichteter Verantwortlicher vertretbare Schritte auch tech-

nischer Art unternehmen muss, um weitere Verantwortliche darüber zu informieren, dass eine betroffene Person von ihnen die Löschung aller Querverweise auf diese personenbezogenen Daten oder von Kopien oder Replikationen dieser Daten verlangt hat. Art. 17 Abs. 3 DSGVO enthält Ausnahmefälle, in denen Abs. 1 und 2 nicht anwendbar sind, wie zum Beispiel den Umgang mit den personenbezogenen Daten zur Ausübung des Rechts auf freie Meinungsäußerung und Information. Diese Informationspflicht geht über die bisherige Löschungspflicht hinaus und scheint Grundlage des Klammerzusatzes „Recht auf Vergessenwerden" in der Überschrift von Art. 17 DSGVO zu sein.

Art. 17 DSGVO lässt mehrere Fragen offen. Erstens bleibt die Rechtsqualität dieser Verpflichtung unklar. Handelt es sich hierbei um eine rechtsdogmatisch neu entwickelte Rechtspflicht, die „ein Vergessen" statuiert oder nur um eine „qualifizierte" Informationspflicht. Zweitens enthält Abs. 3 Ausnahmen von der Löschungs- und der Informationspflicht. Diese enthalten zum einen für einzelne, spezifische Interessenkollisionen der genannten Rechte mit den Interessen Dritter an dem Erhalt der personenbezogenen Daten eine Entscheidung, ohne allerdings umfassend zu sein. So wird zum Beispiel gerade die der Entscheidung des Europäischen Gerichtshofs zugrundeliegende Interessenabwägung zwischen dem Datenschutzrecht und der Pressefreiheit nicht aufgegriffen.[414] Zum anderen ist fraglich, wie das nationale Recht mit diesen Ausnahmeregelungen, die dem Wortlaut nach keine einzelfallbezogene Interessenabwägung zulassen, in Einklang zu bringen ist. Drittens ist offen, welche Maßnahmen zur Erfüllung der Rechtspflichten aus Abs. 2 von dem für die Verarbeitung Verantwortlichen in technischer Hinsicht vorzunehmen sind und wo die Grenze vertretbarer Implementierungskosten liegt.

Die Löschungs- und Informationspflicht des Art. 17 DSGVO ist grundsätzlich sehr abstrakt und allgemein formuliert, so dass sich kaum

[414] *EuGH,* NJW 2014, 2264.

konkrete Schlüsse auf ihre zukünftige Bedeutung für die spezifischen Anwendungsfelder Smart Car, Smart Home, Smart Health sowie Big Data ziehen lassen. In allen diesen Anwendungsfeldern ist die Vorschrift grundsätzlich zu berücksichtigen. Der Eintritt der Löschungspflicht ist dabei maßgeblich von den jeweiligen Zulassungsvorschriften abhängig, allerdings enthält die Datenschutz-Grundverordnung, abgesehen von der Regelung zum Profiling, die auf Big Data Anwendung finden wird, hier ebenfalls keine spezifischen Vorschriften. Die Informationspflicht setzt voraus, dass die Daten von der verantwortlichen Stelle öffentlich gemacht worden sind. Da durch Art. 17 Abs. 2 DSGVO dem „Recht auf Vergessenwerden“ im Netz mehr Geltung verschafft werden soll,[415] ist dieses Merkmal regelmäßig erfüllt, wenn personenbezogene Daten über eine Webseite im Internet für jeden zugänglich abrufbar sind. Bei Smart Car und Smart Home wird der Fokus der Datenverarbeitung voraussichtlich nicht auf einer Verbreitung der Daten über das Internet liegen. Bei Smart Car erfolgt vornehmlich ein Austausch unmittelbar zwischen den vernetzten Fahrzeugen. Für eine Online-Anwendung, zum Beispiel zur Darstellung des aktuellen Verkehrsaufkommens, sind aggregierte und nicht fahrzeugbezogene Daten, zu denen grundsätzlich ein Personenbezug herstellbar ist, zu verwenden. Die Steuerung des Smart Home kann zwar über eine App oder ein Internetportal erfolgen, allerdings wird dies ausschließlich über individuelle Nutzungsbereiche realisiert werden. Die personenbezogenen Daten sind zwar auf diesen Plattformen für die Hausbewohner und gegebenenfalls noch andere Stellen abrufbar, allerdings sind sie beim Einsatz entsprechender Zugriffsschutzmechanismen nicht öffentlich. Beim Wearable Computing kann Art. 17 Abs. 2 DSGVO dagegen durchaus Relevanz entfalten. Der Trend der Selbstvermessung wird von Geschäftsmodellen verstärkt, die gerade einen Vergleich der individuell gemessenen Werte ermöglichen und dadurch anspornen möchten.[416] Die mit den Wearables gesammelten

[415] S. Erwägungsgrund 66 DSGVO.

[416] Z.B. die Laufrangliste des Fitnessportals „runtastic“, https://www.runtastic.com/blog/de/hot-topics-und-reviews/running-leaderboard-auf-runtastic-com/.

Fitness- und Vitaldaten werden auf Fitnessplattformen übertragen, die den Charakter von sozialen Netzwerken aufweisen. Zwar werden diese Fitnessportale regelmäßig die Möglichkeit aufweisen, durch die individuellen Datenschutzeinstellungen den Zugriff auf die Daten zu beschränken. Allerdings besteht weder die datenschutzrechtliche Pflicht, dass bei Anmeldung des Dienstes der höchste Datenschutz voreingestellt ist, noch wird eine Differenzierung der Einstellungsmöglichkeiten zwischen personenbezogenen Daten und sensitiven Gesundheitsdaten vorgenommen. Es kann daher nicht ausgeschlossen werden, dass Fitness- und Gesundheitsdaten über diese Online-Portale öffentlich gemacht werden. Die Informationspflicht des Art. 17 Abs. 2 DSGVO trifft dann, obwohl die Daten vom Betroffenen selbst übermittelt worden sind, den Plattformbetreiber als verantwortliche Stelle. Die größte Relevanz wird die Informationspflicht voraussichtlich für Big Data-Anwendungen entfalten. Alle öffentlich gemachten Daten können als Basis für Big Data-Anwendungen dienen. Entsprechend hoch kann für den Informationspflichtigen die Anzahl der verantwortlichen und zu benachrichtigenden Stellen sein, die diese Daten für Big Data verwenden. In diesem Kontext wird vermutlich die Aufwandsabschätzung für die Erfüllung der Informationspflicht als maßgebliches Argument angeführt werden, um die Informationspflicht gegenüber Big Data-Verarbeitungen zurückzuweisen. Dann würde die Informationspflicht letztlich für eine besonders riskante Datenverarbeitung nicht greifen, sondern nur für die einfach gelagerten Fälle.

5.2.5 Privacy by Design, Privacy by Default

Als besondere Neuerung wurde auch die Übernahme der Gestaltungskonzepte des „Privacy by Design“ und des „Privacy by Default“ angekündigt.[417] Nach Art. 25 Abs. 1 DSGVO ist der für die Datenverarbeitung Verantwortliche verpflichtet, „sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der

[417] Kritisch zum Kommissionsvorschlag *Hornung*, ZD 2012, 103; *Hornung/Sädtler*, CR 2012, 644; *Richter*, DuD 2012, 578 f.; *Roßnagel/Richter/Nebel*, ZD 2013, 105 f.

eigentlichen Verarbeitung angemessene technische und organisatorische Maßnahmen“ zu treffen, „mit denen die wirksame Umsetzung der Datenschutzgrundsätze wie etwa Datenminimierung und die Aufnahme der notwendigen Garantien in die Verarbeitung erreicht werden sollen, um den Anforderungen dieser Verordnung zu genügen und die Rechte der betroffenen Personen zu schützen“. Als Beispiel für solche Maßnahmen nennt die Vorschrift Pseudonymisierung. Datenminimierung wird zu Recht als Ziel zur Gestaltung von Datenverarbeitungsverfahren verstanden und Pseudonymisierung als ein Mittel dazu. Insofern unterscheidet sich Datenminimierung vom Erforderlichkeitsprinzip in Art. 5 Abs. 1 lit. c) DSGVO und entspricht dem Konzept der „Datenvermeidung und Datensparsamkeit“ in § 3a BDSG.[418] Diese Pflicht steht unter dem Vorbehalt der „Berücksichtigung des Stands der Technik und der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die persönlichen Rechte und Freiheiten“.

Art. 25 Abs. 2 Satz 1 DSGVO fordert datenschutzfreundliche „Voreinstellungen“. Sie sollen sicherstellen, dass „durch Voreinstellung grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden“. Auch hat er geeignete technische und organisatorische Maßnahmen zu treffen, die das Gleiche „für den Umfang der erhobenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit“ sicherstellen. „Solche Maßnahmen müssen insbesondere sicherstellen, dass personenbezogene Daten grundsätzlich nicht ohne Eingreifen einer natürlichen Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden.“ Durch diese Anforderung soll der Betroffene in der Lage sein, den Kreis der Empfänger gezielt steuern zu können.

---

418 *Roßnagel* 2011, 42.

Diese beiden Gestaltungsanforderungen stellen einen Fortschritt in dem Bemühen dar, Datenschutz durch Technikgestaltung zu erreichen. Kritisch anzumerken ist, dass sich beide Anforderungen nur an die für die Verarbeitung Verantwortlichen und nicht an die Hersteller von Datenverarbeitungstechnik richten. Datenschutz durch Technik wird aber vielfach misslingen, wenn nicht auch die Hersteller zu „Privacy by Design" verpflichtet werden. Sie entscheiden, wie datenschutzfreundlich die Technik sein kann. Die für die Verarbeitung Verantwortlichen können nur im Rahmen der von den Herstellern zur Verfügung gestellten Technik handeln. Dagegen richten sich die Datenschutzanforderungen etwa des Art. 6 der eCall-Verordnung 2015/758[419] ausdrücklich an die Hersteller der Autos, in denen eCall verfügbar sein muss. Sie müssen die Datenschutzanforderungen gewährleisten. Ihre Einhaltung wird in der Zulassung der Automobile überprüft.

Zu kritisieren ist auch, dass die Verpflichtung zum „Privacy by Design" durch die Risikoabwägungsklauseln und den Vorbehalt des Stands der Technik und der Implementierungskosten in die Abwägungshoheit des Verantwortlichen gestellt wird und damit seine Erfüllung praktisch nicht kontrollierbar und sanktionierbar ist. Das Gleiche gilt weitgehend auch für die Verpflichtung des „Privacy by Default", weil der Verantwortliche nicht die datenschutzfreundlichste Einstellung vorzusehen hat, sondern nur diejenige, die solche Daten liefert, die für den von ihm bestimmten Verarbeitungszweck erforderlich sind. Ist für seinen Zweck die umfassende Erhebung aller erreichbaren Daten erforderlich, darf sich die Voreinstellung auf die Erfassung aller personenbezogenen Daten erstrecken.

„Privacy by Design" und „Privacy by Default" sind entsprechend ihrer Ausgestaltung in Art. 25 Abs. 1 und 2 DSGVO für die spezifischen Anwendungsfelder Smart Car, Smart Home, Smart Health sowie Big Data praktisch kaum relevant, weil sie sich an die falschen Adressaten richten, viel zu abstrakt, der Einschätzung des für die Datenverarbei-

[419] ABl. L 123 vom 19.5.2015, 77.

tung Verantwortlichen überlassen und mit weitreichenden Ausnahmen versehen sind.

5.3 Defizite der allgemeinen Vorschriften

Die Verordnung erreicht keines der selbstgesteckten Ziele. Sie bewirkt weder eine Modernisierung des Datenschutzrechts noch führt sie zu dessen solider, kohärenter Vereinheitlichung und erreicht daher auch keine einheitlichen Wettbewerbsbedingungen im Binnenmarkt. Die Verordnung führt – von wenigen Ausnahmen abgesehen – grundsätzlich die Konzeptionen der Datenschutzrichtlinie weiter. Die Verordnung wird daher auch den künftigen Herausforderungen der technischen Entwicklung nicht gerecht und versucht sie nicht einmal zu adressieren. Einzelne Verbesserungen stehen vielen Verschlechterungen des Datenschutzes gegenüber. Unterm Strich führt die Verordnung für die Bundesrepublik Deutschland zu einer Absenkung des Datenschutzes, die insbesondere deshalb nicht so gravierend ausfällt, weil die Verordnung nicht zu einem einheitlichen unionsweiten Datenschutzrecht führt. Sie belässt nämlich in vielen Fragen den Mitgliedstaaten Entscheidungsspielräume, das bestehende Datenschutzrecht beizubehalten oder neue – bessere oder präzisere – Regelungen zu erlassen. Das aber verhindert, dass auch das zweite Ziel, ein unionsweit einheitliches Datenschutzrecht, erreicht wurde.

Das Hauptproblem der Datenschutz-Grundverordnung liegt vor allem in der hohen Diskrepanz zwischen der enormen Komplexität des Regelungsbedarfs einerseits und der Abstraktheit und damit Unterkomplexität ihrer Vorschriften andererseits. Sie will in 50 Artikeln des materiellen Datenschutzes die gleichen Probleme behandeln, für die im deutschen Datenschutzrecht Tausende von Vorschriften bestehen. Wird unterstellt, dass die vielen Spezialregelungen des deutschen Datenschutzrechts nicht alle einer Verkennung der Regelungsprobleme zu verdanken sind, wird deutlich, welche Defizite die Datenschutz-Grundverordnung aufweisen muss. Der Regelungsansatz der Verordnung verkennt die Breite und Komplexität der Aufgabe. Datenschutz

ist zu einem zentralen Querschnittsthema der Informationsgesellschaft in Europa geworden. Kein Gesellschaftsbereich kann heute ohne die automatisierte Verarbeitung personenbezogener Daten auskommen. Alle Verfahrensabläufe in Verwaltung und Wirtschaft, Wissenschaft und Kultur sind durch sie geprägt. Wer Datenschutz regelt, verursacht Veränderungen in allen Gesellschaftsbereichen – vom Archivwesen bis zum Zeitungsverlag. Wer meint, die vielen und vielfältigen gesetzlichen Regelungen zum Datenschutz in den Mitgliedstaaten durch wenige generelle und abstrakte Regelungen ersetzen zu können, unterschätzt nicht nur diese Aufgabe gewaltig, sondern übersieht auch die negativen Auswirkungen, die dadurch entstehen, dass er die Vielfalt und Differenzierung bestehender Regelungen beseitigt und gewaltige Lücken der Rechtsunsicherheit schafft.

Inhaltlich verursacht die Verordnung Defizite und verfehlt ihr Modernisierungsziel vor allem durch ihren spezifischen Ansatz der Technikneutralität.[420] Dieser Ansatz ist sinnvoll, wenn er bewirken soll, dass rechtliche Vorschriften so formuliert werden, dass sie technische Weiterentwicklungen nicht ausschließen. In der Datenschutz-Grundverordnung wird dieser Ansatz aber im Sinn einer Risikoneutralität genutzt: In keiner Regelung werden die spezifischen Grundrechtsrisiken zum Beispiel von smarten Informationstechniken im Alltag, von Big Data, Cloud Computing oder datengetriebenen Geschäftsmodellen angesprochen oder gar gelöst. Die gleichen Regelungen wie für die Datenverarbeitung „beim Bäcker um die Ecke" sollen auch für diese risikoreichen Datenverarbeitungsformen gelten. Durch solche Regelungen werden gerade die spezifischen Grundrechtsrisiken verfehlt. Nur durch die Berücksichtigung typischer Risiken bestimmter Datenverarbeitungsformen im Verordnungstext hätte die notwendige Rechtssicherheit und Interessengerechtigkeit erreicht werden können. Dass dies im Unionsrecht möglich ist, zeigt Art. 6 der eCall-Verordnung (EU) 2015/758.

---

420 S. zu diesem grundsätzlich kritisch *Roßnagel* 2009, 323.

Ihr Ziel eines soliden, kohärenten, einheitlichen Rechtsrahmens für den Datenschutz in der gesamten Union verfehlt die Verordnung durch eine Reihe von Gründen. Zwar gilt der Text der Datenschutz-Grundverordnung nach Art. 288 Abs. 2 Satz 1 AEUV in allen Mitgliedstaaten unmittelbar.[421] Die Verordnung wird mit ihrem Inkrafttreten Teil der Rechtsordnung eines jeden Mitgliedstaats und gilt für alle Personen und Organisationen in allen Mitgliedstaaten. Diese Wirkung wird jedoch durch allgemeine Rechtsgrundsätze und durch viele Ausnahmeregelungen in der Verordnung erheblich eingeschränkt.

Die Europäische Union hat keine Kompetenz, deutsche Gesetze zu verändern oder außer Kraft zu setzen. Eine Unionsverordnung hat daher keinen Geltungsvorrang.[422] Daher gelten auch nach ihrem Erlass die deutschen Datenschutzregelungen unverändert weiter. Dieses Nebeneinander kann dazu führen, dass sich Regelungen widersprechen und sich die Frage stellt, welche Regelung anwendbar ist. In einem solchen Konflikt genießt die Unionsverordnung Anwendungsvorrang.[423] Sie ist von den nationalen Behörden und Gerichten anzuwenden. Die konfligierende – weiterhin geltende – deutsche Vorschrift darf in diesem konkreten Konfliktfall nicht angewendet werden – gleichgültig, ob sie früher oder später als die Unionsnorm ergangen ist.[424]

---

421 *EuGH*, Rs. 6/64, Costa/ENEL, Slg. 1964, 1251, Ls 3; *EuGH*, Rs. 106/77, Simmenthal II, Slg. 1978, 629, Rn. 17/18; s. näher *Schroeder,* in: Streinz 2012, Art. 288 AEUV, Rn. 56; *Geismann*, in: von der Groeben/Schwarze/Hatje 2015, Art. 288 AEUV, Rn. 34; *Biervert,* in: Schwarze 2012, Art. 288 AEUV, Rn. 20.

422 S. *BVerfGE* 73, 339 (375); 123, 267 (398); 126, 286 (301f.); *Ehlers,* in: Schulze/Zuleeg/Kadelbach 2015, § 11 Rn. 48.

423 *EuGH*, Rs. 6/64, Costa/ENEL, Slg. 1964, 1251, Ls 3 = NJW 1964, 2371; *EuGH*, Rs. 11/70, Internationale Handelsgesellschaft, Slg. 1970, 1125, Rn. 3 = NJW 1971, 343f.; *EuGH*, Rs. 106/77, Simmenthal II, Slg. 1978, 629, Rn. 17f.; *EuGH, Rs. 94/77,* Zerbone, Slg. 1978, 99, Rn. 22, 27; BVerfGE 31, 145 (173 ff.); 73, 223 (244); *Schroeder*, in: Streinz 2012, Art. 288 AEUV, Rn. 40; *Geismann,* in: von der Groeben/Schwarze/Hatje 2015,Art. 288 AEUV, Rn. 37; *Biervert,* in: Schwarze 2012, Art. 288 AEUV, Rn. 22.

424 *EuGH*, Rs. 106/77, Simmenthal II, Slg. 1978, 629, Rn. 17/18.

Trotz des grundsätzlichen Anwendungsvorrangs einer Unionsverordnung können aber mitgliedstaatliche Regelungen aus drei Gründen weiterhin anwendbar sein:

Erstens ist ihre Anwendbarkeit nur insoweit eingeschränkt, als sie den Regelungen der Unionsverordnung widersprechen. Soweit kein Widerspruch vorliegt, sondern nur eine Präzisierung unbestimmter Rechtsbegriffe, eine Konkretisierung ausfüllungsbedürftiger Vorgaben, die Ergänzung unvollständiger Regelungen oder die Schließung von Regelungslücken, ohne das Regelungsziel der Verordnung zu verletzten, kann die mitgliedstaatliche Regelung weiter anwendbar bleiben, auch wenn ihr Wortlaut sich von dem der Verordnung unterscheidet. Ob ein solcher Widerspruch besteht, ist für die Anwendung einer bestimmten Vorschrift der Unionsverordnung im Einzelfall zu prüfen. Ein schlichter Unterschied im Wortlaut reicht für die Feststellung eines solchen Widerspruchs nicht aus. Beispielsweise kann der Betroffene nach Art. 15 Abs. 1 lit. h) DSGVO Auskunft über die „verwendete Logik" der automatisierten Entscheidungsfindung verlangen. Nach § 34 Abs. 2 und 4 BDSG kann der Betroffene unter anderem Auskunft über die Berechnung und das Zustandekommen von Wahrscheinlichkeitswerten fordern. Diese Regelung ist nicht mit Art. 15 Abs. 1 lit. h) DSGVO identisch, kann aber als Präzisierung der „verwendeten Logik" verstanden werden.

Zweitens kann die mitgliedstaatliche Regelung weiter anwendbar sein, wenn die Verordnung explizite oder implizite Spielräume für nationale Regelungen lässt. So können zum Beispiel die Mitgliedstaaten nach Art. 6 Abs. 3 DSGVO die beiden Erlaubnistatbestände der Erfüllung einer rechtlichen Verpflichtung nach Art. 6 Abs. 1 lit. c) DSGVO und der Wahrnehmung einer öffentlichen Aufgabe oder der Ausübung hoheitlicher Gewalt nach Art. 6 Abs. 1 lit. e) DSGVO ausgestalten. Sie können dabei den Zweck der Datenverarbeitung sowie Verarbeitungsbedingungen, Arten von Daten, betroffene Personen, Weitergabe von Daten, Speicherfristen sowie die Verarbeitungsvorgänge und -verfahren näher regeln.

Drittens kann eine von der Verordnung abweichende mitgliedstaatliche Regelung weiter angewendet werden, wenn sie einen impliziten Spielraum der Verordnung ausfüllt. Vollendet erst die mitgliedstaatliche Regelung eine unvollständige Vorschrift der Verordnung in der erforderlichen Bestimmtheit, ermöglicht sie erst den Vollzug der Verordnung durch die nationalen Behörden oder Gerichte, unterstützt sie die Umsetzung der Verordnung durch einen im nationalen Recht notwendigen Rechtsrahmen oder passt sie die Vorschrift der Verordnung in die Systematik und den Sprachgebrauch des nationalen Rechts ein, dann besteht kein Widerspruch zur Unionsverordnung, der ihren Anwendungsvorrang aktiviert und die Nichtanwendbarkeit der nationalen Regelung zur Folge hat. Dies gilt etwa für die Ergänzung des Schutzes von Profiling in Art. 22 DSGVO. Die automatisierte Generierung von Einzelentscheidungen ist nur zulässig, wenn der Mitgliedstaat „geeignete Maßnahmen zur Wahrung der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person“ geregelt hat.

Selbst soweit die Datenschutz-Grundverordnung anwendbar ist, führt dies nicht immer zu einem unionsweit einheitlichen Datenschutzrecht. Gerade die vielen abstrakten und unbestimmten Regelungen der Verordnung bedürfen in der Praxis der Konkretisierung durch die nationalen Aufsichtsbehörden und Gerichte. So wird etwa der wichtige Erlaubnistatbestand der Interessenabwägung in Art. 6 Abs. 1 lit. f) DSGVO nach der jeweiligen nationalen Datenschutzkultur konkretisiert und daher in der Praxis von Mitgliedstaat zu Mitgliedstaat unterschiedlich sein. Zum Beispiel wird sich die Abwägung für die Videoüberwachung in Großbritannien an der bisher sehr großzügigen Praxis dort orientieren, in Deutschland dagegen an der viel restriktiveren Abwägung, die § 6b BDSG zugrunde liegt. Entsprechend wird man sich in Deutschland etwa für die Interessenabwägung für Werbung an § 28 Abs. 3 BDSG, für Auskunfteien an § 28a BDSG, für Scoring an § 28b BDSG und für Marktforschung an § 30a BDSG und für Internetangebote an §§ 14 und 15 TMG ausrichten. Europäischer Daten-

schutz wird hinsichtlich der Zulässigkeit der Datenverarbeitung in jedem Mitgliedstaat praktisch einen anderen Inhalt haben. Dadurch entsteht kein einheitlich durchgesetztes und gelebtes Recht. Wettbewerbsgleichheit ist so nicht zu erreichen.

Indem die Verordnung die Entscheidung über die Abwägung letztlich auf die Gerichte überträgt, entstehen aber noch viel unterschiedlichere Ergebnissen als unter der Datenschutzrichtlinie. Bisher waren die typisierten vom Gesetzgeber vorgenommenen Interessenabwägungen wenigsten für die Bundesrepublik Deutschland einheitlich. Jetzt wird es möglich sein, dass sie für lange Zeit von Gerichtsbezirk zu Gerichtsbezirk unterschiedlich ausfallen. Erst wenn die obersten Gerichte (in den jeweiligen Einzelfällen) für Rechtsklarheit sorgen, wie einzelne Interessenabwägungen vorzunehmen sind, besteht für diese Rechtssicherheit. Dies kann gerade bei datenschutzrechtlichen Fragen besonders lange dauern, da sie sich häufig „nur" um ein ideelles Interesse drehen, nicht aber um finanzielle Forderungen.

Zwar haben für die Anwendung der unbestimmten Rechtsbegriffe die Aufsichtsbehörden des Bundes, der Länder und aller Mitgliedstaaten einen bestimmenden Einfluss. Um diesen unionsweit zu vereinheitlichen, gibt es umständliche Koordinationsmechanismen. Da aber die Beschlüsse nach Art. 65 DSGVO nur die Aufsichtsbehörden verpflichten und kein allgemeinverbindliches (Exekutiv-)Recht setzen, unterliegen die divergierenden oder vereinheitlichten Interpretationsversuche der Verordnung durch die Aufsichtsbehörden der Überprüfung durch die örtlichen Gerichte. Diese können jeden vereinheitlichten Interpretationsversuch durch den Datenschutzausschuss konterkarieren. Eine Vereinheitlichung der Rechtsprechung ist allenfalls in einzelnen Fällen bezogen auf die jeweils enge Fallfrage nach jahrelangen Prozessen[425] durch den Europäischen Gerichtshof zu erwarten.

---

[425] Das Urteil zur Vorratsdatenspeicherung vom 8.4.2014 erfolgte über acht Jahre nach Erlass der Richtlinie zur Vorratsdatenspeicherung, das Urteil zu Safe Harbor vom 6.10.2015 erging über 15 Jahre nach der Entscheidung der Kommission zur Anerkennung des Safe-Harbor-Systems.

Zusammenfassend kann festgehalten werden: Aufgrund der Unterkomplexität der Unionsregelungen sind mitgliedstaatliche Präzisierungen, Ausfüllungen und Ergänzungen notwendig, um die Verordnung für die faktischen Probleme, die es zu bewältigen gilt, anwendbar zu machen. In der Folge ist die Datenschutz-Grundverordnung kein homogenes, in sich geschlossenes Gesetzeswerk für den Datenschutz in der Union, sondern gleicht eher einem „Schweizer Käse“, der zwar einige strukturierende Elemente aufweist, vor allem aber durch die Löcher dazwischen auffällt. Anders als bei einem Schweizer Käse, werden diese Löcher aber unterschiedlich gefüllt werden. In der Folge wird kein einheitliches Datenschutzrecht in allen Mitgliedstaaten zur Anwendung kommen. Vielmehr werden vergleichbar viele Unterschiede wie zuvor unter der Datenschutzrichtlinie bestehen – nur an anderen Stellen und mit erheblicher Rechtsunsicherheit.

5.4 Verbesserungsvorschläge für allgemeine Regelungen

Ihre Ziele der Vereinheitlichung und Modernisierung des Datenschutzrechts sowie der Vereinheitlichung der Wettbewerbsbedingungen werden nur zu erreichen sein, wenn der Unionsgesetzgeber seine Fixierung auf Risikoneutralität aufgibt und risikoorientierte Regelungen für die jeweils spezifischen Herausforderungen der modernen Technikanwendungen trifft. Auch für risikoorientierte Regelungen kann vermieden werden, dass sie so technikspezifisch sind, dass eine weitere technische Fortentwicklung ausgeschlossen ist. Es genügt, Datenschutzfunktionen festzulegen, die vom dem für die Datenverarbeitung Verantwortlichen oder dem Hersteller zu erfüllen sind. Ein gutes Beispiel für eine europäische risikoorientierte und nicht technikfixierte Regelung ist Art. 6 der eCall-Verordnung (EU) 2015/758.

„Smarte“ Informationstechniken im Alltag verursachen vor allem dadurch Risiken für Grundrechte, dass sie angesichts der im Hintergrund ablaufenden Verarbeitung von Daten alltägliche Lebensvollzüge mit hoher Aussagekraft umfassend erfassen. Dadurch verlieren die Datenschutzgrundsätze der Transparenz, der Einwilligung, der

Zweckbindung, der Erforderlichkeit, der Datenminimierung und der Betroffenenrechte ihre Eignung, die informationelle Selbstbestimmung zu schützen. Risikoadäquate Regelungen zu diesen Risiken können für Smart Cars, für Smart Home und für Smart Health die genannten Datenschutzfunktionen[426] regeln, die den jeweils spezifischen Risiken gerecht werden. Diese fehlen in der Datenschutz-Grundverordnung. Durch die Aufgabe des ausdrücklichen Opt-in bei der Einwilligung, die Aufweichung der Zweckbindung und die Stärkung des Erlaubnistatbestands der Interessenabwägung werden viele Anwendungen des Ubiquitous Computing durch die Datenschutz-Grundverordnung erleichtert, ohne dass risikoadäquate Schutzmaßnahmen bestehen. Die Datenschutz-Grundverordnung sollte daher um solche risikospezifischen Schutzregelungen[427] ergänzt werden.

Big Data verursacht vor allem dadurch Risiken für Grundrechte, dass sehr viele personenbezogene Daten, die für andere Zwecke erhoben wurden, zweckentfremdet genutzt werden, um über Betroffene mehr zu erfahren und dieses Wissen für eigene Zwecke zu nutzen. Darüber hinaus kann statistisches Wissen auch auf die Betroffenen angewendet werden, die einer Datenerhebung oder Zweckänderung nicht zugestimmt haben. Auch für Big Daten-Analysis sollten spezifische Regelungen getroffen werden, die die speziellen Risiken von Big Data-Anwendungen adressieren.[428]

5.5 Europäische Richtlinie für Justiz und Inneres

Parallel zur Datenschutzgrundverordnung wurde die Richtlinie für Justiz und Inneres (JI-RL)[429] erlassen. Sie ersetzt den Rahmenbeschluss

---

426 S. Kap. 4.2.1 bis 4.2.3.

427 S. zu diesen Kap. 4.2.1 bis 4.2.3.

428 S. Kap. 4.2.4.

429 Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates, EU ABl. L 119 vom 4.5.2016, 89.

2008/ 977/JI[430] und weitet den Anwendungsbereich des europäischen Datenschutzrechts gegenüber diesem aus. Anders als die Datenschutz-Grundverordnung muss die Richtlinie von den Mitgliedstaaten umgesetzt werden, um innerstaatlich anwendbar zu sein. Der Umsetzungsbedarf erstreckt sich auf eine breite Palette von datenschutzrechtlichen Bestimmungen in zahlreichen Gesetzen, insbesondere den Polizeigesetzen des Bundes und der Länder sowie der Strafprozessordnung. Gemäß Art. 1 Abs. 3 JI-RL können die Mitgliedstaaten aber strengere Datenschutzvorschriften einführen oder beibehalten. Es handelt sich also ausdrücklich um eine Mindestharmonisierung.

Der Rahmenbeschluss war in seiner Anwendung auf die Verarbeitung personenbezogener Daten bei der grenzüberschreitenden polizeilichen und justiziellen Zusammenarbeit beschränkt. Die Richtlinie erfasst dagegen auch die innerstaatliche Datenverarbeitung. Sie normiert gemäß Art. 3 Nr. 7 JI-RL insbesondere die Datenverarbeitung zur Aufgabenerfüllung durch die Strafverfolgungs- und Gefahrenabwehrbehörden. Sie regelt den Datenschutz bei der Datenverarbeitung durch die Sicherheitsbehörden in der Breite und systematisch, indem sie grundlegende Regeln für die Rechtmäßigkeit von Datenverarbeitungen in Art. 4 und 8 JI-RL enthält. Besondere Kategorien personenbezogener Daten werden in Art. 9 JI-RL adressiert. Betroffenenrechte werden in Art. 12 ff. JI-RL ausführlich geregelt. Besondere Pflichten der Datenverarbeiter, zum Beispiel zum technischen Datenschutz finden sich in Art. 19 ff. JI-RL. Da der Bereich von Strafverfolgung und Gefahrenabwehr in Deutschland auch bisher schon über ein vergleichbares Datenschutzkonzept verfügt, ist nicht zu erwarten, dass die Umsetzung der Richtlinie zu grundlegenden Umwälzungen führen wird. Herauszuarbeiten, in welchen Bereichen Anpassungen notwendig sein werden, dürfte dennoch einen erheblichen Arbeitsaufwand bedeuten.

---

[430] Rahmenbeschluss 2008/977/JI des Rates vom 27. November 2008 über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden, EU ABl. L 350 vom 30.12.2008, 60.

Auch die Richtlinie sieht kaum spezifische Regelungen im Hinblick auf Smart Car, Smart Home, Smart Health und Big Data vor. Lediglich die automatisierte Einzelentscheidung wird auch für den Sicherheitsbereich in Art. 11 JI-RL ausdrücklich geregelt. Sie soll nach derzeitigem Stand verboten sein, es sei denn, sie wird durch das Recht eines Mitgliedstaats mit ausreichenden Maßnahmen zur Sicherung der Rechte der Betroffenen erlaubt.

6 Zusammenfassung

„Smarte“ Informationstechniken im Alltag ermöglichen Erleichterungen und Unterstützungen durch Delegation von unerwünschten Aufgaben an Technik, kontextbezogene Assistenz und Ergänzung unserer körperlichen und geistigen Fähigkeiten. Big Data-Anwendungen ermöglichen neue Erkenntnisse, die für die Lösung von Problemen in vielen unterschiedlichen Gesellschafts- und Wirtschaftsbereichen genutzt werden können.

Diese Technikanwendungen ermöglichen – vor allem in ihrer Kombination – aber auch eine umfassende Überwachung und Rekonstruktion vieler oder gar aller Ereignisse im Leben eines Menschen. Dies gilt sowohl für die Datenerhebung und -verarbeitung durch staatliche Stellen wie auch durch viele große und kleine Unternehmen, die Informationstechnikanwendungen anbieten. Ob wir mit diesen Technikanwendungen besser leben als ohne sie, ist letztlich eine Frage des Datenschutzes.

Auf das bestehende Datenschutzrecht kann nur begrenzt vertraut werden, weil die beschriebenen Entwicklungen vielfach dessen gegenwärtiges Schutzprogramm leer laufen lassen. Bedingung für die künftige Verwirklichung informationeller Selbstbestimmung ist ein modifiziertes und ergänztes Schutzprogramm, in dem die Konzepte und Instrumente des Datenschutzes den spezifischen Risiken der Technikanwendungen angepasst sind. Notwendig ist eine objektivierte Ordnung der Datenverarbeitung und -kommunikation bei professioneller Kontrolle, mit vorsorgender Gestaltung von Strukturen und Systemen, der Inpflichtnahme von Herstellern zur Umsetzung von Datenschutz in Technik sowie der Nutzung von Eigennutz durch Anreize zu datenschutzgerechtem Handeln. Diese Bedingung ist eine notwendige, aber keine hinreichende. Hinzukommen müssen bei den Individuen das Bewusstsein, dass informationelle Selbstbestimmung ein hohes, aber gefährdetes Gut ist, und der Wunsch, es zu bewahren, und in der Ge-

sellschaft die Erkenntnis, dass hierfür Strukturänderungen erforderlich sind, und der politische Wille, sie auch umzusetzen.

Die unvollständige und unterkomplexe Verordnung führt durch ihren nur partiellen Anwendungsvorrang und das Fortgelten des deutschen Datenschutzrechts sowie durch ihre vielen Öffnungsklauseln für den nationalen Gesetzgeber zu einer sehr schwer zu durchschauenden Gemengelage von Unionsrecht und deutschem Recht. Daher muss der deutsche Gesetzgeber das deutsche Datenschutzrecht daraufhin überarbeiten, dass aus der Datenschutz-Grundverordnung und aus dem weiter anwendbaren deutschen Datenschutzrecht sowie aus zusätzlichen Regelungern, die zu erlassen sind, um die Vorschriften der Datenschutz-Grundverordnung zu präzisieren, zu konkretisieren und zu ergänzen, eine kohärente, widerspruchsfreie und vollzugsfähige Gesamtregelung des Datenschutzrechts wird. Diese Aufgabe sollte auch dafür genutzt werden, risikogerechte Regelungen für die neuen Herausforderungen durch „smarte" Informationstechniken im Alltag und Big Data-Analysen zu erlassen.

Hierfür könnten die Regelungsspielräume genutzt werden, die unter anderem Art. 6 Abs. 2 DSGVO für alle nationalen Erlaubnistatbestände gewährt, die die Erfüllung einer rechtlichen Verpflichtung zur Datenverarbeitung (Art. 6 Abs. 1 lit. c) DSGVO), die Wahrnehmung einer öffentlichen Aufgabe und die Ausübung hoheitlicher Gewalt (Art. 6 Abs. 1 lit. e) DSGVO) betreffen. Genutzt werden könnten etwa auch die Regelungsspielräume in Art. 9 Abs. 2 und 4 DSGVO (Ausnahmen vom Verbot der Verarbeitung sensitiver Daten, Verarbeitung von Gesundheits- und genetischen Daten), Art. 22 Abs. 2 DSGVO (Ausnahmen vom Verbot automatisierter Generierung von Einzelentscheidungen), Art. 88 DSGVO (Datenverarbeitung im Beschäftigungskontext) und Art. 89 DSGVO (Datenverarbeitung für wissenschaftliche, statistische oder historische Zwecke). Soweit die Datenschutz-Grundverordnung keinen Ansatzpunkt für eine risikogerechte Regelung neuer Grundrechtsrisiken bietet, muss mit ihrem Inkrafttreten die Diskussion über ihre geeignete Fortentwicklung beginnen.

Literatur

ADM/ASI/BVM/DGOF: Erklärung für das Gebiet der Bundesrepublik Deutschland zum ICC/ESOMAR Internationalen Kodex für die Markt- und Sozialforschung, 2008.

Art. 29-Datenschutzgruppe: Auswirkungen der eCall-Initiative auf den Datenschutz und die Privatsphäre, Working Paper 125 vom 26.9.2006.

Art. 29-Datenschutzgruppe: Opinion 03/2013 on purpose limitation, Working Paper 203, 2013.

Atzert, M. / Franck, L.: Zulässigkeit und Verwertbarkeit von Videoaufzeichnungen durch Dashcams, RDV 2014, 136.

Backu, F.: Datenschutzrechtliche Relevanz bei Onlinespielen – Überblick über die einzelnen Problemstellungen ZD 2012, 59.

Balzer, T. / Nugel, M.: Minikameras im Straßenverkehr - Datenschutzrechtliche Grenzen und zivilprozessuale Verwertbarkeit der Videoaufnahmen, NJW 2014, 1622.

Balzer, T. / Nugel, M.: Das Auslesen von Fahrzeugdaten zur Unfallrekonstruktion im Zivilprozess, NJW 2016, 193.

Becker, T.: Zulässigkeit der Auftragsdatenverarbeitung von Patientendaten – auch in der Cloud, in: Taeger, J. (Hrsg.), Law as a Service (LaaS) - Recht im Internet- und Cloud-Zeitalter, DSRITB, Edewecht 2013, 343.

Bender, R. / Kahlen, C.: Neues Telemediengesetz verbessert den Rechtsrahmen für Neue Dienste und Schutz vor Spam-Mails, MMR 2006, 590.

Bergemann, B.: Besorgte Reaktionen auf Leaks zur EU-Datenschutzreform, 9.3.2015, netzpolitik.org, https://netzpolitik.org/2015/besorgte-reaktionen-auf-leaks-zur-eu-datenschutzreform/.

Bergmann, L. / Möhrle, R. / Herb, A.: Datenschutzrecht, Stuttgart 2011.

Bergmann, K. / Pauge, B. /Steinmeyer, H.-D.: Gesamtes Medizinrecht, 2. Aufl., Baden-Baden 2014.

Bizer, J. / Dingel, K. / Fabian, B. / Günther, O. / Hansen, M. / Klafft, M. / Möller, J. / Spiekermann, S.: Technikfolgenabschätzung Ubiquitäres Computing und Informationelle Selbstbestimmung (TAUCIS), Studie im Auftrag des Bundesministeriums für Bildung und Forschung, hrsg. v. Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein u. Institut für Wirtschaftsinformatik der Humboldt-Universität Berlin, Berlin 2006.

Borchers, D.: Precrime: Datenschützer haben keine Einwände gegen Predictive Policing-Software, heise online, 12.2.2015, http://heise.de/-2548388.

Bönninger, J.: Das moderne Auto – Messgerät und Datenspeicher, in: 52. Deutscher Verkehrsgerichtstag, Hamburg 2014, 229.

Bönninger, J.: Mobilität im 21. Jahrhundert: sicher, sauber, datengeschützt, DuD 2015, 388.

Brühann, U.: Mindeststandards oder Vollharmonisierung des Datenschutzes in der EG, EuZW 2009, 639.

Buchner, B.: Datenschutz im vernetzten Automobil, DuD 2015, 372.

Busch, J.-D.: Auswirkungen des Volkszählungsurteils des Bundesverfassungsgerichts, DVBl. 1984, 385.

Christl, W.: Kommerzielle digitale Überwachung im Alltag - Studie im Auftrag der österreichischen Bundesarbeitskammer, Wien 2014.

Deutsch, E.: Das Persönlichkeitsrecht des Patienten, AcP 1992 (192), 161.

Dix, A. (Hrsg.): Datenschutz und Informationsfreiheit, Jahresbericht des Berliner Beauftragten für Datenschutz und Informationsfreiheit 2013, Berlin 2013.

Ehmann, E. / Helfrich, H.: EG-Datenschutzrichtlinie – Kurzkommentar, Köln 1999.

Fuchs, D.: Verwendung privater Kameras im öffentlichen Raum. Datenschutz bei Dash-Cams, Helm-, Wildkameras & Co, ZD 2015, 212.

Geminn, C. L. / Roßnagel, A.: „Privatheit" und „Privatsphäre" aus der Perspektive des Rechts – ein Überblick, JZ 2015, 703.

Geppert, M. / Schütz, R. (Hrsg.): Beck'scher TKG-Kommentar, 4. Aufl., München 2013 (zitiert: Bearbeiter, in: Geppert/Schütz 2013).

Gluba, A.: (LKA Niedersachsen), Predictive Policing – eine Bestandsaufnahme, Historie, theoretische Grundlagen, Anwendungsgebiete und Wirkung, Hannover 2014.

Graf, J.-P. (Hrsg.): Beck'scher Online-Kommentar StPO mit RiStBV und MiStra, München 2015 (zitiert: Bearbeiter, in: Graf 2015).

Grabenwarter, C. (Hrsg.): Europäischer Grundrechtsschutz, Baden-Baden 2014.

Grabitz, E. / Hilf, M. / Nettesheim, M. (Hrsg.): Das Recht der Europäischen Union, Band I EUV/AEUV, Kommentar, Loseblatt, 57. Ergänzungslieferung, München 2015.

Greger, R.: Kamera on board – Zur Zulässigkeit des Video-Beweises im Verkehrsunfallprozess, NVZ 2015, 114.

Greveler, U. / Justus, B. / Löhr, D.: Identifikation von Videoinhalten über granulare Stromverbrauchsdaten, in: Suri, N. / Waidner, M. (Hrsg.), Sicherheit 2012, GI-Edition, Lecture Notes in Informatics, Proceedings 195, Bonn 2012, 35.

Gundermann, L.: Das Datenschutzrecht in Europa kommt in Bewegung, VuR 2011, 74.

von der Groeben, H. / Schwarze, J. / Hatje, A. (Hrsg.): Europäisches Unionsrecht, 4 Bände, 7. Aufl., Baden-Baden 2015.

Hänlein, A. / Kruse, J. / Schuler, R. (Hrsg.): Sozialgesetzbuch V, 4. Aufl., Baden-Baden 2012.

Hannich, R. (Hrsg.): Karlsruher Kommentar zur Strafprozessordnung, München 2013 (zitiert als Bearbeiter, in: Hannich 2013).

Hansen, M.: Das Netz im Auto das Auto im Netz, DuD 2015, 367.

Helbing T.: Big Data und der datenschutzrechtliche Grundsatz der Zweckbindung, K&R 2015, 145.

Heußner, H.: Datenverarbeitung und die Rechtsprechung des Bundesverfassungsgerichts im Spannungsfeld zwischen Recht und Politik, AuR 1985, 309.

Hornung, G.: Die digitale Identität – Rechtsprobleme von Chipkartenausweisen: Digitaler Personalausweis, elektronische Gesundheitskarte, JobCard-Verfahren, Baden-Baden 2005.

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

Hornung, G. / Hofmann, K.: Die Zulässigkeit der Markt- und Meinungsforschung nach Datenschutz- und Wettbewerbsrecht (Teil 1), WRP 2015, 776.

Hornung, G. / Sädtler, S.: Europas Wolken. Die Auswirkungen des Entwurfs für eine Datenschutz-Grundverordnung auf das Cloud Computing, CR 2012, 638.

Horvath, S.: Aktueller Begriff Big Data, Wissenschaftliche Dienste Deutscher Bundestag, Nr. 37/13, 6.11.2013.

Hufen, F.: Das Volkszählungsurteil des Bundesverfassungsgerichts und das Grundrecht auf informationelle Selbstbestimmung – eine juristische Antwort auf „1984"?, JZ 1984, 1072.

ICC/ESOMAR: Internationaler Kodex für die Markt- und Sozialforschung, 2007.

Jandt, S.: Vertrauen im Mobile Commerce – Vorschläge für die rechtsverträgliche Gestaltung von Location Based Services, Baden-Baden 2008.

Jandt, S.: Datenschutz und Datensicherheit im Smart Grid - Rechtliche Anforderungen an Energiedienstleiter, smart.ER - Recht und Steuern der Smart Energy Services, I/2014, 10.

Jandt, S. / Laue, P.: Voraussetzungen und Grenzen der Profilbildung bei Location Based Services, K&R 2006, 316.

Jandt, S. / Nebel, M.: Die elektronische Zukunft der Anwaltstätigkeit, NJW 2013, 1570.

Jandt, S. / Roßnagel, A.: Qualitätssicherung im Krankenhaus – Fragen des Daten- und Geheimnisschutzes, MedR 2011, 140.

Jandt, S. / Roßnagel, A.: Datenschutz in Social Networks, ZD 2011, 160.

Jandt, S. / Roßnagel, A. / Volland, B.: Datenschutz für Smart Meter – Spezifische Neuregelungen im EnWG, ZD 2011, 99.

Jandt, S. / Roßnagel, A. / Wilke, W.: Krankenhausinformationssysteme im Gesundheitskonzern, RDV 2011, 222.

Jandt, S. / Steidle, R.: One Device Fits All? – Ein Endgerät für mehrere Arbeitgeber – Rechtliche Bewertung und Handlungsempfehlungen bei BYID, CR 2013, 338.

Janssen, J.-K.: Big Brother und die Körperdaten – Cloud-Zwang, Datenschutz und Versicherungen: Sind Aktivitätstracker gefährlich?, c't 03/2015, 114.

Kamp, M. / Rost, M.: Kritik an der Einwilligung, DuD 2013, 80.

Keppeler, L. M.: Der US-amerikanische Entwurf des „Security and Privacy in your Car Act" – eine Analyse vor dem Hintergrund der deutschen Connected Car Debatte, RDV 2015, 299.

Kinast, K. / Kühnl, C.: Telematik und Bordelektronik - Erhebung und Nutzung von Daten zum Fahrverhalten, NJW 2014, 3057.

Kingreen. T. / Kühling, J.: Gesundheitsdatenschutzrecht, Baden-Baden 2015.

Knyrim, R. / Trieb, G.: Videokameras in Autos – vom Teufelszeug zum Beweismittel. Vereinbarkeit von Dash-Cams mit datenschutzrechtlichen Grundsätzen, ZD 2014, 547.

Konferenz der Datenschutzbeauftragten: Auswirkungen des Volkszählungsurteils, DÖV 1984, 504.

Krause, P.: Das Recht auf informationelle Selbstbestimmung – BVerfGE 65, 1, JuS 1984, 268.

Krauß, C. / Waidner, M.: IT-Sicherheit und Datenschutz im vernetzten Fahrzeug, DuD 2015, 383.

Kremer, S., Datenschutz bei Entwicklung und Nutzung von Apps für Smart Devices, CR 2012, 438.

Krempel, S.: EU-Datenschutzreform: Zweckbindung und Datensparsamkeit ausgehebelt, 15.6.2015, heise online, http://heise.de/-2690862.

Kroschwald, S.: Kollektive Verantwortung für den Datenschutz in der Cloud, ZD 2013, 388.

Kroschwald, S.: Informationelle Selbstbestimmung auch auf der Straße?, in: Schartner, P. u.a. (Hrsg.), DACH Security 2015, 86.

Kroschwald, S. / Wicker, M.: Zulässigkeit von Cloud Computing für Berufsgeheimnisträger: Strafbarkeit von Anwälten und Ärzten durch die Cloud?, in: Taeger, J. (Hrsg.), Law as a Service (LaaS) - Recht im Internet- und Cloud-Zeitalter, DSRITB, Edewecht 2013, 733.

Langheinrich, M.: Die Privatsphäre im Ubiquitous Computing – Datenschutzaspekte der RFID-Technologie, in: Fleisch, E. / Mattern, F. (Hrsg.), Das Internet der Dinge, Berlin 2005, 329.

Lenaerts, K.: Die EU-Grundrechtecharta: Anwendbarkeit und Auslegung, EuR 2012, 3.

Löwe, E. / Rosenberg, W.: Die Strafprozessordnung und das Gerichtsverfassungsgesetz, Bd. 11: EMRK/IPBPR, hrsg. v. Erb, V. / Esser, R. / Franke, U. / Graalmann-Scheerer, K. / Hilger, H. / Ignor, A., 26. Aufl., Berlin 2012.

Lüdemann, V.: Connected Cars. Das vernetzte Auto nimmt Fahrt auf, der Datenschutz bleibt zurück, ZD 2015, 247.

Lüdemann, V. / Sengstacken, C. / Vogelpohl, K.: Schlaue Schilder – Kommt das intelligente Autokennzeichen? Umfangreiche Einsatzfelder im privaten Bereich, ZD 2015, 55.

Lutz, L. S.: Autonome Fahrzeuge als rechtliche Herausforderung, NJW 2015, 119.

Lutz, L. S. / Tang, T. / Lienkamp, M.: Die rechtliche Situation von teleoperierten und autonomen Fahrzeugen, NZV 2013, 57.

Maier, N. / Ossoinig, V.: Rechtsfragen und praktische Tipps bei der Ortung durch Smartphone-Apps, VuR 2015, 330.

Mangoldt von, H. / Klein, F. / Starck, C.: Kommentar zum Grundgesetz, Bd. 1: Präambel, Artikel 1 bis 19, 6. Aufl., München 2010 (zitiert: Bearbeiter, in: Mangoldt/Klein/Starck Bd. 1, 2010).

Mattern, F.: Ubiquitous Computing: Eine Einführung mit Anmerkungen zu den sozialen und rechtlichen Folgen, in: Taeger, J. / Kliebe, A. (Hrsg.): Mobilität, Telematik, Recht, Köln 2005, 11.

Maurer, M. / Gerdes, J. C. / Lenz, B. / Winner, H. (Hrsg.): Autonomes Fahren – Technische, rechtliche und gesellschaftliche Aspekte, Berlin 2015.

Mayer-Schönberger, V. / Cukier, K.: Big Data – Die Revolution, die unser Leben verändern wird, München 2013.

Meyer, J. (Hrsg.): Charta der Grundrechte der Europäischen Union, Kommentar, 4. Aufl., Baden-Baden 2014.

Meyer-Ladewig, J.: Europäische Menschenrechtskonvention, Handkommentar, 3. Aufl., Baden-Baden 2011.

Mielchen, D.: Verrat durch den eigenen PKW – wie kann man sich schützen?, in: 52. Verkehrsgerichtstag, Köln 2014, 241.

Mielchen, D.: Verrat durch den eigenen PKW – wie kann man sich schützen?, NVZ 2014, 81.

Monroy, M.: LKA-Studie erklärt Für und Wider von „Predictive Policing2 – Auch BKA liebäugelt jetzt mit Vorhersagesoftware, https://netzpolitik.org/2015/lka-studie-erklaert-fuer-und-wider-von-predictive-policing-auch-bka-liebaeugelt-jetzt-mit-vorhersage software/, 9.1.2015.

Mückenberger, U.: Datenschutz als Verfassungsgebot – Das Volkszählungsurteil des Bundesverfassungsgerichtes, KJ 1984, 1.

Münch, von, I . / Kunig, P.: Grundgesetz-Kommentar: GG, Band 1: Präambel bis Art. 69, 6. Aufl., München 2012 (zitiert: Bearbeiter, in: v. Münch/Kunig Bd. 1, 2012).

Nebel, M.: Schutz der Persönlichkeit – Privatheit oder Selbstbestimmung? Verfassungsrechtliche Zielsetzungen im deutschen und europäischen Recht, ZD 2015, 517.

Ochs, C.: BIG DATA – little privacy? Eine soziologische Bestandsaufnahme, in: Richter (Hrsg.), Privatheit, Öffentlichkeit und demokratische Willensbildung in Zeiten von Big Data, Baden-Baden 2015, 169.

Pieroth, B. / Schlink, B. / Kniesel, M.: Polizei- und Ordnungsrecht, 7. Aufl., München 2012.

Pflüger, F.: Haftungsfragen der Telemedizin, VersR 1999, 1070.

Plath, K.-U. u.a. (Hrsg.): BDSG Kommentar, Köln 2013 (zitiert als Bearbeiter, in: Plath 2013).

Pohle, J. / Zoch, B.: eCall = Der gläserne Fahrer?. Datenschutz in Kraftfahrzeugen im Rahmen von eCall und anderen kommunizierenden Bordsystemen, CR 2014, 409.

Raabe, O. / Weis, E.: Datenschutz im „SmartHome", RDV 2014, 231.

Rehmann, W. A. / Wagner, S. A.: Medizinproduktegesetz, Kommentar, 2. Aufl., München 2010 (zitiert, als: Bearbeiter, in Rehmann/Wagner 2010).

Reibach, B.: Private Dashcams & Co. – Household Exemption ade?, DuD 2015, 157.

Reiners, W.: Datenschutz in der Personal Data Economy - Eine Chance für Europa, ZD 2015, 52.

Richter, P.: Datenschutz durch Technik und die Grundverordnung der EU-Kommission, DuD 2012, 576.

Richter, P.: Die Wahl ist geheim… so what? Big Data Mining im US-Wahlkampf. Und hier?, DÖV 2013, 961.

Richter, P.: Datenschutz zwecklos? – Das Prinzip der Zweckbindung im Ratsentwurf der DSGVO, DuD 2015, 735.

Richter, P. (Hrsg.): Privatheit, Öffentlichkeit und demokratische Willensbildung in Zeiten von Big Data, Baden-Baden 2015.

Rieke, A. / Robinson, D. / Yu, H.: Civil Rights, Big Data, and Our Algorithmic Future – A September 2014 report on social justice and technology, https://bigdata.fairness.io/predictive-policing/, 2014.

Rieß, J. / Greß, S.: Privacy by Design für Automobile auf der Datenautobahn, DuD 2015, 402.

Rogall-Grothe, C.: Ein neues Datenschutzrecht für Europa, ZRP 2012, 193.

Roßnagel, A. (Hrsg.): Handbuch Datenschutzrecht, München 2003 (zitiert, als: Bearbeiter, in Roßnagel 2003).

Roßnagel, A.: Datenschutz in der künftigen Verkehrstelematik, NVZ 2006, 281.

Roßnagel, A.: Datenschutz bei der künftigen Kommunikation vom und zum Kraftfahrzeug, in: 44. Deutscher Verkehrsgerichtstag, Hamburg 2006, 142.

Roßnagel, A.: Datenschutz in einem informatisierten Alltag, Berlin 2007.

Roßnagel, A.: Das Telemediengesetz – Neuordnung für Informations- und Kommunikationsdienste, NVwZ 2007, 743.

Roßnagel, A.: Selbst- oder Fremdbestimmung – die Zukunft des Datenschutzes, in: Roßnagel, A. / Sommerlatte, T. / Winand, U. (Hrsg.), Digitale Visionen – Zur Gestaltung allgegenwärtiger Informationstechnologien, Berlin 2008, 123.

Roßnagel, A.: Technikneutrale Regulierung: Möglichkeiten und Grenzen, in: Eifert, M. / Hoffmann-Riem, W. (Hrsg.), Innovationsfördernde Regulierung, Berlin 2009, 323.

Roßnagel, A.: Datenschutzaudit – ein modernes Steuerungsinstrument, in: Hempel, L. / Krasmann, S. / Bröckling, U. (Hrsg.), Sichtbarkeitsregime – Überwachung, Sicherheit und Privatheit im 21. Jahrhundert, Leviathan Sonderheft 2010, 263.

Roßnagel, A.: Die „Überwachungs-Gesamtrechnung" – Das BVerfG und die Vorratsdatenspeicherung, NJW 2010, 1238.

Roßnagel, A.: Modernisierung des Datenschutzes – Nicht die Definition von Personendaten muss geändert werden, sondern die Anforderungen an ihren Schutz, digma 2011, 160.

Roßnagel, A.: Das Gebot der Datenvermeidung und -sparsamkeit als Ansatz wirksamen technikbasierten Persönlichkeitsschutzes?, in: Eifert, M. / Hoffmann-Riem, W. (Hrsg.), Innovation, Recht und öffentliche Kommunikation, Berlin 2011, 41.

Roßnagel, A. (Hrsg.): Recht der Telemediendienste, München 2013 (zitiert als Bearbeiter, in: Roßnagel 2013).

Roßnagel, A.: Big Data - Small Privacy?, ZD 2013, 562.

Roßnagel, A.: Fahrzeugdaten - wer darf über sie entscheiden? Zuordnungen – Ansprüche – Haftung, SVR 2014, 281.

Roßnagel, A.: Neue Maßstäbe für den Datenschutz in Europa. Folgerungen aus dem Urteil des EuGH zur Vorratsdatenspeicherung, MMR 2014, 372.

Roßnagel, A.: Grundlegende Rechtsverhältnisse und Ansprüche, in: 52. Verkehrsgerichtstag, Köln 2014 (a), 259.

Roßnagel, A.: Regulierung – was leistet unser Datenschutzrecht (nicht)? in: Hill, H. (Hrsg.), E-Transformation. Veränderung der Verwaltung durch digitale Medien, Baden-Baden 2014 (b), 78.

Roßnagel, A.: Datenschutzfragen des Cloud Computing, in: Roßnagel, A. (Hrsg.), Wolken über dem Rechtsstaat? Recht und Technik des Cloud Computing in Verwaltung und Wirtschaft, Baden-Baden 2015, 21.

Roßnagel, A.: Das vernetzte Automobil – sichere und freie Mobilität, DuD 2015, 345.

Roßnagel, A.: Schriftliche Stellungnahme zur Sachverständigenanhörung am 30. November 2015 zum Entwurf eines Zweiten Gesetzes zur Änderung des Bundesdatenschutzgesetzes – Verbesserung der Transparenz und der Bedingungen beim Scoring (Scoringänderungsgesetz), Kassel 24.11.2015.

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

Roßnagel, A.: Die neue Vorratsdatenspeicherung. Der nächste Schritt im Ringen um Sicherheit und Grundrechtsschutz, NJW 2016, 533.

Roßnagel, A. / Jandt, S. / Müller, J. /Gutscher, A. /Heesen, J.: Datenschutzfragen mobiler kontextbezogener Systeme, Wiesbaden 2006.

Roßnagel, A. / Moser-Knierim, A. / Schweda, S.: Interessenausgleich bei der Vorratsdatenspeicherung, Baden-Baden 2013.

Roßnagel, A. / Pfitzmann, A. / Garstka, H.-J.: Modernisierung des Datenschutzrechts, Berlin 2001.

Roßnagel, A. / Richter, P. / Nebel, M.: Besserer Internetdatenschutz für Europa – Vorschläge zur Spezifizierung der DS-GVO, ZD 2013, 103.

Roßnagel, A. / Scholz, P.: Datenschutz durch Anonymität und Pseudonymität, Rechtsfolgen der Verwendung anonymer und pseudonymer Daten, MMR 2000, 721.

Schaffland, H.-J. / Wiltfang, N.: Bundesdatenschutzgesetz, Loseblatt: Stand Oktober 2015, Berlin.

Schaub, G. (Begr.) Arbeitsrechtshandbuch, München 2015 (zitiert als Bearbeiter, in. Schaub 2015).

Scherer, J.: eCall: Ein Lehrstück für Politik, Regulierung und Datenschutz, MMR 2014, 353.

Schlink, B.: Das Recht auf informationelle Selbstbestimmung, Der Staat 25 (1986), 233.

Schönke, A. / Schröder, H.: Strafgesetzbuch – Kommentar, 29. Aufl., München 2014.

Scholz, P.: Datenschutz beim Internet-Einkauf: Gefährdungen – Anforderungen – Gestaltungen, Baden-Baden 2003.

Schulz, S. / Hoffmann, C.: Staatliche Datenerhebung in sozialen Netzwerken, DuD 2012, 7.

Schulz, T. / Roßnagel, A. / David: K.: Datenschutz bei kommunizierenden Assistenzsystemen. Wird die informationelle Selbstbestimmung von der Technik überrollt?, ZD 2012, 510.

Schulzki-Haddouti, C.: Die EU wurschtelt sich zur Großreform, Zeit Online, 12.3.1015, http://www.zeit.de/digital/datenschutz/2015-03/datenschutzverordnung-zweckbindung-datensparsamkeit.

Schulze, R. / Zuleeg, M. / Kadelbach, S. (Hrsg.): Europarecht, 3. Aufl., Baden-Baden 2015.

Schwarz, M.: Die Menschenwürde als Ende der Europäischen Wertegemeinschaft?, Der Staat 2011, 533.

Schwarze, J. (Hrsg.), EU-Kommentar, 3. Aufl., Baden-Baden 2012.

Schwichtenberg, S.: „Pay as you drive" – neue und altbekannte Probleme, DuD 2015, 378.

Seiler, D.: Auftragsdatenverarbeitung im Gesundheitswesen im Spannungsfeld mit dem Berufsgeheimnis, in: Taeger, J. (Hrsg.), Internet der Dinge, DSRITB 2015, Edewecht 2015, 69.

Simitis, S.: Die informationelle Selbstbestimmung – Grundbedingung einer verfassungskonformen Informationsordnung, NJW 1984, 398.

Simitis, S. (Hrsg.): Bundesdatenschutzgesetz Kommentar, 8. Aufl., Baden-Baden 2014 (zitiert als Bearbeiter, in: Simitis 2014).

Skistims, H.: Smart Homes – Rechtsprobleme intelligenter Haussysteme unter besonderer Beachtung des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme, Baden-Baden 2016.

Spindler, G.: Verbandsklagen und Datenschutz – das neue Verbandsklagerecht, ZD 2016, 114.

Spindler, G. / Schuster, F.: Recht der elektronischen Medien, München 2015 (zitiert als Bearbeiter, in: Spindler/Schuster 2015).

Spyra, G.: Der Schutz von Daten bei vernetzten (Software-)Medizinprodukten aus Herstellersicht, MPR 2015, 15.

Steinebach, M. /Halvani, O. / Schäfer, M. / Winter, C. / Yannikos, Y.: Big Data und Privatheit, Darmstadt 2014.

Steinmüller, W.: Das Volkszählungsurteil des Bundesverfassungsgerichts, DuD 1984, 91.

Streinz, R. (Hrsg.): EUV/AEUV, 2. Aufl., München 2012.

Störing, M.: Spion am Handgelenk – Kommerzieller Wearables-Einsatz und Datenschutz, c't 03/2015, 132.

Theile, M.: Liken, posten und wählen, Die ZEIT, 8.8.2013, 8.

Thiel, M.: Polizei- und Ordnungsrecht, 2. Aufl., Baden-Baden 2014.

Taeger, J. / Gabel, D. (Hrsg.): Bundesdatenschutzgesetz und Datenschutzvorschriften des TKG und TMG, Frankfurt a. M. 2013 (zitiert als: Bearbeiter, in: *Taeger/Gabel* 2013).

Ulsenheimer, K. / Heinemann, N.: Rechtliche Aspekte der Telemedizin – Grenzen der Telemedizin? MedR 1999, 197.

Urry, J.: Inhabiting the car, The Sociological Review 54 (2006), Issue Supplement s1, 17.

Verbraucherzentrale Bundesverband (Hrsg.): Smart Meter Einbau: Zwangsdigitalisierung durch die Kellertür, Stellungnahme des Verbraucherzentrale Bundesverbandes zum Entwurf eines Gesetzes zur Digitalisierung der Energiewende vom 9. Oktober 2015.

Vogelgesang, K.: Grundrecht auf informationelle Selbstbestimmung?, Baden-Baden 1987.

Voigt, C.: Die gläserne Seele – Big Data und Emotionserkennung, FAZ.NET, 10.3.2015.

Wehlau, A. / Lutzhöft, N.: Grundrechte-Charta und Grundrechts-Checkliste – eine dogmatische Selbstverpflichtung der EU-Organe, EuZW 2012, 45.

Weichert, T.: Big Data und Datenschutz, ZD 2013, 251.

Weichert, T.: Scoring in Zeiten von Big Data, ZRP 2014, 168.

Weichert, T.: Datenschutz im Auto, in: 52. Verkehrsgerichtstag, Köln 2014, 305.

Weichert, T.: Datenschutz im Auto – Das Kfz als großes Smartphone mit Rädern, SVR 2014, 201 und 241.

Wiener, N.: Mathematik – Mein Leben. Düsseldorf/Wien 1962 (engl. 1956), 208 ff.

Wilmer, S.: Wearables und Datenschutz - Gesetze von gestern für die Technik von morgen? in: Taeger, J. (Hrsg.), Internet der Dinge, Edewecht 2015, 1.

Wolfangel, E.: Können Maschinen rassistisch sein?, Technology Review (dt. Ausgabe) 1/2016, 59.

Bald werden viele Alltagsgegenstände und Alltagsumgebungen mit „intelligenter" und vernetzter Informationstechnik ausgestattet sein. Beispiele sind Smart Car, Smart Home und Smart Health. Dadurch werden immer weitere Lebensregungen in der körperlichen Welt, bis hinein in höchst private Bereiche des Autos, der Wohnung sowie des Gesundheitszustandes, als Daten verfügbar. Mit Big Data-Techniken können diese vielfältigen Daten analysiert, zu Persönlichkeitsprofilen zusammengeführt und als statistische Muster für wirtschaftliche Zwecke genutzt werden, um das Verhalten von Menschen und Gruppen zu prognostizieren und zu steuern. Gegen die damit verbundenen Risiken für Grundrechte helfen weder das geltende Datenschutzrecht noch die neue Datenschutz-Grundverordnung. Daher stehen der europäische und der deutsche Gesetzgeber vor der drängenden Aufgabe, sich der Modernisierung des Datenschutzrechts für eine Welt smarter Informationstechnik im Alltag anzunehmen. Das Buch enthält viele konkrete Vorschläge, diese Aufgabe zu erfüllen.

ISBN 978-3-7376-0154-2