ISSN 0178-8930

G 20 141

Zeitschrift für Datenschutz-, Informations- und Kommunikationsrecht

RDV

5/2014

Recht der Datenverarbeitung

Herausgegeben von

Peter Gola · Andreas Jaspers · Rolf Schwartmann · Gregor Thüsing
in Kooperation mit der
Gesellschaft für Datenschutz und Datensicherheit e.V. (GDD), Bonn

Aufsätze

Kurzbeiträge

Rechtsprechung

Aus dem Inhalt

30. Jahrgang
Oktober 2014
Seiten 229–290

GDD
Gesellschaft für Datenschutz und Datensicherheit e.V.

DATAKONTEXT
www.rdv-online.de

Zeitschrift für
Datenschutz-, Informations-
und Kommunikationsrecht

30. Jahrgang 2014
Heft 5
Seiten 229–290

RDV

Recht der Datenverarbeitung

Inhaltsverzeichnis

Beilagenhinweis GDD-Mitteilungen 5/2014; VERLAG C.H. BECK, München

Manuskripte
Zuschriften und Manuskriptsendungen, die den Inhalt der Zeitschrift betreffen, werden an die Schriftleitung erbeten. Für unverlangt eingesandte Manuskripte wird keine Haftung übernommen. Sie können nur zurückgesandt werden, wenn Rückporto beigefügt ist. Beiträge werden grundsätzlich nur angenommen, wenn sie nicht einer anderen Zeitschrift zur Veröffentlichung angeboten wurden. Mit der Annahme zur Veröffentlichung erwirbt der Verlag vom Autor alle Rechte, insbesondere das Recht der weiteren Vervielfältigung zu gewerblichen Zwecken mit Hilfe fotomechanischer oder anderer Verfahren.

Schriftleitung
Prof. Peter Gola (federführend)
RA Dr. Georg Wronka
RA Andreas Jaspers
RDV-Schriftleitung@gdd.de

Redaktionsanschrift
Birgit Koppitsch
Heinrich-Böll-Ring 10, 53119 Bonn
Telefon: (02 28) 96 96 75-00
Telefax: (02 28) 96 96 75-25
RDV-Redaktion@gdd.de

Erscheinungsweise
6 x jährlich

Bezugspreis
Jahresabonnement € 139,–
Einzelheft € 25,–
MwSt. im Preis enthalten
jeweils zzgl. Versandkosten

Bestellungen
DATAKONTEXT
Verlagsgruppe Hüthig Jehle Rehm GmbH
Standort Frechen
Jürgen Weiß
Augustinusstraße 9d
D-50226 Frechen-Königsdorf
Telefon: (0 22 34) 9 89 49-71
Telefax: (0 22 34) 9 89 49-32
E-Mail: weiss@datakontext.com
www.datakontext.com
Geschäftsführer: Dr. Karl Ulrich
Leitung: Hans-Günter Böse
HRB 337678

Abbestellungen
Der Abonnementpreis wird im Voraus in Rechnung gestellt. Das Abonnement verlängert sich zu den jeweils gültigen Bedingungen um ein Jahr, wenn es nicht mit einer Frist von 8 Wochen zum Ende des Bezugszeitraumes gekündigt wird.

Verlag
DATAKONTEXT
Verlagsgruppe Hüthig Jehle Rehm GmbH
Standort Frechen
Augustinusstraße 9d
D-50226 Frechen-Königsdorf
Telefon: (0 22 34) 9 89 49-30
Telefax: (0 22 34) 9 89 49-32
www.datakontext.com
Geschäftsführer: Dr. Karl Ulrich
Leitung: Hans-Günter Böse
HRB 337678

Satz
alka mediengestaltung gmbh
Ottostraße 6, 53332 Bornheim-Sechtem

Druck
AZ Druck und Datentechnik GmbH
Heisinger Straße 16, 87437 Kempten

Anzeigenverwaltung
DATAKONTEXT
Verlagsgruppe Hüthig Jehle Rehm GmbH
Thomas Reinhard-Rief
Hultschiner Straße 8
D-81677 München
Telefon: (089) 21 83-89 35
Fax: (089) 21 83-96 02 33
E-Mail: reinhard@datakontext.com
www.datakontext.com
Geschäftsführer: Dr. Karl Ulrich
Leitung: Hans-Günter Böse
HRB 337678

Zeitschrift für
Datenschutz-, Informations- und Kommunikationsrecht
Schriftleitung:
Prof. Peter Gola, Königswinter
(federführend)
RA Dr. Georg Wronka, Bonn
RA Andreas Jaspers, Bonn
Redaktion: Birgit Koppitsch
30. Jahrgang 2014 Heft 5
Seiten 229–290

RDV
Recht der Datenverarbeitung

30. Jahrgang · Oktober 2014 · Seiten 229–290

Editorial

Willkommen in der Smart World

Die Bundesregierung befasst sich derzeit mit dem Thema Fracking. Es ist zunächst ein befristetes Verbot geplant, weil die Umweltrisiken unwägbar sind. Auch mit Fragen der vernetzten Welt setzt sich die Bundesregierung auseinander. Der Innenminister betont zu Recht, dass im Netz dasselbe Recht gilt wie in der körperlichen Welt. Der Justizminister warnt vor der Entmündigung der Bürger durch Google: "Die Nutzer verlieren die Kontrolle über ihre Daten und damit über einen wichtigen Teil ihres Lebens." Wer will ihm da widersprechen? Regulatorisch fordert der Minister: "Google muss die Kriterien, nach denen die Suchergebnisse geordnet werden, offenlegen." Das ist eine gewichtige Forderung, die so massiv in die Berufsfreiheit des Datengiganten eingreift, wie die nach der Preisgabe des Coca Cola-Rezepts gegenüber dem Softdrinkgiganten wirken würde, aber noch nicht so intensiv wie ein befristetes Verbot wie beim Fracking. Mit welchem Recht soll der Staat so intensive Einblicke in Geschäftsgeheimnisse verlangen dürfen? Vielleicht mit demselben Recht, mit dem er das Fracking reglementiert: Weil der Dienst, den Google betreibt, unwägbare Risiken für Staat und Gesellschaft birgt, die Staaten nur dulden können, wenn sie die Regeln, nach denen sie funktionieren, kennen. Das ist deshalb so problematisch, weil man mit den Netzdiensten zugleich auch Kommunikationsmöglichkeiten reguliert, die für die bürgerliche Freiheit so elementar sind, wie die Luft zum Atmen. Zudem schaffen diese Datendienste Arbeitsplätze. Aber das ist kein Grund, sie nicht zu regulieren und ihre Gefahren kalkulierbar zu machen.

Welche Unwägbarkeiten von solchen Diensten für Daten ausgehen können, kann man sich leicht an Anwendungen der Smart World veranschaulichen. Wie könnte eine Krankmeldung 4.0 lauten? „Guten Morgen Chef, ich bin heute nicht fit. Meine Herzfrequenz ist zu hoch und ich habe Fieber. Dabei ist mein Blutdruck völlig o.k. und ich habe mich in letzter Zeit immer gesund ernährt und auch kaum Alkohol getrunken. Ich muss mich krank melden. Muss ich zum Arzt oder reichen Ihnen aktuelle Screenshots von Apple Health? Ich habe alles da und könnte Ihnen aus den Vitalzeichen Atemfrequenz, Blutdruck, Herzfrequenz und Körpertemperatur mailen. Gerne kann ich auch Blutalkoholwert, Inhalatorgebrauch und Co. schicken. Falls Sie eine Schlafanalyse wollen, ist das auch kein Thema, ebenso gebe ich gerne meine Ernährungswerte wie Cholesterin, Magnesium und so weiter durch. Dann können Sie gleich mal prüfen lassen, ob Sie Anhaltspunkte dafür finden, dass das Essen in der Kantine schlecht war…". Eine solche Krankmeldung ist Stand der Technik. Wer zu seinem Smartphone mit iOS 8 eine Apple-Watch oder ein anderes Wearable am Körper trägt, der kann alle diese Daten über die App Health – die iOS 8 beim Update mit überträgt – jedem mitteilen. Er kann das gegenüber dem Arbeitgeber tun und dieser wiederum kann die Informationen je nach vertraglicher Vereinbarung mit dem Arbeitnehmer, einer Versicherung, einem Automobilhersteller usw. anbieten. Der CloudAnbieter hat die Daten ohnehin. Da hat nicht nur der Gesetzgeber viel zu regeln, sondern auch der betriebliche Datenschutzbeauftragte viel zu erklären. Willkommen in der Smart World.

Rolf Schwartmann

Prof. Dr. Rolf Schwartmann
Leiter der Kölner Forschungsstelle für Medienrecht an der Fachhochschule Köln, Mitherausgeber der Fachzeitschrift RDV sowie Vorstandsvorsitzender der GDD e.V., Bonn

Termin	Thema	Ort	Kontakt
27.10.2014	Der Teilzeit-Datenschutzbeauftragte	Köln	GDD e.V. und DATAKONTEXT
28.10.2014	Personalprozesse datenschutzkonform organisieren	Köln	GDD e.V. und DATAKONTEXT
28.10.2014	Drop Box und Iphone: dienstliche Nutzung privater IT – Bring Your Own Device-Strategie	Frankfurt/M.	GDD e.V. und DATAKONTEXT
28.10.2014	Datenschutzaudit leicht gemacht	Köln	GDD e.V. und DATAKONTEXT
30.10.2014	Das neue Melderecht	Köln	GDD e.V. und DATAKONTEXT
04.11.2014	Was der Datenschutzbeauftragte von der IT-Sicherheit wissen sollte!	Frankfurt/M.	GDD e.V. und DATAKONTEXT
05.11.2014	Die Datenpanne! Ein Albtraum jedes Unternehmens	Köln	GDD e.V. und DATAKONTEXT
06.11.2014	Herausforderung: Internationaler Datenverkehr	Köln	GDD e.V. und DATAKONTEXT
10.11.2014	Umsetzung des neuen Datenschutzstandards bei Dienstleistern – Workshop	Köln	GDD e.V. und DATAKONTEXT
12.11.2014	Audit Technisch-organisatorischer Datenschutz	Köln	GDD e.V. und DATAKONTEXT
12.-13.11.2014	Datenschutz-Management – Teil 3	Berlin	GDD e.V. und DATAKONTEXT
13.11.2014	Prüfung von SAP-Systemen durch Datenschutzbeauftragte	Frankfurt/M.	GDD e.V. und DATAKONTEXT
19.11.2014	33. RDV-Forum	Köln	GDD e.V. und DATAKONTEXT
20.-21.11.2014	38. DAFTA „Smart Future – Intelligenter Datenschutz“	Köln	GDD e.V. und DATAKONTEXT
24.11.2014	Datenschutz Aktuell	Stuttgart	GDD e.V. und DATAKONTEXT
26.11.2014	Repetitorium GDDcert.	Berlin	GDD e.V. und DATAKONTEXT
24.-26.11.2014	Das SAP-System für Datenschutzbeauftragte	Köln	GDD e.V. und DATAKONTEXT
27.11.2014	Social Media im Unternehmen – aber sicher!	Köln	GDD e.V. und DATAKONTEXT
01.-02.12.2014	ARGE IT-Sicherheit	Köln	GDD e.V. und DATAKONTEXT
01.-05.12.2014	Einführung in den Datenschutz für die Privatwirtschaft – Teil 1	Berlin	GDD e.V. und DATAKONTEXT
09.-10.12.2014	ARGE Datenschutz International	Köln	GDD e.V. und DATAKONTEXT
16.12.2014	Zertifizierung zum betrieblichen Datenschutzbeauftragten (GDDcert.)	Köln	GDD e.V. und DATAKONTEXT s.o.
27.-27.01.2015	GDD-Winter-Workshop	Garmisch-Partenkirchen	GDD e.V. und DATAKONTEXT
02.-06.03.2015	Auditierung der Auftragsdatenverarbeitung – Workshop	Köln	GDD e.V. und DATAKONTEXT
14.04.2015	Kontrolle von Auftragnehmern im Rahmen der Auftragsdatenverarbeitung – Workshop	Stuttgart	GDD e.V. und DATAKONTEXT

DATAKONTEXT, Verlagsgruppe Hüthig Jehle Rehm GmbH, Telefon: 02234/9894940

Aufsätze

Dr. Oliver Raabe / Eva Weis

Datenschutz im „SmartHome“

Für die Rechtsanwendung ist mit der Einführung neuer Oberbegriffe, wie dem des im vorliegenden Beitrag untersuchten „SmartHome“, zunächst kein Mehrwert verbunden. Schon der definitorische Kern ist regelmäßig vom Blickwinkel der Fachdomäne des jeweiligen Betrachters geprägt. Gleichwohl können die Erscheinungen, die hinter diesen Begriffen stehen, im Hinblick auf ihre rechtlich relevanten Besonderheiten sondiert werden. Charakteristika des SmartHomes sind ähnlich wie z.B. beim sogenannten „Internet of Everything“[1] darin zu vermuten, dass Netze, Dinge, Prozesse, soziales Verhalten und Daten allumspannend zusammengeführt werden. Dies offenbart bereits die datenschutzrechtliche Relevanz des „SmartHomes“, welcher sich der vorliegende Beitrag widmet.

I. Einleitung

Die nachfolgende Untersuchung will den Versuch einer Systematisierung der Phänomene, welche sich im Zusammenhang mit SmartHomes stellen, anhand typisierter, für Datenschutzaspekte besonders kennzeichnender Fallgestaltungen unternehmen. Dies erweist sich im Ergebnis als Betrachtung von auch rechtswissenschaftlich und gesetzlich mehr oder weniger schon antizipierten jüngeren Technikerscheinungen wie der Einführung von RFID, neuer Adressierungsschemata oder gar der Öffnung von privater Sensorik und Transportkapazität an den Enden des Netzes. Ebenso sind in diesem Zusammenhang soziale Phänomene, wie die freiwillige Informatisierung des Heimbereiches mit proprietärer Hard- und Software, ihre Verbindung mit sozialen Netzen oder gar Gesundheitsdienstleistungen bis hin zum gesellschaftlichen Phänomen der staatlich geforderten Preisgabe von Energiedaten und der Pflicht zum Einbau von standardisierten und zertifizierten Kommunikationsschnittstellen in den betroffenen Haushalten[2], zu nennen. Bisher lag der Fokus der datenschutzrechtlichen Bewertungen nur auf den verpflichtend einzubauenden Smart Metern[3], während die weitaus größeren datenschutzrechtlichen Herausforderungen eines vollumfänglich vernetzten SmartHomes noch weitgehend unbetrachtet geblieben sind[4].

Um die neuen datenschutzrechtlichen Aspekte aufzeigen zu können, bedarf es aufgrund der Vielzahl der unterschiedlichen Anwendungsmöglichkeiten innerhalb eines SmartHomes[5] systematisierender Ordnungskriterien. Diese lassen sich vorliegend zum einen in den Entwicklungslinien und -treibern in ökonomischer, technologischer und gesellschaftlicher Perspektive verorten. Zum anderen kann, aus dem Blickwinkel einer schichtspezifischen technischen Sicht nach der Innengestaltung der Sensorik (Innenbereich), der Außenanbindung durch eine Kommunikationsschnittstelle (Außenschnittstelle) sowie der Situierung der zweckspezifischen Verarbeitungstechniken in Internetarchitekturen (Außenbereich) und ihren neuen sozialen Funktionen differenziert werden.

II. Technische Grundlagen

Bislang ist keine einheitliche Definition des Begriffs „SmartHome“ ersichtlich. Arbeitshypothetisch soll die folgende Beschreibung als Grundlage dienen: „Das Smart Home ist ein privat genutztes Heim (z.B. Eigenheim, Mietwohnung), in dem die zahlreichen Geräte der Hausautomation (wie Heizung, Beleuchtung, Belüftung), Haushaltstechnik (wie z.B. Kühlschrank, Waschmaschine), Konsumelektronik und Kommunikationseinrichtungen zu intelligenten Gegenständen werden, die sich an den Bedürfnissen der Bewohner orientieren. Durch Vernetzung dieser Gegenstände untereinander können neue Assistenzfunktionen und Dienste zum Nutzen des Bewohners bereitgestellt werden und einen Mehrwert generieren, der über den einzelnen Nutzen der im Haus vorhandenen Anwendungen hinausgeht.“[6]

Ein allen Sachgestaltungen zugrundeliegendes technologisches Charakteristikum von SmartHomes ist, dass die jeweiligen Häuser und Wohnungen mit verteilter Sensorik und entsprechender Gerätesteuerung versehen sind. Die Sensorik ist durch unterschiedliche Trägertechnologien und Adressierungsschemata für Objekte im Haushalt vernetzt und bietet Schnittstellen zu einem öffentlichen Netz an. Die von den Sensoren erfassten unterschiedlich granularen Echtzeitdaten können zudem mit klassischen Internetanwendungen oder in Service-Architekturen adressiert und zweckspezifisch weiterverarbeitet werden.

1 Vgl. nur http://internetofeverything.cisco.com/de.

2 Die Pflicht zum Einbau intelligenter Messsysteme besteht unter den Voraussetzungen des § 21c EnWG.

3 Siehe z.B. Wiesemann, ZD 2012, 447; Jandt/Roßnagel/Volland, ZD 2011, 99; noch zur alten Rechtslage Wiesemann, MMR 2011, 355, 356 ff.; Raabe/Pallas/Weis/Lorenz/Boesche, Datenschutz in Smart Grids.

4 Siehe z.B. zum Ambient Assisted Living (AAL) Regnery, DSRI Tagungsband 2012, 579 oder zum „Smart Life“ Heckmann K&R 2011, 1.

5 Siehe zu einer Übersicht möglicher Anwendungen Strese/Seidel/Knape/Botthof, Smart Home in Deutschland, S. 9.

6 Strese/Seidel/Knape/Botthof, Smart Home in Deutschland, S. 8.

Aus datenschutzrechtlicher Perspektive ist die technische „Intelligenz“ zur zweckgerichteten Assistenz und zur Bereitstellung von Diensten zum Nutzen der Bewohner noch weiter zu differenzieren. Die Funktionen der Sensorik zur Datenerfassung und Steuerung können einerseits zweckgerichtet über Hardware umgesetzt werden, was aufgrund dieses Charakteristikums eine Zweckänderung nur bedingt zulässt. Andererseits können die Sensorik und die Steuerungseinheiten zukünftig in eine auf diesen Komponenten realisierte Softwareumgebung eingebunden sein, welche eine Datenverwendung nicht nur im ursprünglichen Zweckbereich zulässt, sondern eine Anpassung der Datenerfassung und Gerätessteuerung bereits allein durch Änderung der Softwarekonfiguration erlaubt. Es ist demzufolge möglich, dass die zu erfassenden Daten, die Kombinatorik von Daten und die gewünschten Steuerungsoptionen von der Hardware unabhängig sind und insofern durch reine Softwareanpassungen verändert werden können. Auf dieser Basis lassen sich unbemerkt und in Echtzeit bedarfsgerecht flexible Messungen und Schaltaufgaben realisieren, die von den Ursprungszwecken der Hardware nicht erfasst waren. Relevant ist die Möglichkeit der Softwarekonfiguration von Sensorik und Steuerungseinheit aus datenschutzrechtlicher Perspektive auch deshalb, weil durch entsprechende Softwarekonfiguration automatisierte Entscheidungen für den Bewohner getroffen werden können, welche sich unmittelbar durch Steuerung durchsetzen lassen. Diese Entscheidungen werden künftig „intelligent“ durch Algorithmen bestimmt und gerade nicht mehr durch für den Bewohner bekannte Hardwarefunktionalitäten und nachvollziehbare Zwecke.

Die „Intelligenz“ durch freie Softwarekonfigurierbarkeit kann sich im SmartHome auch auf die hausinternen Kommunikationsinfrastrukturen beziehen. Mit der individuellen Adressierbarkeit von Datenquellen und Steuerungseinheiten durch IPv6[7] deutet sich dieser Trend bereits an. Hausinterne Datenquellen und -senken sind bereits heute von außen erreichbar. Dies führt dazu, dass die Erwartungshaltung der Bewohner auf die rollen- und ortsspezifische Verwendung der Daten regelmäßig nicht mehr den tatsächlichen Gegebenheiten entspricht. Mit anderen Worten, die Erwartung von Innen- und Außenbereich der Netze, wie sie sich heute auch im Regulierungskonzept des TKG spiegelt, wird aufgelöst. Neue Adressierungskonzepte wie das „Content-Centric Networking“[8] werden sich auch zur Suche nach Datengrundlagen für heute noch unbekannte Zwecke in Privathaushalten etablieren. Damit kann eine Differenz zwischen Ursprungskontext der Daten, der Sensorik sowie infolgedessen auch der Erwartungshaltung der Bewohner und der flexiblen „intelligenten“ Generierung von Informationen und Zusammenhängen an entfernten Orten und in ursprünglich nicht intendierten Kontexten entstehen.

Ferner wird die freie Konfigurierbarkeit durch flexible Softwaresteuerung auch die internen Netze des SmartHomes betreffen und dynamische Konfigurationen in Echtzeit erlauben, welche für die Betroffenen unsichtbar sind. Als Beispiel soll die flexible Nutzung von verschiedenen hausinternen Routern zur Bereitstellung von temporärem Bandbreitenbedarf dienen, die zukünftig durch einen (externen) Kontroller oder allein durch Algorithmen erfolgt. Auch hier können Entscheidungen für Betroffene nicht mehr nur durch die ursprünglich intendierten Zwecke der Hardware, sondern ebenso durch unvorhersehbare und nachträgliche Entscheidungen einer Kontrollinstanz durchgesetzt werden. Diese technischen Optionen können in unterschiedlicher Kombination und Ausprägung in SmartHome-Architekturen umgesetzt werden.

III. Sachgestaltungen des SmartHomes

Im Folgenden sollen drei exemplarische Sachgestaltungen des SmartHomes dargestellt werden, wobei insbesondere die historische Entwicklung unter dem Gesichtspunkt des ökonomischen Treibers sowie die Entwicklung und Änderung der sozialen Funktion beachtet werden. Auf Basis dieser Sachgestaltungen sollen die datenschutzrechtlichen Besonderheiten des SmartHomes erläutert werden.

1. Sachgestaltung [1]: Private „einfache“ Hausautomatisierung

Die erste spezifische datenschutzrelevante Ausprägung setzt historisch bei der klassischen Hausautomatisierung an. Diese bezieht sich auf rein private Zwecke im Innenbereich eines Haushaltes. Beispiele hierfür sind die Überwachung von Pflanzenwachstum, Sicherheitsmechanismen zur Hausüberwachung und einfache interne Gerätesteuerungen. Die verwendeten Basistechnologien der hier noch stationären Sensorik und rein internen Vernetzung sind regelmäßig Standardkomponenten ohne eigene Intelligenz. Diese nutzen private Adressierungsschemata, wobei der jeweilige Sensor immer nur zu einem singulären Zweck verwendet werden kann. Dennoch können in der heimischen Datenzentrale, abhängig vom konkreten Verwendungszweck und der jeweiligen Aufbereitung der Daten, – wenn auch nur als Reflex – schon einfache Ableitungen zu Interaktionen der Bewohner mit der Sensorik und somit in Bezug auf deren Verhalten vorgenommen werden. Die datenschutzrechtlich relevanten Rollen sind hier der private Technikgestalter, d.h. derjenige, der die einzelnen Geräte beschafft, installiert und verwendet, sowie Familienmitglieder und gegebenenfalls Besucher und Mieter.

2. Sachgestaltung [2]: Private Datenverwendung unter Einbeziehung standortbezogener Sensorik und externer Dienstleister

Die nächste Ausprägung von Charakteristika des SmartHomes ergibt sich aus der Einbeziehung von Sensorik und Datenverwaltung, welche über Schnittstellen ihren jeweiligen Standort preisgeben und auf die auch aus der Ferne zugegriffen werden kann. Diese Sachgestaltung adressiert noch immer den privaten Akteur und den Markt als Entwicklungstreiber. Die von Smartphones erfassten Daten bzw. Gesundheitsdaten z.B. aus

7 Vgl. Freund/Schnabel, MMR 2011, 495, 495 f.

8 Jacobson/Smetters/Thornton et al., Networking Named Content, CoNEXT, 09, Proceedings of the 5th international conference on Emerging networking experiments and technologies, S. 1 ff.

Aktivitätstrackern weisen technologisch den Weg zu zunehmend proprietären und geschützten standardisierten Basistechnologien, was die Abhängigkeit von Lösungsanbietern wie Google oder Apple als Entwicklungstreiber erhöht. Gleichzeitig werden neben den Kommunikationsprotokollen durch diese Akteure faktische Standards für die erstrebten Mehrwerte der Vernetzung gesetzt, die sich regelmäßig in der Nutzung von öffentlichen Netzen und der Verwendung von Dienstarchitekturen zur Datenrepräsentation manifestieren. In gesellschaftlicher Perspektive ist die faktische Nutzung dieser Angebote durch Private, bedingt durch Plug&Play-Versprechen der Hersteller und die Bereitschaft zur öffentlichen Einbindung der Datengrundlagen in angebotenen Anwendungen sozialer Medien, zu konstatieren. Technologisch bedeutet diese Entwicklung die faktische Akzeptanz von verschiedenartig implementierten orts- und personenbezogenen – ehemals in privaten Netzen isolierten – Sensoren und Netzen in den Haushalten, die Option der vollkommen ortsunabhängigen Einsicht in die hierdurch generierten Daten durch den Berechtigten und damit die zwangsläufige Nutzung und Relevanz von Außenschnittstellen des vormaligen Privatbereiches. Der Kreis der relevanten Rollen wird im Vergleich zu Sachgestaltung [1] noch um den Dienstprovider für die Basiskommunikation und die Inhaltsdatenverarbeitung erweitert. Hinsichtlich der Zwecke, die mit diesen Datenverwendungen verfolgt werden, ist exemplarisch insbesondere der Gesundheitsbereich hervorzuheben[9], bei dem einerseits die individuell erstrebten positiven Effekte und andererseits die potentiellen Angriffsszenarien, insbesondere auch auf besondere Arten personenbezogener Daten im Sinne des § 3 Abs. 9 BDSG, auf der Hand liegen.

3. Sachgestaltung [3]: Staatlich beeinflusste Technikgestaltung

Die dritte systematisierende Ausprägung erfährt das SmartHome derzeit durch die Einführung von Smart Metern, insbesondere durch das Smart Meter Gateway (SMGW). Das motivierende Ziel ist, dem Kunden die aktive Beteiligung am Energiemarkt zu ermöglichen[10]. Durch die Erfassung von Energiedaten und die Steuerung von schaltbaren Lasten im Haushalt soll zur Steigerung der Energieeffizienz beigetragen werden[11]. Aus der Perspektive der Entwicklungstreiber, also dem gesellschaftlich relevanten Kriterium, ob sich der Einzelne dieser Entwicklung im Wege einer autonomen Entscheidung entziehen kann, liegt der maßgebliche Unterschied darin, dass nach der EnWG-Novelle 2011 nun jeder der nach § 21c Abs. 1 EnWG relevanten Betroffenen zur Duldung einer Kommunikationsschnittstelle zu einem öffentlichen Netz verpflichtet ist. Die diesbezüglichen, öffentlich dokumentierten, alle technischen Schichten[12] betreffenden Standardisierungen[13] von energiebezogener Sensorik und ihrer Adressierbarkeit sowie die Datenaufbereitung im Innen- und Außenbereich, die durchzuführenden nachgelagerten Prozesse, vorgegebenen Nachrichtenformate[14] und die legitimen Verarbeitungszwecke[15] können für den Energiebereich als gesetzt gelten[16]. Diesbezüglich sind insbesondere die produktbezogenen technischen Sicherheitsvorgaben des Bundesamtes für Sicherheit in der Informationstechnik (BSI) an das SMGW[17] zu nennen. Gleichzeitig wird im derzeitigen normativen Prozess zu den Spezifika des SMGW aber auch eine für die zukünftige Entwicklung des SmartHomes maßgebliche Verbindungslinie zu den vorgenannten privaten Beispielausprägungen angelegt. So wird im Entwurf zur Messsystemverordnung (MsysV-E) ausgeführt, dass das SMGW „als sicherer Kommunikationsanker vielfältigste Anwendungen und Dienste im intelligenten Energienetz und darüber hinaus (z.B. Anwendungen im Bereich betreutes Wohnen)“ ermögliche[18]. Es bleibt allerdings anzumerken, dass die Interoperabilitäts- und Sicherheitsanforderungen des BSI in ihrem verbindlichen Gehalt nur produktbezogen[19] auf das Schnittstellendesign wirken, nicht aber die nachfolgenden Prozesse und Kontexte, in denen die relevante Datenverarbeitung und Aufbereitung stattfindet, ordnungsrechtlich und technikgestaltend terminieren. Insofern bleibt es bei den nicht energiebezogenen Szenarien bei den im vorgängigen Beispiel genannten Phänomenen der Herrschaft über die Kontexte von Datenverwendungen und der Option unterschiedlicher paralleler Technikentwicklungen. In der Folge unterscheiden sich auch die fallspezifischen Möglichkeiten von für die Datensicherheit relevanten Angriffen auf die Sensorik, Netze und Schnittstellen sowie die Optionen der technischen Überwachungsmöglichkeiten durch private und staatliche Akteure.

IV. Herausforderungen für den Schutz der informationellen Selbstbestimmung

Voraussetzung für eine datenschutzrechtliche Prüfung ist zunächst die Anwendbarkeit der datenschutzrechtlichen Normen für die konkrete Sachgestaltung. Diese hängt davon ab, ob im konkreten Verwendungszusammenhang überhaupt ein personenbezogenes Datum im Sinne von § 3 Abs. 1 BDSG vorliegt und ob gegebenenfalls eine Ausnahme von der Gesetzesanwendung, wie z.B. § 1 Abs. 2 Nr. 3 BDSG, greift. Insofern ist in Sachgestaltung [1][20] das adressierte Charakteristikum rele-

9 Zu den Möglichkeiten des Ambient Assisted Living Regnery, DSRI Tagungsband 2012, 579, 580 ff.

10 Anhang I Abs. 2 der RL 2009/72/EG; Erwägungsgrund 31 der RL 2012/27/EU.

11 Vgl. z.B. Benz, ZUR 2008, 457, 458 ff.

12 Unter technischen Schichten werden diejenigen des ISO/OSI-Modells verstanden. Siehe zur Unterscheidung dieser Schichten aus rechtlicher Sicht Eckhardt in: BeckOK TKG, § 109a Rn. 9.

13 Vgl. BSI, TR-03109-1, S. 31.

14 Siehe zu den verbindlichen Geschäftsprozessen sowie Nachrichtenformaten im Energiebereich insb. BNetzA, Beschluss BK6-06-009 sowie BNetzA, Beschluss BK6-09-034.

15 § 21g Abs. 1 EnWG enthält im Rahmen seines Anwendungsbereiches eine abschließende Aufzählung der legitimen Verarbeitungszwecke, vgl. Lorenz/Raabe in: Säcker, Energierecht, § 21g Rn. 17.

16 Eine „Verrechtlichung“ soll durch Erlass der bereits von der EU notifizierten MsysV erfolgen, MsysV-E, S. 24.

17 Siehe BSI, TR-03109-1 und BSI, SMGW-PP.

18 MsysV-E, S. 20.

19 Siehe zum ausschließlich produktbezogenen Schutz Raabe/Lorenz/Pallas/Weis, CR 2011, 831, 834, 838 ff.

20 Auf die in III. dargestellten Sachgestaltungen wird im Folgenden entsprechend der ihnen zugewiesenen Nummerierung [1, 2, 3] referenziert.

vant, dass es sich bei der Nutzung der Inhaltsdaten der Sensorik um eine Tätigkeit handelt, die zunächst nur im privaten Raum wirkt. Ebenso ist augenfällig, dass sich die Adressaten der bereichsspezifisch dienstbezogenen Datenschutzregelungen des TMG und der netzbezogenen Regelungen des TKG, unabhängig von der Klassifikation der Daten, grundsätzlich am „Dienstbegriff“ orientieren. Dies weist auf ein durchgehendes Motiv des Gesetzgebers hin, den klassischen privaten Bereich der Lebensführung vom Anwendungsbereich der Vorschriften auszunehmen. Ob dies de lege lata für das SmartHome in Sachgestaltung [1] gelten kann, erscheint allerdings zweifelhaft.

1. Allgemeine Anwendbarkeit datenschutzrechtlicher Regelungen

a) BDSG

Nach dem Wortlaut des § 1 Abs. 2 Nr. 3 BDSG würde man in den Fällen der privaten Hausautomatisierung [1] sowie auch im Fall [2] im Hinblick auf den privaten Betreiber der vernetzten Sensorik von einer prinzipiellen Privilegierung der Datenverwendung im persönlichen oder familiären Bereich ausgehen. Infolgedessen wäre hinsichtlich der Inhaltsdaten der Anwendungsbereich des BDSG nicht eröffnet. Allerdings ist zu konstatieren, dass durch die Möglichkeit die Sensordaten auszuwerten und somit die persönlichen Verhältnisse beliebiger Dritter im Haushaltsbereich in einem elektronischen System zu erfassen, eine Gefahr für die informationelle Selbstbestimmung der Betroffenen regelmäßig gegeben ist. Dies gilt besonders, sofern, wie in Fall [2], eine unbemerkte Überwachung unabhängig vom Aufenthaltsort des Datenverwenders stattfinden kann. Analysen auf Basis dieser Daten, welche bis hin zur Bestimmung des gerade eingeschalteten Fernsehprogrammes[21] oder des zimmergenauen Aufenthaltsortes einer Person reichen können, eröffnen ganz neue Möglichkeiten der wechselseitigen innerfamiliären Kontrolle. Der Privilegierungstatbestand für den innerfamiliären Bereich in § 1 Abs. 2 Nr. 3 BDSG muss hier nach dem Schutzzweck deshalb grundsätzlich eng ausgelegt werden. Die Bedrohungslage ist insofern weitaus größer, als bei Sachgestaltungen, die den Gesetzgeber in der historischen Perspektive zur Eingrenzung des Anwendungsbereiches des BDSG bewogen haben. Dass SmartHome-Anwendungen erheblich über den originären Sinn und Zweck dieser Regelung hinausgehen, zeigt sich deutlich an den genannten Beispielen des Schriftverkehrs oder des Führens von Anschriftenverzeichnissen in der EG-DSRL[22], auf welcher der Privilegierungstatbestand beruht[23]. Damit ist zu konstatieren, dass zukünftig auch der private Technikgestalter des SmartHomes hinsichtlich der Inhaltsdaten grundsätzlich dem Pflichtenkanon des BDSG unterworfen sein muss.

Für die Erweiterungen in Sachgestaltung [2] gilt dies für den Dienstanbieter, der die Auswertung und Präsentation der Inhaltsdaten der Sensorik übernimmt, erst recht. Hier stehen zudem abhängig von der technischen Übertragungstechnik auch oftmals Fälle einer Drittstaatenübermittlung mit den Obligationen aus §§ 4bff BDSG in Frage.

b) TMG

Verwendet der private Technikgestalter [1] zur Datenaufbereitung funktional gleichgerichtete Dienste und Datenkategorien, wie die Bestands- und Nutzungsdaten von Telemediendiensten, so wird er bei der zweckgerichteten Verwendung regelmäßig nicht selbst zu einem Anbieter von Telemediendiensten im Sinne des § 2 Nr. 1 TMG. Gleiches gilt für den privaten Technikgestalter in den Fällen der Nutzung von Plattformen eines Drittanbieters [2]. Im Hinblick auf die Gefahranlagen der Plattformnutzung und Verarbeitung der relevanten Daten hat er regelmäßig keine Gestaltungsmöglichkeiten, welche über die von mitnutzenden Familienangehörigen hinausgehen. Ebenso besteht keine erhöhte Gefahranlage, da die Nutzungs- und Bestandsdaten dem privaten Technikgestalter in diesen Fällen schon bekannt sind oder nur geringen Informationsgehalt aufweisen. Bei internetbasierten Datenauswertungen [2] von SmartHome-Umgebungen trifft die Verantwortlichkeit nach dem TMG vielmehr den zumeist kommerziellen Anbieter, bei welchem auch das im TMG betrachtete Gefahrenpotential für Massenauswertungen dieser dienstspezifischen Datenkategorien kumuliert.

c) TKG

Auch der Anwendungsbereich des TKG adressiert den privaten Sachgestalter der SmartHome-Sensorik grundsätzlich nicht. Die Regelungen der §§ 91ff TKG richten sich nach § 91 Abs. 1 TKG ausdrücklich an Anbieter, „die geschäftsmäßig Telekommunikationsdienste in Telekommunikationsnetzen, einschließlich Telekommunikationsnetzen, die Datenerfassungs- und Identifizierungsgeräte unterstützen, erbringen oder an deren Erbringung mitwirken“. Eine Einbeziehung des privaten Technikgestalters und Nutzers im SmartHome wäre zwar über die Formulierung „mitwirken“ in Sachgestaltung [2] nach dem Wortlaut grundsätzlich möglich oder gar bei der regelmäßigen Einbeziehung von privaten Datentransportinfrastrukturen, wie privaten Routern zur Versorgung Dritter, z.B. bei Wohneinheiten jenseits der bislang regulierten „letzten Meile“, sogar aus dem wettbewerblichen Blickwinkel notwendig. Aber diese Perspektive bedingt eine solche Änderung der Konzeption des telekommunikationsrechtlichen Rahmens und ein Ausrollen der dazu verfügbaren Konzepte zu Mischformen aus bislang schon verschieden regulierten Trägertechnologien, dass eine Betrachtung dieses Sonderfalls den Rahmen dieses Beitrags übersteigt.

Somit sind die Regelungen des TKG zunächst nur in Bezug auf den Anbieter der klassischen Kommunikationsinfrastrukturen anwendbar, womit nur diesen die Verantwortlichkeit nach dem TKG für die datenschutzkonforme Verwendung der Verkehrs- und Standortdaten der Sensorik im privaten Bereich trifft. Diese Verantwortlichkeit reicht allerdings nach der ge-

21 Greveler/Justus/Löhr, Identifikation von Videoinhalten über granulare Stromverbrauchsdaten, in: Sicherheit 2012, GI-Edition – Lecture Notes in Informatics (LNI), P 195, S. 35, 39ff.

22 Erwägungsgrund 12 der RL 95/46/EG.

23 Schmidt, in: Taeger/Gabel, BDSG, § 1 Rn. 27 ff.

genwärtigen gesetzlichen Konzeption nur bis zur Grenze der durch ihn adressierbaren Endgeräte im SmartHome; in Fall [1] also regelmäßig bis zum adressbeziehenden Router. Die sich für Sachgestaltung [2] ergebende Schutzlücke ist offenbar. Einerseits kann der Anbieter von proprietären Gesamtlösungen, z.B. zur Gesundheitsdatenerfassung und Auswertung, durch geeignete Protokoll- und Softwaregestaltungen auf dem Router oder dem PC, der bislang die Schnittstelle zum regulierten Außenbereich markiert, die netzspezifischen Objekt-, Adress- und Standortinformationen der Sensoren und zu steuernden Geräte, die derzeit funktional bereichsspezifisch dem TKG zugeordnet sind, lokal erfassen, auswerten und in seinen Herrschaftsbereich bringen. Zum Mitwirkenden einer TK-spezifischen Dienstleistung wird er aber gleichwohl nicht. Andererseits kennt der TK-Dienstleister weder die proprietären Protokolle zwischen lokaler Anwendung und Sensor noch die funktionalen Adressschemata und ist daher ebenfalls nicht aus dem TKG als Verantwortlicher berufen. Es deutet sich also an, dass insbesondere die (nicht) regulierten Adressschemata und Standortinformationen im vormals privaten Bereich, wegen der Möglichkeit der frühzeitigen Kapselung dieser Informationen durch Software, einer klarstellenden Generalrevision bedürfen, sofern Anwendung und Kommunikationsparadigma wie beim hier angedeuteten „Software-Defined Networking“[24] immer enger verschmelzen.

Für die Fälle der Einbeziehung von funktionalen TK-Daten der (standortbeziehbaren) Sensorik durch proprietär gestaltete Protokolle und Software im SmartHome [2], erscheint es einstweilen naheliegend, auf die Subsidiaritätsklausel des § 1 Abs. 3 BDSG abzustellen und nach dem Schutzzweck den Komplettlösungsanbieter auch für die „internen“ TK-Daten des SmartHomes als verantwortliche Stelle zu betrachten. Sofern für den jeweiligen konkreten Anwendungsfall eine das Schutzgut besser verwirklichende datenschutzrechtliche Regelung des TKG vorliegt, sollte wegen der offensichtlich planwidrigen, ungewollten Regelungslücke eine analoge Anwendung in Betracht gezogen werden.

d) EnWG

Die staatlich vorgegebene Duldungspflicht zum Einbau einer Kommunikationsschnittstelle [3] aus § 21c EnWG fokussiert auf Daten, die im Zusammenhang mit Energiemanagementsystemen stehen. Durch die granulare Aufzeichnung des Energieverbrauchs und dessen Veranschaulichung gegenüber dem Nutzer soll auf einer ersten Stufe der Gesamtenergieverbrauch gesenkt und auf einer zweiten Stufe das Abnahmeverhalten der momentanen Stromerzeugungssituation angepasst werden. Für Daten aus dem Messsystem und somit aus dem SMGW hat der Gesetzgeber im Zuge der EnWG-Novelle 2011 in den §§ 21cff EnWG bereichsspezifische Datenschutzregelungen erlassen[25]. Diese gelten für energiebezogene Daten, die gemäß § 21g Abs. 1 EnWG aus dem Messsystem stammen oder mit dessen Hilfe gewonnen wurden. Allerdings dürften die das SMGW adressierenden bereichsspezifischen Regelungen nicht für Daten einschlägig sein, welche zwar mittels der technischen Funktionen des SMGW übertragen, aber für gänzlich andere Zwecke, wie das beispielhaft genannte Betreute Wohnen[26], erhoben werden[27]. Im Falle einer solchen Verwendung des SMGW wäre insofern nicht auf die – ohnehin unpassenden – bereichsspezifischen Regelungen des EnWG zurückzugreifen.

2. Besonderheiten im „Innenbereich“

a) Personenbezug und neue Gefahren

Im Fall der privaten Hausautomatisierung [1] ergibt sich bei der Verwendung von einfacher nur für einen singulären Verwendungszweck konzipierter Hardwaresensorik im Innenbereich des Haushaltes noch kein gesteigertes Gefahrenpotential für die Bewohner. Entweder lassen, wie bei der Erfassung von Umweltdaten zur Gartenpflege, die Sensoren schon keine relevanten Schlüsse auf persönlich sachliche Verhältnisse der Betroffenen zu, oder die Eingriffsintensität ist regelmäßig gering. Beim Einsatz von Sensorik und Auswertungs bzw. Steuerungskomponenten zu Überwachungszwecken, z.B. bei Videoauswertungen, ist hingegen eine gesteigerte Eingriffsintensität zu bejahen.

In Sachgestaltung [2] sind dagegen grundsätzlich erhebliche Eingriffe zu erwarten. So können bei der Einbeziehung der Sensorik von Smartphones oder von Sensoren mit dediziertem Ortsbezug innerhäusliche Bewegungsprofile der Anwesenden erstellt werden. Dies ist sowohl in Echtzeit als auch historisch aufbereitet möglich. Ebenso können z.B. Daten aus gesundheitsbezogenen Sensoren die Erstellung eines Gesundheitsprofils des Betroffenen erlauben. Durch freie Kombination der Datenquellen ist folglich die Erfassung relativ exakter Lebensquerschnitte der Betroffenen möglich. Dies erreicht eine bislang ungeahnte Eingriffsqualität. Im Fall der Verwendung von Smart Metern ist, wie bereits erwähnt, z.B. schon nachgewiesen, dass sogar das zu einem gegebenen Zeitpunkt konsumierte Fernsehprogramm aus feinaufgelösten Strommessdaten extrahiert werden kann[28].

Netzbezogene Auswertungen der Basiskommunikation schaffen darüber hinaus wegen des spezifischen Personenbezuges der Daten paradigmatisch neue Dimensionen der Eingriffsqualität. So sind z.B. interne Auswertungen des Nutzungsverhaltens von Sensoren und Datenquellen durch Bewohner schon deshalb leichter nachvollziehbar, da interne Logfiles nicht mehr manuell nach IP-Adresse und zugehörigem Sensor ausgewertet werden müssen, um einen Inhaltsbezug herzustellen. Vielmehr lässt schon das selbstbeschreibende Namensschema der Adressierung in Content-Centric-Networks, welches eine automatisiert zu interpretierende Klartext-

24 Siehe zu „Software-Defined Networking“ z.B. Hasan, Emerging Trends in Communication Networks, S. 19 ff.

25 BR-Drucks. 343/11, S. 192 ff.

26 MsysV-E, S. 20.

27 In anderem Kontext Weis/Pallas/Raabe/Lorenz in: Boesche/Franz/Fest/Gaul, Berliner Handbuch zur Elektromobilität, S. 304 ff.

28 Greveler/Justus/Löhr, Identifikation von Videoinhalten über granulare Stromverbrauchsdaten, in: Sicherheit 2012, GI-Edition-Lecture Notes in Informatics (LNI), P 195, S. 35, 39 ff.

beschreibung des Inhalts enthält[29], eine Zuordnung der Netzwerk-Protokollinformationen zu dem jeweiligen Inhalt zu. Die Netzschicht verliert folglich ihren ehemals transparenten Charakter und wird selbst Träger von Inhaltsinformationen. Ebenso erlaubt z.B. die freie softwarebasierte Routerkonfiguration für innerhäusliches Bandbreitenmanagement, welches unter Umständen sogar selbstgesteuert ist, in ihren Protokollen eine leichte Zuordnung von Zeitpunkt und Bandbreiteninanspruchnahme. Dies ermöglicht z.B. eine historische Auswertung des Medienkonsums im SmartHome unmittelbar aus Informationen der Kommunikationsschicht. Diese Profilbildungsmöglichkeiten bleiben den Betroffenen weitestgehend verborgen.

b) Transparenz

Ebenso steht das hinsichtlich der Informationspflichten in § 4 Abs. 3 BDSG statuierte und als Grundlage für eine autonome Entscheidung in der Einwilligung des § 4a BDSG zum Ausdruck kommende Transparenzgebot[30] im SmartHome vor vollkommen neuartigen Herausforderungen. Dies gilt im Innenbereich umso mehr, als sich die Drittbetroffenen hier klassischerweise keiner besonderen Gefahr für ihre informationelle Selbstbestimmung ausgesetzt sehen. Dennoch ist die mit dem Transparenzprinzip adressierte Erwartungs- und Verhaltenssicherheit[31] der Betroffenen im Fall der Verwendung von dediziert hardwarekodierter Sensor- und Steuerungstechnik [1] nur geringfügig eingeschränkt, da der Zweck der Sensoren und Steuerungseinheiten den Hausbewohnern in der Regel bekannt und deren Verhalten vorhersehbar ist. In diesen Fällen dürften die Informationspflichten nach § 4 Abs. 3 BDSG schon wegen anderweitiger Kenntniserlangung entfallen.

Herausfordernd wird die Gewährleistung der notwendigen Transparenz jedoch spätestens bei Sachgestaltungen, in denen die interne Sensorik, Steuerung und Auswertung durch die Einbettung in von der Hardware abstrahierte Software für sich und in der Gesamtsicht „intelligent“, d.h. unabhängig vom Ursprungszweck frei konfigurierbar wird [2]. Hier bleibt den Betroffenen schon im Innenbereich regelmäßig verborgen, wann welche Sensordaten vom privaten Technikgestalter oder vom Lösungsanbieter für welche u.U. auch neuen Zwecke verwendet bzw. kombiniert werden. Insofern stoßen im Innenbereich die insbesondere in § 4 Abs. 3 Nr. 2 BDSG für diese Situation vorgesehenen Pflichtangaben für die Betroffenen zu „Zweckbestimmungen der Erhebung, Verarbeitung oder Nutzung“ an ihre Grenzen. Zum einen erscheint es für SmartHomes impraktikabel, jedem Gast eine hinreichende Aufklärung zukommen zu lassen. Zum anderen übersteigen diese Informationen in der notwendigen Dichte wegen der vielfältig möglichen Sensorik und Verwendung zumeist ohnehin den Erkenntnishorizont der Betroffenen. Das gilt umso mehr, als der Hersteller in der Lage ist, im Fall der Nutzung proprietärer Systeme mit unveröffentlichten Protokollstandards die Sensorik und die Datenauswertungen durch Softwareupdates umzukonfigurieren, was für den privaten Technikbetreiber unerkennbar sein kann. Dementsprechend verfügt der zur Aufklärung verpflichtete private Technikgestalter schon selbst nicht mehr über eine hinreichende Sachgrundlage zur Informationsvermittlung. Dazu kommen die Möglichkeiten des Betreibers der Infrastruktur, spontane Zweckänderungen und Auswertungen nachträglich durchzuführen und mithin eine Willensbildung und Entscheidung des Betroffenen zu konterkarieren. Ob auch für SmartHomes die vorhandenen Ansätze zur Veränderung der informatorischen Basis hin zu Strukturinformationen[32] abhelfen können, erscheint fraglich.

Selbst für den bereits gesetzlich strukturierten Bereich staatlich beeinflusster Technikgestaltung bei Smart Metern [3] ist aus dem Gesichtspunkt der Transparenz zu konstatieren, dass der Gesetzgeber für den Fall der Visualisierung des Energieverbrauchs durch ein lokales Display noch keine Detailregelungen zur Information der betroffenen Haushaltsmitglieder geschaffen hat, obwohl durch die materiellen Zweckbegrenzungen in § 21g EnWG ein ordnungsrechtlich strukturiertes Konzept denkbar wäre. Eine zumindest partielle Umsetzung des Transparenzgebotes im Wege des für die Phase der Erhebung in § 4 Abs. 2 BDSG normierten Mitwirkungsaktes des jeweils Betroffenen scheidet aus Gründen der Praktikabilität und der fehlenden Option der Durchsetzung im SmartHome wohl ebenfalls aus[33]. Denn hier treffen Grundprämissen des SmartHomes, neue Assistenzfunktionen und Dienste vom Nutzer unbemerkt zu realisieren, und die gesetzlichen Schutzfunktionen geradezu diametral aufeinander.

c) Erlaubnistatbestände

Die gesetzlichen Erlaubnistatbestände zur Erhebung und Verwendung der Inhaltsdaten der Sensorik ergeben sich im Innenbereich des SmartHomes regelmäßig aus § 28 BDSG. Für den privaten Technikgestalter ist insbesondere das Prinzip der Erforderlichkeit maßgeblich, welches eine Verwendung der vorhandenen Sensordaten in der Regel stark begrenzen wird. Allerdings wird bei Nutzung von Komplettlösungen [2] der verantwortliche private Betreiber schon keinen Einfluss auf die Qualität und Quantität der Inhaltsdaten haben. Hinzu kommt, dass der Komplettlösungsanbieter seinen Sitz in einem Drittstaat mit abweichenden Datenschutzstandards haben könnte. Hier kann sich bereits die Verwendung solcher Standardkomponenten aufgrund ihrer mangelnden Steuerungsfähigkeit im Hinblick auf die erfassten und ausgewerteten Daten als Hindernis für die Implementierung einer Lösung erweisen, welche eine Begrenzung auf das Erforderliche vorsieht und insofern einen zulässigen Betrieb nach § 28 BDSG erlaubt.

29 Vgl. Jacobson/Smetters/Thornton et al., Networking Named Content, CoNEXT ,09, Proceedings of the 5th international conference on Emerging networking experiments and technologies, S. 1, 6 f.

30 Siehe hierzu z.B. Bizer, DuD 2007, 350, 353 f.; Wolff in: Wolff/Brink, BeckOK Datenschutzrecht, IX. Rn. 43 f.; Sokol in: Simitis, Bundesdatenschutzgesetz, § 4 Rn. 39.

31 Vgl. Wolff, in: Wolff/Brink, BeckOK Datenschutzrecht, IX. Rn. 43 f.

32 Roßnagel/Jandt, Datenschutzfragen eines Energieinformationsnetzes, S. 39; Raabe/Lorenz/Pallas/Weis, Datenschutz in Smart Grids, S. 45.

33 Siehe zu dieser Diskussion im Zusammenhang mit Smart Metern, allerdings nicht im Innenbereich ULD , Datenschutzrechtliche Bewertung des Einsatzes von „intelligenten“ Messeinrichtungen für die Messung von gelieferter Energie (Smart Meter), S. 4 ff.; Roßnagel/Jandt, Datenschutzfragen eines Energieinformationsnetzes, S. 35 f.; Wiesemann, MMR 2011, 355, 358.

Für den Fall der Verwendung der Sensorik zur Erfassung von Gesundheitsdaten [2] sind auch im Innenbereich gegenüber dritten Personen im Haushalt durch den privaten Technikbetreiber grundsätzlich § 28 Abs. 6-8 BDSG zu berücksichtigen, welche besondere Arten personenbezogener Daten (§ 3 Abs. 9 BDSG) betreffen. Die gesetzliche Erlaubnis dürfte hier auch in „innerfamiliären Beziehungen“ grundsätzlich begrenzend wirken. Sachgerecht ist es hier, die informierte Einwilligung der weiteren Haushaltmitglieder nach § 4a BDSG als alleinige Legitimationsgrundlage in Betracht zu ziehen.

Hinsichtlich der Verwendung der Verkehrsdaten verbleibt es bei der bereits beschriebenen Schutzlücke[34] und dementsprechend bei einem Fehlen der notwendigen Erlaubnistatbestände für diesbezügliche Datenverwendungen. Diesem Umstand könnte allenfalls durch Einwilligungen nach § 4a BDSG analog abgeholfen werden. Dies gilt ebenso für die Verwendung von ortsbezogenen Informationen in Sachgestaltung [2]. Zudem verbleibt es auch bei Datenkategorien, die in klassischer Sicht dem TK-Recht zugeordnet sind, grundsätzlich bei einer Begrenzung auf das Erforderliche, was die Vielzahl der zwar technisch möglichen, aber zweckspezifisch nicht erforderlichen Datenverwendungen deutlich begrenzt. Eine erste Andeutung über de lege ferenda sinnvolle neue bereichsspezifische gesetzliche Erlaubnisse und Begrenzungen dieser Datenverwendungen findet sich in § 21g Abs. 3 EnWG. Dieser bestimmt unter Beachtung der Verhältnismäßigkeit die zulässigen Zwecke und das Verfahren hinsichtlich der Verwendung von Verkehrsdaten, welche bei der Nutzung von Smart Metern anfallen[35]. Die dort adressierten Verkehrsdaten dürfen dann verwendet werden, wenn „tatsächliche Anhaltspunkte für die rechtswidrige Inanspruchnahme eines Messsystems oder seiner Dienste vorliegen“. Eine vergleichbare Kategorie von im Wege der Vorabwägung durch den Gesetzgeber aus Gründen der Verkehrsfähigkeit anzuerkennenden Verwendungszusammenhängen und Verfahrenssicherungen in Bezug auf die Verkehrsdaten könnte im SmartHome für sicherheitskritische Überwachungsmechanismen und vergleichbar regelmäßige Aktivitäten gesetzlich geregelt werden, ohne die telekommunikationsrechtlichen Regelungen zu überladen. Schließlich ist im Hinblick auf die grundsätzliche Fähigkeit insbesondere softwareterminierter Sensorik und Gerätessteuerung [2] und der Option rein algorithmischer Entscheidungsfindung und -durchsetzung noch als Besonderheit anzumerken, dass das Verbot automatisierter Einzelentscheidungen aus § 6a BDSG von seinem Anwendungsbereich hier grundsätzlich eröffnet und auch vom privaten Technikgestalter zu berücksichtigen ist.

d) Datensparsamkeit

Eng verknüpft mit der Erforderlichkeit einer Datenverwendung im SmartHome ist auch das Gebot der Datensparsamkeit in § 3a BDSG. Dieses ist ebenfalls vom privaten Technikgestalter der klassischen Hausautomatisierung [1] zu berücksichtigen. Dies spiegelt sich auch im Hinblick auf die Auswahl von proprietären Standardkomponenten in Sachgestaltung [2] wieder, bei denen der private Technikgestalter eine Auswahlentscheidung zwischen verschiedenen Angeboten zu treffen hat. Ebenso trifft ihn die Obliegenheit zur Anonymisierung und Pseudonymisierung der Daten auf allen technischen Schichten, was ebenfalls durch eine geeignete Auswahl der verwendeten Standardkomponenten erfüllbar ist.

e) Datensicherheit

Grundsätzlich trifft den privaten Technikgestalter als „Verantwortliche Stelle“ gegenüber Dritten im Haushalt auch die Verantwortlichkeit für die Datensicherheit, also insbesondere für technische und organisatorische Maßnahmen nach § 9 BDSG. Hier ist den Herstellern von standardisierten Lösungen [2] zu empfehlen, die entsprechenden Informationen und Prüfungen schon in ihre Vertriebsspezifikationen aufzunehmen, da die notwendigen schichtspezifischen Bedrohungsanalysen hinsichtlich der Sensoren, Angreifertypen und Schutzgüter nicht vom einzelnen privaten Technikgestalter durchgeführt werden können. Exemplarisch können hier die Spezifizierungskriterien des BSI aus Schutzprofilen und technischen Richtlinien herangezogen werden, die in Bezug auf die Innenkommunikation im Home Area Network (HAN) schon die relevanten Perspektiven zeigen[36].

3. Besonderheiten der Außenschnittstellen

a) Anwendbares Recht

Hinsichtlich der Außenschnittstellen im SmartHome ist im Fall der einfachen privaten Hausautomatisierung [1] noch keine datenschutzrechtliche Besonderheit bezüglich der Verantwortlichkeiten und relevanten Datenkategorien zu verzeichnen. Aus Netzwerkperspektive bleibt es bei den klassischen Netzgrenzen, die das Schutzregime für den TK-Provider in der Regel bis zum Router terminiert.

Nichts anderes gilt de lege lata für die Anwendbarkeit der datenschutzrechtlichen Normierungen des TKG, auch wenn sich, wie z.B. im Falle der Adressierbarkeit von Endgeräten im Hausbereich über IPv6 [2], die Grenzen des öffentlichen Netzes in den Privatbereich verschieben. Problematisch ist, inwiefern sich wegen der feingranularen Auflösung, z.B. des Interaktionsverhaltens der Sensorik mit Diensten im öffentlichen Netz, die relevanten Ermächtigungen zum Speichern von Verkehrsdaten und die korrespondierenden staatlichen Überwachungsoptionen noch in den grundrechtlichen Grenzen ausgestalten lassen. Dies gilt umso mehr bei einem Wandel der Adressierungsschemata für Sensorik und Steuerung zu einem inhaltsbezogenen Routing von Informationen[37]. Hier kann schon aus dem Namensschema des Verkehrsdatums unmittelbar auf die angefragten Inhalte geschlossen werden[38]. Für den

34 Siehe IV.1.c).

35 Vgl. Lorenz/Raabe, in: Säcker, Energierecht, § 21g Rn. 64 ff.

36 BSI, SMGW-PP; BSI, TR-03109-1.

37 „Content-Centric Networking“; siehe hierzu Jacobson/Smetters/Thornton et al., Networking Named Content, CoNEXT ,09, Proceedings of the 5th international conference on Emerging networking experiments and technologies, S. 1.

38 Vgl. Jacobson/Smetters/Thornton et al., Networking Named Content, CoNEXT ,09, Proceedings of the 5th international conference on Emerging networking experiments and technologies, S. 1, 6 f.

Bereich des Smart Metering liegt in materieller Hinsicht mit der Regelung des § 21g Abs. 1 Nr. 8 i.V.m. Abs. 3 EnWG bereits eine bereichsspezifische Erlaubnisnorm vor, welche die Verwendung der Verkehrsdaten aus dem SMGW hinreichend bestimmt und verhältnismäßig auf die Fälle der Leistungserschleichung begrenzt[39]. Die Schaffung einer solchen telekommunikationsrechtlichen Norm im materiellen Energiewirtschaftsrecht stellt indes eine Besonderheit dar. Der Erlass einer solchen Regelung wäre aber z.B. auch für den Fall von Gesundheitsdaten eine denkbare Option.

b) Kommunikationsparadigma

Im Hinblick auf die Außenschnittstelle haben die in den Routern, adressierbaren Sensoren oder Verarbeitungseinheiten eines SmartHome [2] zum Einsatz kommenden Kommunikationsparadigmen Auswirkungen auf die Frage der einschlägigen datenschutzrechtlichen Normierungen des BDSG. Konkret geht es um die Frage, ob die Kommunikation der Inhaltsdaten mittels Push- oder Pull-Verfahren umgesetzt wird.

i) „Push“

Die datenschutzrechtlichen Verantwortlichkeiten knüpfen z.B. etwaige Mitwirkungsakte und Informationspflichten für Dritte nach § 4 BDSG an die Erhebung der Inhaltsdaten an. Da die Legaldefinition des Erhebens das Beschaffen von Daten über den Betroffenen, mithin ein aktives Handeln der verantwortlichen Stelle, voraussetzt[40] und jene Daten, die der verantwortlichen Stelle „zuwachsen“, nicht erhoben sind[41], können die Verantwortlichkeiten für die Einhaltung der datenschutzrechtlichen Verpflichtungen bei Dienstangeboten von Komplettlösungsanbietern [2], die z.B. eine internetbasierte Auswertung der Sensordaten über proprietäre Apps erlauben, in Frage stehen. In bestehenden Systemen ist dieses Paradigma sogar technisch vorgegeben, da keine Möglichkeit der direkten Adressierbarkeit von Endgeräten besteht. Aus Gründen der Datensicherheit erscheint dieses Verfahren vorzugswürdig, da bei Push-Betrieb ein (unbemerkter) Außenzugriff nicht möglich ist. Deshalb wurde dieses Paradigma für die Spezifikation des SMGW durch das BSI gewählt. Allerdings sind im Fall des SMGW eine Reihe von verfahrensrechtlichen und materiellen Begleitmaterien, wie die vorgängige Einwilligung in das Fernmessen nach § 21g Abs. 6 S. 5 EnWG, bereichsspezifisch normiert, für die es keine Entsprechung in den allgemeinen Regelungen des BDSG gibt. Insofern ist es zur Vermeidung von Schutzlücken de lege ferenda angezeigt, jedenfalls für Sachmaterien, wie die Auswertung von Gesundheitsdaten, eine entsprechende Regelung zu treffen.

ii) „Pull“

Beim Pull-Betrieb, also dem Abruf der Inhaltsdaten durch einen internetbasierten Dienst direkt von der Sensorik oder einem Vermittlungsrechner, verbleibt es bei den annoncierten Bedenken zur Datensicherheit. Im Falle der Steuerung von Heimgeräten über das Internet ist die Verwendung eines Pull-Verfahrens allerdings unumgänglich, da nur so eine sinnvolle Echtzeitkommunikation aufgebaut werden kann. Dem hat das BSI für den Energiebereich in seinen Schutzprofilen insofern Rechnung getragen, als ein kryptographisch gesicherter Tunnel zwischen Messsystem und externem Datenverarbeiter vorgegeben wird. Die zur Transparenzsicherung für den Betroffenen erforderlichen Mitwirkungsakte werden in diesem Fall ebenfalls durch vorgelagerte Einwilligungslösungen bereichsspezifisch normiert. De lege ferenda bedarf es nach Vorgesagtem entweder einer allgemeinen Verfahrensregelung zum Schnittstellendesign im BDSG oder einer bereichsspezifischen Ausprägung z.B. für den Fall von Gesundheitsdaten.

iii) Kommunikationsparadigma des SMGW

In diese Richtung weist auch die Begründung zur MsysV-E, welche die Verwendung des SMGW zu weiteren Zwecken explizit adressiert. Als Beispiel werden Anwendungen im Bereich des betreuten Wohnens[42] und somit tendenziell auch aus dem Gesundheitsbereich genannt. Ein Vorteil, der sich bei der Verwendung dieses Konzeptes auch für Gesundheitsdaten ergeben könnte, ist die Einführung der Rolle des Gateway Administrators[43]. Dieser überwacht als neutraler Dritter, wer in welcher Weise mit dem SMGW kommuniziert, da nur er Konfigurationen an den hinterlegten Kommunikationsprofilen vornehmen kann[44]. Diese Konfigurationen sind für den Betroffenen ersichtlich, wodurch ein Missbrauch des SMGW erschwert wird.

4. Besonderheiten im „Außenbereich“ (Internet)

a) Private Hausautomatisierung

i) Personenbezug und Gefahren

Im Außenbereich wird die Gefahr eines scherwiegenden Eingriffs in das informationelle Selbstbestimmungsrecht durch eine für den Betroffenen unsichtbare Bildung von Personenprofilen und der Möglichkeit unentdeckter Zweckänderungen offenbar. Der private Technikgestalter kann eine entfernte Überwachung der betroffenen Haushaltsmitglieder realisieren [2], die in jedem Falle jenseits einer Privilegierung durch § 1 Abs. 2 Nr. 3 BDSG angesiedelt ist. Dritte Dienstanbieter [2] wiederum können aus Verkehrsdaten, 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.

ii) Verantwortliche Stelle

Beim Betrieb der Dienstarchitektur durch den privaten Technikgestalter [1] verbleibt es bei seiner Verantwortlichkeit für die datenschutzrechtlichen Obliegenheiten. Sofern ein Anbie-

39 Vgl. Lorenz/Raabe, in: Säcker, Energierecht, § 21g Rn. 64 ff.

40 Dammann, in: Simitis, Bundesdatenschutzgesetz, § 3 Rn. 102.

41 Dammann, in: Simitis, Bundesdatenschutzgesetz, § 3 Rn. 104; Gola/Schomerus, BDSG, § 3 Rn. 24.

42 MsysV-E, S. 20.

43 Siehe insb. § 7 MsysV-RefE; zur Rolle des Gateway Administrators Wiesemann, ZD 2012, 447, 449.

44 BSI, TR-03109-1, S. 21.

ter von proprietären Gesamtlösungen in Frage steht [2], kumuliert die datenschutzrechtliche Verantwortlichkeit derzeit in dieser Rolle. So bleiben die Kategorien der telemedienrechtlich relevanten Daten im exklusiven Verantwortungsbereich des externen Dienstleisters. Des Weiteren ist in diesem Zusammenhang noch die mögliche Verarbeitung der Daten in Drittstaaten nach § 4b BDSG oder die Verwendung von Cloud-Dienstleistungen denkbar, die komplexe, grenz- und regulierungsregimeüberschreitende Mehrpersonenverhältnisse von Verantwortlichkeiten und verfahrensrechtlichen Obliegenheiten generieren können[45].

iii) Auftragsdatenverarbeitung

Für Grenzfälle, wie z.B. zusammengesetzte Dienstangebote[46], muss hinsichtlich der tatsächlichen Möglichkeit der Durchsetzung datenschutzrechtlicher Pflichten in Bezug auf die Inhaltsdaten und deren Verwendung grundsätzlich auch die Option der Auftragsdatenverarbeitung nach § 11 BDSG in Betracht gezogen werden. Hat der private Technikgestalter als verantwortliche Stelle z.B. faktisch keine Einflussmöglichkeit auf eine Datenverarbeitung auf fremden Servern, so wird er zukünftig, jedenfalls in den Fällen, in welchen den Serverbetreiber hinsichtlich spezifischer Datenkategorien keine eigenen Verantwortlichkeiten treffen, die Sicherung der informationellen Selbstbestimmung der Betroffenen im Haushalt im Wege der Vereinbarung einer Auftragsdatenverarbeitung sicherstellen müssen. Für dedizierte Anwendungskategorien könnten sich hier, entsprechend dem Gedanken, der Standardvertragsklauseln zugrunde liegt, vereinheitlichte Klauseln als hilfreich erweisen.

b) Smart Metering

Für die Sachgestaltung der staatlich verordneten Technikgestaltung [3] ist in Bezug auf den Außenbereich bezeichnend, dass im Energiesektor der technische Datenschutz nur produktbezogen[47] etabliert wurde, obwohl die im Außenbereich durchzuführenden Geschäftsprozesse weitgehend verbindlich festgelegt[48] und somit bekannt sind. Sobald die Daten das SMGW verlassen haben, endet der konkretisierend untergesetzlich ausgestaltete technische Datenschutz weitestgehend. In Bezug auf das weitere potentielle Einsatzfeld der Gesundheitsdaten[49] erscheinen jedoch lediglich produktbezogene Schutzmaßnahmen nicht ausreichend, da sich die Gefahranlage gerade im Hinblick auf eine mögliche zweckentfremdete Verwendung oder eine nicht vorgesehene Kombination der Daten im Außenbereich zeigt. Insbesondere sind in diesen Fällen jedoch, anders als beim Smart Metering, die konkreten Verwendungszwecke und Kontexte der Datenverwendung nicht bekannt. Für eine Nutzung des SMGW im bereits adressierten und aus Datenschutzsicht besonders relevanten Bereich der Gesundheitsdaten bedürfte es daher wohl expliziter bereichsspezifischer Regelungen zur Technikgestaltung und zu den zulässigen Verarbeitungsschritten. Gleichwohl würde es derzeit im Außenbereich bei einer Verwendung des SMGW für diese Sachgestaltung bei den gegenwärtig bestehenden datenschutzrechtlichen Verantwortlichkeiten verbleiben.

V. Grundrechtliche Relevanz möglicher Überwachungsmaßnahmen

Mit den mittels SmartHome-Anwendungen generierten Daten ist es schließlich möglich, Überwachungsmaßnahmen durchzuführen, welche nicht zuletzt zu Zwecken der Strafverfolgung dienen können. Vorhandene Daten lassen naturgemäß auch das Interesse einer zweckfremden Nutzung wachsen. Wie im Bereich des Smart Metering[50], ist es insofern notwendig, eine grundrechtlich motivierte Debatte zu führen, inwiefern Daten aus solchen Systemen zweckentfremdet für Überwachungsmaßnahmen verwendet werden dürfen, wobei hier nur auf einige insofern wesentliche Aspekte hingewiesen werden soll.

Neben dem Recht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG sind im Zusammenhang mit SmartHome-Anwendungen die bereits im Zusammenhang mit Smart Metern diskutierten Grundrechte[51] der Unverletzlichkeit der Wohnung aus Art. 13 GG und der Vertraulichkeit und Integrität informationstechnischer Systeme aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG zu nennen. Anders als in Fällen der reinen Stromverbrauchsmessung mittels Smart Metering[52] könnte in SmartHome-Sachgestaltungen insbesondere das Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme betroffen sein, da es sich hier nicht nur um die Erfassung einer Datenkategorie, sondern um die Erfassung einer Vielzahl durch Sensorik generierter Daten handelt[53]. Das BVerfG hat explizit ausgeführt, dass das Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme nicht in Fällen der *„nicht vernetzte[n] elektronischen Steuerungsanlagen der Haustechnik“* greift[54], was vorliegend der Sachgestaltung [1] entsprechen würde. Für Fälle vernetzter Haustechnik, wie in Sachgestaltung [2], könnte sich hingegen etwas anderes ergeben, da nicht mehr nur Daten *„mit punktuellem Bezug zu einem bestimmten Lebensbereich“*[55] erfasst werden. In Bezug auf das Grundrecht der Unverletzlichkeit der Wohnung stellen sich insbesondere Fragen wie z.B., ob erfasste Bewegungen innerhalb eines Haushaltes bereits mit visuellen Überwachungsmaßnahmen vergleichbar sind[56]. Diese und weitere grundrechtlich motivierte Fragen gilt es künftig zu beantworten.

45 Vgl. Balaban/Pallas, DSRI Tagungsband 2013, 325; zur Drittstaatenproblematik Brennscheidt, Cloud Computing und Datenschutz, S. 159 ff.

46 Siehe Balaban/Pallas, InTeR 2013, 193.

47 Vgl. Raabe/Lorenz/Pallas/Weis, CR 2011, 831, 839.

48 Siehe insb. BNetzA, Beschluss BK6-06-009 und BNetzA, Beschluss BK6-09-034.

49 MsysV-E, S. 20.

50 Hornung/Fuchs DuD 2012, 20; Guckelberger, DÖV 2012, 613, 619 ff.; Göge/Boers ZNER 2009, 368.

51 Siehe Hornung/Fuchs DuD 2012, 20; Guckelberger, DÖV 2012, 613, 619 ff.; zu Art. 13 GG auch Göge/Boers ZNER 2009, 368, 369 f.

52 Das Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme in diesem Bereich ablehnend Hornung/Fuchs DuD 2012, 20, 23; Guckelberger, DÖV 2012, 613, 321.

53 Bejahend Guckelberger, DÖV 2012, 613, 620 für den Fall der Vernetzung weiterer elektronischer Geräte.

54 BVerfG NJW 2008, 822, 827.

55 BVerfG NJW 2008, 822, 827.

56 Für den Bereich des Smart Meterings ablehnend Guckelberger, DÖV 2012, 613, 620, sowie Göge/Boers ZNER 2009, 368, 369, allerdings noch unter anderen Annahmen.

VI. Fazit

Hinter dem Begriff SmartHome verbergen sich eine Reihe von technischen, ökonomischen und gesellschaftlichen Wandlungen. Bei einer systematisierenden Betrachtung lassen sich die für eine differenzierte datenschutzrechtliche Analyse notwendigen ökonomischen und sozialen Treiber identifizieren und technische Grundparadigmen eingrenzen, die allen Sachgestaltungen innewohnen. Herausforderungen aus datenschutzrechtlicher Sicht ergeben sich insbesondere für das Transparenzprinzip mit seinen vorhandenen Ausprägungen und dem Verschwimmen der Grenzen des klassischen Schichtenparadigmas aus rechtlicher Sicht durch neue Formen der Objektadressierung. Letztere führt dazu, dass zukünftig keine eindeutige Zuordnung der Datenkategorien und Verantwortlichkeiten im SmartHome nach der bestehenden Dreiteilung von anwendungsbezogenem Inhaltsdatenschutz, telemedienrechtlichen Obligationen und dem transportbezogenen Telekommunikationsrecht mehr vorgenommen werden kann. Der Gesetzgeber ist daher zu einer Generalrevision berufen, wofür sich erste Ansätze einer regulatorischen Konzeption in der modernen Technikregulierung des novellierten EnWG finden.

Dr. Oliver Raabe
Dr. Oliver Raabe ist Leiter der Forschungsgruppe „Compliance“ am Zentrum für Angewandte Rechtswissenschaft am Karlsruher Institut für Technologie (KIT). Er beschäftigt sich schwerpunktmäßig mit informationsrechtlichen Fragen im Zusammenhang mit neuen IT-Trends. Insbesondere stehen Themen wie Smart Energy, Cloud Computing und Big Data in seinem Fokus. Einen weiteren Kernpunkt seiner Tätigkeit nimmt die Rechtsinformatik ein.

Eva Weis
Eva Weis ist akademische Mitarbeiterin in der Forschungsgruppe „Compliance“ am Zentrum für Angewandte Rechtswissenschaft am Karlsruher Institut für Technologie (KIT). Sie beschäftigt sich schwerpunktmäßig mit rechtlichen Fragen künftiger intelligenter Energiesysteme und der Etablierung von Elektromobilität. In diesem Bereich hat sie kürzlich auch ihr Promotionsverfahren abgeschlossen. In ihrem Fokus steht neben den informationsrechtlichen Aspekten insbesondere das Energierecht.

Sascha Kremer

Connected Car – intelligente Kfz, intelligente Verkehrssysteme, intelligenter Datenschutz?

Im Kfz von heute werden fortlaufend nicht nur Zustand und Umgebung des Fahrzeugs, sondern auch das Verhalten des Fahrers aufgezeichnet und ausgewertet. Es kommuniziert außerdem mit seiner Umgebung, um auf überfüllte Straßen oder Gefahrenquellen hinzuweisen oder zu reagieren, und sorgt selbständig für einen energieeffizienten Fahrverlauf. Intelligente Verkehrssysteme und hierauf basierende Anwendungen und Dienste fordern insbesondere das Datenschutzrecht heraus. Dieser Beitrag dient der Bestandsaufnahme zum Stand der Technik und der datenschutzrechtlichen Bewertung des Umgangs mit personenbezogenen Daten im „Connected Car“.

1. Einführung

„Was wir nicht wollen, ist der gläserne Autofahrer, für den Bewegungsprofile erstellt und Daten über den Fahrstil gesammelt werden“, so Bundesjustiz- und Verbraucherschutzminister Maas im Juli 2014[1], der damit eine Forderung des früheren Bundesbeauftragten für den Datenschutz Schaar aus dem Jahr 2006 wiederholt hat[2]. Dabei sind intelligente Verkehrssysteme und deren Auswertung mittels Big Data[3] längst Realität. Der Autobahnschütze, der jahrelang aus „Frust im Straßenverkehr“ auf Lastwagen geschossen hat, konnte erst durch die Auswertung und den Abgleich von Daten aus Kfz-Kennzeichen-Scannern, Mobilfunkstationen und seinem elektronischen Fahrtenschreiber ermittelt werden[4].

Bereits 2012 hielten in einer Verbraucherumfrage zum „Auto der Zukunft“ 76% der Befragten Fahrassistenten und intelligente Navigation für wichtig oder sehr wichtig, 48% eine integrierte Kommunikation und immerhin 39% eine „Vernetzung

1 Http://www.cio.de/news/wirtschaftsnachrichten/2962888/.

2 Pressemitteilung des Bundesbeauftragten für den Datenschutz Nr. 13/06 v. 28.3.2006 = MMR 2006, VI.

3 Zum Datenschutz bei Big Data Ehmann, K&R 2014, 394; Mielchen, ITRB 2014, 110; Bornemann, RDV 2013, 232; Schaar, RDV 2013, 223; Ulmer, RDV 2013, 227; Roßnagel, ZD 2013, 562.

4 Http://www.spiegel.de/panorama/justiz/prozess-gegen-autobahnschuetzen-anwaelte-kritisieren-ermittlungsmethode-a-986176.html.

mit Zuhause“[5]. Dabei wünschten sich 53% der Befragten ausdrücklich Fahrhilfen, die auf „Car to Car“ Kommunikation beruhen[6]. Es verwundert deshalb nicht, dass das „Connected Car“ einer der Treiber von Forschung und Entwicklung bei Kfz ist[7] und „Connectivity“ als entscheidender Meilenstein der gesamten Automobilindustrie angesehen wird[8].

Dieser Beitrag fasst zunächst den Stand der Technik zusammen und beschreibt den Umgang mit Daten im und aus dem Kfz (Ziff. 2). Es folgen allgemeine datenschutzrechtliche Erwägungen (Ziff. 3), in deren Mittelpunkt der Personenbezug der im und aus dem Kfz gewonnenen Daten und das hierauf anwendbare Datenschutzrecht stehen. Anschließend werden verschiedene Anwendungsfälle aus der Praxis und deren Rechtmäßigkeit untersucht (Ziff. 4), bevor auf weitere Herausforderungen bei Anwendungen und Diensten intelligenter Verkehrssysteme (Ziff. 5) eingegangen wird. Der Beitrag endet mit einem Fazit und Empfehlungen des Autors (Ziff. 6).

2. Stand der Technik

Der Begriff „Connected Car“ legt die Vermutung nahe, dass sich das Intelligente auf die Vernetzung von Kfz im Straßenverkehr beschränkt. Tatsächlich sind jedoch nicht nur die Kfz, sondern auch die umgebenden Verkehrssysteme intelligent. Kfz und Verkehrssysteme sind wiederum an vorhandene technische Infrastrukturen angeschlossen, z.B. im Unternehmensfuhrpark, in der öffentlichen Notfallvorsorge, bei den Herstellern oder in der „Cloud“. Deshalb geht es nach dem Stand der Technik[9] tatsächlich um eine Kommunikation mittels und über die im jeweiligen System erhobenen oder gespeicherten Daten von Kfz zu Kfz (C2C = „Car to Car“), Kfz zur Verkehrssystemen als infrastrukturelle Einrichtungen (C2I = „Car to Infrastructure“) und Kfz zu anderen Systemen (C2X = „Car to Anything“) – selbstverständlich auch in die jeweils umgekehrte Richtung[10].

2.1 Sensoren im Kfz

In Kfz erfolgt die Erhebung von Daten durch Sensoren[11]. Diese beziehen sich auf das Kfz, dessen Umgebung sowie die Insassen und deren Tun. Die Sensoren werden entweder von den Herstellern bei der Fertigung oder nachträglich von Dritten wie Arbeitgeber oder Flottenbetreiber mittels Telematik-Boxen (zum Begriff Telematik unten Ziff. 2.3) im Kfz angebracht.

Im Kfz selbst werden, abhängig von Hersteller, Modell und Ausstattung, fortlaufend u.a. Achslast, Motorbelastung, Reifendrehzahl, Reifendruck, Temperatur, Querbeschleunigung, Geschwindigkeit, Glasbruch und Verformungen überwacht. Hinzu kommen Sensoren im Bremssystem (ABS), der elektronischen Stabilitätskontrolle (ESP), der Beleuchtung des Pkw und in den verschiedenen Motoren (etwa zum Öffnen von Fenstern oder Zuziehen von Heckklappen). Zudem wird die Umgebung über Kamera- und Radarsysteme überwacht[12].

Die auf die Insassen bezogenen Sensoren erfassen zunächst äußerliche Merkmale, etwa die Sitzbelegung über das auf den Sitz ausgeübte Gewicht und das Schließen des Sicherheitsgurtes oder die Aufmerksamkeit des Fahrers, die mittels (unangekündigter) Spurwechsel, der Dauer einer nicht durch Pausen unterbrochenen Fahrt, den Geradeauslauf des Kfz oder zukünftig mittels Erfassung der Augenbewegung durch Kameras im Innenraum beurteilt wird. Hinzu treten zunehmend medizinische Sensoren zur unmittelbaren Messung von Körperfunktionen des Fahrers, z.B. seines Atemalkoholgehalts (z.B. Volvo Alcolock)[13], seiner Herzfunktionen (etwa Ford SYNC)[14] oder seiner psychischen Verfassung[15].

Die mit den Sensoren erhobenen Daten *(zu deren Personenbeziehbarkeit unten Ziff. 3.2)* werden sodann Fahrer und ggf. Insassen zugänglich gemacht, um diesen mit Fahrassistenzsystemen[16] z.B. auf Gefahrensituationen oder die Verkehrslage hinzuweisen, zur Steuerung des Kfz genutzt, etwa um die Bremskraft richtig zu dosieren und ein Ausbrechen des Kfz zu verhindern, oder von den Herstellern für die Diagnose von Störungen herangezogen. So ist kürzlich über den ADAC ein Fall bekannt geworden, in dem die Beseitigung eines während der gesetzlichen Mängelhaftung aufgetretenen Schadens unter Hinweis auf die vom Sensor aufgezeichnete Überschreitung der zulässigen Last auf der Hinterachse abgelehnt worden[17].

2.2 Intelligente Verkehrssysteme

Der Begriff intelligente Verkehrssysteme geht auf die Richtlinie 2010/40/EU vom 7.7.2010 zum Rahmen für die Einführung intelligenter Verkehrssysteme im Straßenverkehr und für deren Schnittstellen zu anderen Verkehrssystemen *(IVS-RL)*[18] sowie dem 2013 zur Umsetzung in nationales Recht verabschiedeten Gesetz über Intelligente Verkehrssysteme im Straßenverkehr und deren Schnittstellen zu anderen Verkehrsträgern (*IVSG*)[19] zurück.

5 Ernst & Young, Verbraucherumfrage März 2012, Seite 16: http://www.ey.com/Publication/vwLUAssets/Connected_Car_-_das_Auto_der_Zukunft_2012/$FILE/Connected%20Car%202012.pdf.

6 Ernst & Young, Verbraucherumfrage März 2012, Seite 21: http://www.ey.com/Publication/vwLUAssets/Connected_Car_-_das_Auto_der_Zukunft_2012/$FILE/Connected%20Car%202012.pdf.

7 Siehe das Leitprojekt „Connected-Car“ (http://www.imst.de/imst/de/forschung/connectedcar.php) und das Projekt „simtd – Sichere Intelligente Mobilität Testfeld Deutschland“ (http://www.simtd.de/index.dhtml/deDE/index.html).

8 So 2011 Elmar Frickenstein, BMW Bereichsleiter Elektrik/Elektronik: http://www.car-it.com/frickenstein-connectivity-wird-zum-meilenstein/id-0029485.

9 Definiert von Stiemerling als „die gegenwärtigen und künftigen technischen Möglichkeiten der elektronischen Datenverarbeitung“, CR 2012, 60 (64).

10 Schulz/Roßnagel/David, ZD 2010, 510, ergänzen dies noch um C2P = Car to Pedestrian (Fußgänger).

11 Grafische Darstellung verschiedener Sensoren im Fahrzeug unter http://www.kfztech.de/kfztechnik/elo/sensoren/sensoren.htm, von Umgebungssensoren am Beispiel der S-Klasse von Mercedes unter http://www.focus.de/auto/autoentwicklung/technik/auto-und-technik-autopilot-an-bord_id_3635914.html.

12 Zur Zulässigkeit sog. Dashboard-Cams siehe AG München, Urteil v. 6.6.2013 – 343 C 4445/13; VG Arnsbach, Urteil v. 12.8.2014 – AN 4 K 13.01634 mit Anmerkung Lachenmann/Schwiering, ZD-Aktuell 2014, 04300; ausführlich Atzert/Franck, RDV 2014, 136.

13 Http://www.shortnews.de/id/884387/volvo-verbaut-alcolocks.

14 Http://www.presseportal.de/print/2544042-s-max-concept-zeigt-die-moeglichkeiten-von-design-und-technologie-kommender.html.

15 Http://www.spiegel.de/spiegel/a-656024.html.

16 Zu Fahrassistenzsystemen Deutschle, SVR 2005, 249.

17 Bericht in ADAC Motorwelt, Ausgabe 7/2014.

18 Http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:207:0001:0013:DE:PDF.

19 Intelligente Verkehrssysteme Gesetz: http://www.gesetze-im-internet.de/ivsg/BJNR155300013.html.

Bei intelligenten Verkehrssystemen handelt es sich nach § 2 Nr. 1 IVSG um „Systeme, bei denen Informations- und Kommunikationstechnologien im Straßenverkehr und an Schnittstellen zu anderen Verkehrsträgern eingesetzt werden". „Anwendungen Intelligenter Verkehrssysteme" i.S.d. § 2 Nr. 2 IVSG sind sodann technische Systeme, Verfahren oder Geräte für den Einsatz intelligenter Verkehrssysteme, auf deren Grundlage sodann die „Dienste Intelligenter Verkehrssysteme" bereitgestellt werden. Entscheidend ist, dass Anwendungen und Dienste gemäß § 3 IVSG die sich aus der IVS-RL ergebenden Spezifikationen einhalten, insbesondere um die EU-weite Interoperabilität und Kompatibilität der Systeme zu gewährleisten. Dabei dienen intelligente Verkehrssysteme nach § 4 Nr. 4 IVSG insbesondere auch der „Verbindung zwischen Fahrzeug und Verkehrsinfrastruktur".

Das Kfz mit seinen Sensoren und der eingebauten Technik ist damit ein Bündel von Anwendungen intelligenter Verkehrssysteme, ebenso die umgebenden Einrichtungen, z.B. Parkleitsysteme, „kollektive Verkehrsbeeinflussungsanzeigen" (z.B. Matrixanzeigen über Autobahnen) oder Fernsteuerungen zur Ampelschaltung. Über diese Anwendungen wird wiederum eine Vielzahl von Diensten intelligenter Verkehrssysteme erbracht.

2.3 Kommunikation vom und zum Kfz

Die Kommunikation zwischen Kfz und Verkehrssystemen findet C2C, C2I/C2X und umgekehrt statt (*zu den Begriffen oben Ziff. 2*). Praktische Anwendungsfälle für die Kommunikation C2C sind Fahrassistenzsysteme und Abstandswarner (etwa zum Kolonnenfahren), für die Kommunikation C2I/C2X Verkehrssteuerungs- und Notrufsysteme, aber ebenso die Erfassung von Kfz- oder fahrerbezogenen Daten zur Bewertung des Fahrverhaltens z.B. durch den Arbeitgeber oder Versicherungen (*zu Telematik-Tarifen unten Ziff. 4.3*).

Wenn in diesem Zusammenhang von Telematik[20] gesprochen wird, meint dies nichts anderes. Denn Telematik ist „das Mittel der Informationsverknüpfung von mindestens zwei Informationssystemen mit Hilfe eines Telekommunikationssystems, sowie einer speziellen Datenverarbeitung",[21] also der abstrakte Oberbegriff für das, was bei der Kommunikation C2C und C2I/C2X geschieht.

2.4 Einbindung von Smart Devices im Kfz

Nicht mehr auf obere Mittelklasse und Oberklasse beschränkt sind die sog. „Infotainment-Systeme"[22] der Kfz-Hersteller. Standen dabei zunächst selbständige Systeme und Premiumdienste mit eigenen Apps im Kfz im Vordergrund[23], vollzieht sich derzeit ein Wandel hin zur Integration von Smart Devices wie Smartphones und Tablets[24] in die Intelligenz der Kfz.

Diese Integration geschieht auf Grundlage standardisierter Schnittstellen der Hersteller von Betriebssystemen solcher Smart Devices, insbesondere „CarPlay" von Apple[25] (Betriebssystem iOS) und „Android Auto" von Google[26] (Betriebssystem Android)[27]. Bereits 57 Automobilhersteller haben sich für eines dieser Systeme entschieden, wobei zwischen Apple und Google etwa Gleichstand herrscht[28]. Dabei führt die Integration nicht zu einer Einbahnstraße vom Smart Device zum Kfz: auch umgekehrt lassen sich Daten aus dem Kfz zur Nutzung in Apps auf dem Smart Devices übermitteln[29].

2.5 Autonome Kfz

Die in Kfz verbaute Intelligenz erlaubt grundsätzlich ein autonomes Fahren. Dieses beschränkt sich nicht mehr auf automatische Brems- und Parkassistenten, sondern erfasst auch die aktive Teilnahme am Straßenverkehr ohne steuernde Eingriffe oder Kontrolle eines Fahrers. Mercedes hat bereits 2013 eine selbstfahrende S-Klasse vorgestellt, und Volvo will bis 2017 die Selbstfahrtechnik optimieren[30]. Google arbeitet seit 2010[31] am autonomen „Google Car" und hat bereits mehr als eine Million unfallfreie Kilometer zurückgelegt[32], wobei noch unklar ist, ob Google selbst ein solches Fahrzeug herstellen oder nur Technologielieferant sein will. So sollen nach Schätzungen bis 2035 weltweit 35 Millionen autonome Kfz unterwegs sein[33].

Bislang verbot allerdings Art. 8 Abs. 2 des Wiener Übereinkommens über den Straßenverkehr vom 7./8.11.1968[34] autonome Kfz. Hiernach muss der Führer eines Fahrzeugs dieses „dauernd [...] beherrschen", was bei einem autonomen Kfz nicht der Fall ist. Erst mit einer u.a. auf Drängen von Deutschland beschlossenen Änderung vom Mai 2014 ist Art. 8 Abs. 2

20 Zum früheren Verständnis der Verkehrstelematik „Leitfaden Verkehrstelematik" des Bundesverkehrsministeriums von 2005: http://www.bmvi.de/SharedDocs/DE/Anlage/VerkehrUndMobilitaet/leitfaden-verkehrstelematik.pdf?__blob=publicationFile.

21 Definition von Nora/Minc, L'informatisation de la société: rapport à M. le Président de la République, 1978, zitiert nach Wikipedia: http://de.wikipedia.org/wiki/Telematik.

22 Zu Begriff und Technik http://de.wikipedia.org/wiki/Infotainmentsystem.

23 Beispielsweise „BMW ConnectedDrive" (http://www.bmw.com/com/de/insights/technology/connecteddrive/2013/connectivity_technologies/index.html), „Mercedes me" (https://www.mercedes.me/de/) oder „Audi connect" (http://origin-www.audi.com/de/brand/de/neuwagen/infotainment_und_kommunikation/audi_connect_dienste.html).

24 Zu Smart Devices und Datenschutz Kremer, CR 2012, 438; Kremer/Sander, ITRB 2012, 275; Lober, K&R 2013, 357; Art. 29 Gruppe, WP202, „Opinion 02/2013 on apps on smart devices" vom 27.2.2013: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf; Düsseldorfer Kreis, „Orientierungshilfe zu den Datenschutzanforderungen an App-Enwickler und App-Anbieter" vom 16.6.2014: http://www.lda.bayern.de/lda/datenschutzaufsicht/lda_daten/Orientierungshilfe_Apps_2014.pdf.

25 Https://www.apple.com/ios/carplay/.

26 Http://www.android.com/auto/.

27 Ein vom Betriebssystem unabhängiges System zur Integration von Apps in Kfz bietet Bosch mit MySpin an: http://www.bosch-softtec.com/myspin.html.

28 29 zu 28 Hersteller stand es im Juli 2014 zu Gunsten von Apple: http://www.heise.de/newsticker/meldung/Fahrzeugintegration-Apple-gegen-Google-bei-29-zu-28-2244427.html.

29 Das Fahren kann auch durch sog. „Wearables" (http://de.wikipedia.org/wiki/Wearable_Computing), etwa Google Glass (http://www.google.com/glass/start/), beeinflusst werden, wenn etwa die Navigationsanweisungen in einer Datenbrille unmittelbar vor dem Gesicht des Fahrers statt auf der hierfür vorgesehenen Anzeige im Kfz eingeblendet werden. Ob die Benutzung ggf. ein Verstoß gegen § 23 Abs. 1, Abs. 1a StVO ist, ist derzeit offen. Zu den Rechtsfragen von Google Glass Schwenke, K&R 2013, 685.

30 Http://www.handelsblatt.com/auto/test-technik/google-baut-eigenes-selbstfahrendes-auto-sieht-so-die-zukunft-des-autos-aus/9961054.html.

31 Http://googleblog.blogspot.de/2010/10/what-were-driving-at.html.

32 Zu den technischen Schwierigkeiten bei unbekannten oder baulich veränderten Wegstrecken http://www.heise.de/tr/artikel/Schlagloecher-Papierfetzen-und-andere-Probleme-2327769.html.

33 Http://www.handelsblatt.com/auto/test-technik/google-baut-eigenes-selbstfahrendes-auto-sieht-so-die-zukunft-des-autos-aus/9961054.html.

34 Http://www.admin.ch/opc/de/classified-compilation/19680244/index.html.

dahingehend ergänzt worden, dass autonomes Fahren dann zulässig ist, wenn der Fahrer das System jederzeit stoppen und selbst die Kontrolle übernehmen kann[35]. Ungeklärt ist jedoch weiterhin, wer für Schäden durch autonome Kfz haftet. Während § 7 Abs. 1 StVG für die verschuldensunabhängige Halterhaftung allein auf den Betrieb eines Kfz abstellt, worunter begrifflich auch ein autonomes Kfz fällt, stellt sich die Frage, ob eine verschuldensabhängige Haftung des Fahrers aus § 823 Abs. 1 BGB oder § 823 Abs. 2 BGB in Verbindung mit einem Schutzgesetz noch in Betracht kommt, wenn sich das Tun des Fahrers ausschließlich auf Starten des Kfz und Festlegung des Fahrziels beschränkt[36].

2.6 Speicherung von Daten im und über das Kfz

Die Erhebung der Daten aus den Sensoren im Kfz (*dazu oben Ziff. 2.1*) und den intelligenten Verkehrssystemen (d*azu oben Ziff. 2.2*) erfolgt unmittelbar im jeweiligen System. Dabei wird zwischen der flüchtigen, semiflüchtigen und beständigen Speicherung der erhobenen Daten unterschieden.

Flüchtig gespeicherte Daten werden unmittelbar nach ihrer Erhebung genutzt (z.B. für die Steuerung von Motoren im Kfz) und nur für die Dauer der Nutzung selbst gespeichert, anschließend aber sofort überschrieben oder gelöscht. Semiflüchtige Daten sind solche, die fortlaufend gespeichert, nach Ablauf einer bestimmten Zeitspanne ohne Eintritt eines besonderen Ereignisses aber wieder gelöscht oder überschrieben werden, etwa die von einer lediglich für die letzten x Sekunden vor einem Unfall gespeicherten Daten aus den einem Unfalldatenschreiber zugeordneten Sensoren. Beständig gespeicherte Daten werden dauerhaft im jeweiligen System abgelegt.

Ob und welche Daten flüchtig, semiflüchtig oder beständig gespeichert werden, ist von wenigen Ausnahmen abgesehen das Geheimnis des Herstellers oder Betreibers des jeweiligen Systems. Ebenso unklar ist häufig, ob die Daten ausschließlich im System gespeichert oder ergänzend/alternativ an externe Systeme übermittelt und gespeichert werden. So senden aktuelle Navigationsgeräte Daten über Standort, Fahrstrecke und Bewegungsgeschwindigkeit an zentrale Systeme der Anbieter, die hieraus Verkehrsinformationen in Echtzeit ermitteln, die wiederum an die Navigationsgeräte zur Optimierung der Routenplanung übermittelt werden. Entsprechendes gilt für Telematik-Boxen (*zum Begriff oben Ziff. 2.1 und 2.2*), die Daten über das Fahrverhalten an Dritte übermitteln, insbesondere Arbeitgeber und Flottenbetreiber, aber auch Versicherer, die auf Grundlage dieser Daten sodann die Routenplanung vornehmen, arbeitsrechtliche Sanktionen ergreifen oder Versicherungstarife ermitteln (*zu Telematik-Tarifen unten Ziff. 4.3*). Auch der EU-weite verpflichtende eCall-Dienst wird zu einer Übermittlung und externen Speicherung von Daten aus dem Kfz führen (*dazu unten Ziff. 4.2*).

3. Erwägungen zum Datenschutzrecht[37]

Im Kfz werden über die Sensoren (*dazu oben Ziff. 2.1*) und eingebundenen Smart Devices (*dazu oben Ziff. 2.4*) potentiell eine Unmenge von Daten erhoben und semiflüchtig oder beständig gespeichert (*dazu oben Ziff. 2.6*), die anschließend vom Fahrer selbst oder Dritten verwendet werden. Dabei stellt sich jeweils die Frage nach dem Personenbezug dieser Daten, dem hierauf anwendbaren Datenschutzrecht sowie der Art und Weise im Umgang[38] mit etwaigen personenbezogenen Daten.

3.1 Potentiell betroffene Daten

Potentiell sind in Kfz und intelligenten Verkehrssystemen insbesondere folgende Daten betroffen:

- Kennungen der Hardware des Kfz (z.B. die Fahrzeug-Identifizierungsnummer = FIN[39]),
- Daten zum Fahrverhalten (z.B. Beschleunigung, Geschwindigkeit),
- Bewegungs- und Positionsdaten,
- Bestands-, Verkehrs- und Standortdaten von Mobilfunkkarten,
- Benutzerzugangsdaten zu Bordsystemen oder externen, im jeweiligen System genutzten Diensten (Benutzername und Passwort, ggf. biometrische Informationen),
- während der Fahrt abgerufene oder erzeugte Inhalte (z.B. Kontakte oder Nachrichten des Fahrers),
- der sog. MSD-Datensatz beim eCall-Dienst (*dazu unten Ziff. 4.2*),
- Gesundheitsdaten von Fahrer und ggf. Insassen, sowie
- Zahlungsdaten zu Abrechnungszwecken bei der Nutzung von Anwendungen oder Diensten intelligenter Verkehrssysteme.

Diese Daten, die von der Bundesregierung in Daten für Fahrzeugfunktionen und Daten für Servicefunktionen unterteilt werden[40], können im Kfz oder externen Systemen von einer Vielzahl von Beteiligten mit anderen Daten aus dem Kfz oder externen Systemen kombiniert oder abgeglichen werden, so etwa die Angaben zur gefahrenen Geschwindigkeit mit einer Karte, welche die jeweils zulässige Höchstgeschwindigkeit ausweist. Der Kombinationsvielfalt und dem Vorstellungsvermögen sind dabei keine Grenzen gesetzt.

3.2 Personenbezug der Daten

Solange die oben genannten Daten anonym erhoben oder ausschließlich anonymisiert i.S.d. § 3 Abs. 5 BDSG verarbeitet und genutzt werden, sind intelligente Kfz und Verkehrssysteme datenschutzrechtlich ohne Bedeutung.

35 Http://www.welt.de/motor/news/article128190138/Autonomes-Fahren.html.

36 Zur bisherigen Forschung siehe die Ausführungen zu den Legal Issues im Projekt „AdaptiVe – Automated Driving“: http://adaptive-ip.eu/index.php/legal_issues.html.

37 Nicht Gegenstand dieses Beitrags ist die Bestandsaufnahme zum Umgang mit den aus intelligenten Kfz und Verkehrssystemen erhobenen personenbezogenen Daten zur Strafverfolgung. Die sich hieraus ergebenden Fragen werden in einem Folgebeitrag betrachtet.

38 Der Begriff des Umgangs mit personenbezogenen Daten wird in diesem Beitrag i.S.d. § 1 Abs. 1 BDSG als Oberbegriff für das Erheben, Verarbeiten und Nutzen personenbezogener Daten i.S.v. § 3 Abs. 3 bis 5 BDSG verwendet.

39 Http://de.wikipedia.org/wiki/Fahrzeug-Identifizierungsnummer.

40 BT-Drucksache 18/1362 v. 2.5.2014, S. 2: http://dipbt.bundestag.de/dip21/btd/18/013/1801362.pdf.

Fraglich ist jedoch, wann aus oder im Kfz erhobenen Daten tatsächlich anonym sind. Die Bundesregierung hat sich im Mai 2014 in ihrer Antwort auf eine kleine Anfrage vor einer Beantwortung genau dieser Frage gedrückt. Die Bundesregierung räumt in ihrer Antwort zwar ein, dass „technische Messdaten in Fahrzeugsteuergeräten […] zunächst nur personenbeziehbar" seien, will dies dann aber dadurch korrigiert sehen, „dass eine Verknüpfung mit der natürlichen Person des Fahrers unmittelbar" nicht erfolge[41].

Für § 3 Abs. 1 BDSG genügt es indes, wenn Daten einer bestimmbaren Person zugeordnet werden können, also personenbeziehbar sind. Diese Personenbeziehbarkeit liegt nicht nur dann vor, wenn die verantwortliche Stelle (*dazu unten Ziff. 3.4*) mit ihren Kenntnissen, Mitteln und Möglichkeiten den Personenbezug herstellen kann[42]. Vielmehr genügt es, wenn objektiv für einen beliebigen Dritten die Möglichkeit zur Herstellung des Personenbezugs besteht, gleich ob dies, so der Wortlaut des Entwurfs von Art. 4 Abs. 2 Allgemeine Datenschutzverordnung[43], „direkt oder indirekt" möglich ist[44]. Damit handelt es sich bei den Daten für Fahrzeugfunktionen ebenso wie bei den Daten für die ohnehin personalisierten Servicefunktionen (*dazu oben Ziff. 3.1*) um personenbezogene Daten i.S.d. § Abs. 1 BDSG, lassen sich diese doch durch den Fahrer selbst oder verschiedene Dritte, wie Hersteller, Werkstatt, Flottenbetreiber, Arbeitgeber oder Versicherung, ohne oder mit geringem Aufwand zumindest dem Halter, Fahrer oder Eigentümer des Kfz zuordnen[45]. Auch die weitere Relativierung in der Antwort der Bundesregierung, wonach die Personenbeziehbarkeit „im Einzelfall nur im Fall des Hinzutretens weiterer Ereignisse oder besonderer Umstände von Bedeutung (bspw. im Fall eines schweren Unfalls)" werde, sodass „die faktische Bedeutung einer Herstellung des Personenbezuges im Alltag der Fahrzeugnutzer eingeschränkt" sei[46], geht deshalb an der Rechtslage vorbei. Erklärlich ist dies aber, wenn man die Antwort der Bundesregierung vom März 2014 auf eine weitere kleine Anfrage auf die Frage kennt, wie verhindert werden könne, dass Bewegungsprofile oder Halterinformationen von Fahrzeugen ungehindert gespeichert und verarbeitet werden: „Die Bundesregierung hat diese Frage noch nicht vertieft geprüft."[47]

Auch die Aufsichtsbehörden scheinen bislang die Augen vor der Realität zu verschließen, worauf eine von diesen gemeinsam mit dem Verband der deutschen Automobilindustrie (VDA)[48] erstellte „Muster-Information über Datenspeicher im Fahrzeug"[49] hinweist. Dort wird ebenso wie in der Antwort der Bundesregierung eine Personenbeziehbarkeit der Daten über Fahrzeugfunktionen verneint: „Eine Vielzahl elektronischer Komponenten Ihres Fahrzeugs enthalten Datenspeicher, die technische Informationen über Fahrzeugzustand, Ereignisse und Fehler temporär oder dauerhaft speichern. […] Diese Daten sind ausschließlich technischer Natur und dienen der Erkennung und Behebung von Fehlern sowie der Optimierung von Fahrzeugfunktionen. […] Bei der Nutzung des Fahrzeugs sind Situationen denkbar, in denen diese technische Daten in Verbindung mit anderen Informationen (Unfallprotokoll, Schäden am Fahrzeug, Zeugenaussagen etc.) – gegebenenfalls unter Hinzuziehung eines Sachverständigen – personenbeziehbar werden könnten".[50]

Besonders misslich ist dieses Verkennen der Rechtslage, weil sich unter den Daten auch solche befinden, die als besondere Arten personenbezogener Daten i.S.d. § 3 Abs. 9 BDSG (Gesundheitsdaten) oder als eine Informationspflicht auslösende Daten i.S.d. § 42a BDSG (Bank- und Kreditkartendaten) besonderen Schutzes bedürfen. Zu beachten ist ferner, dass nicht nur Daten von Fahrer und Insassen betroffen sind, sondern auch personenbezogene Daten anderer Verkehrsteilnehmer und Dritter, wenn über die Einbindung von Smart Devices in das Kfz und die Nutzung entsprechender Dienste (*dazu oben Ziff. 2.4*) Fahrer oder Insassen mit Dritten aus dem Kfz kommunizieren.[51]

3.3 Zuordnung der Daten im Kfz

An Daten ohne Personenbezug gibt es kein Eigentum, welches über Art. 14 Abs. 1 GG Schutz genießen könnte. Diese dürfen deshalb frei genutzt werden. Eine Grenze ergibt sich erst, wenn über das Urheberrecht oder den Schutz von Betriebs- und Geschäftsgeheimnissen Schutzrechte an Daten oder Datensammlungen begründet werden, die mit dinglicher Wirkung die Nutzung durch Dritte beschränken. Ob und inwieweit ein derartiger Schutz bei nicht personenbezogenen Daten aus Kfz und intelligenten Verkehrssystemen greift, bedarf gesonderter Betrachtung.

Auch an personenbezogenen Daten, die regelmäßig vorliegen dürften (dazu oben Ziff. 3.2), gibt es kein Eigentum[52]. Mit der Ableitung eines Rechts auf informationelle Selbstbestimmung aus dem allgemeinen Persönlichkeitsrecht in Art. 2 Abs. 1 GG durch das BVerfG[53] und dem in der Folge im BDSG in § 4 Abs. 1 BDSG normierten Verbot mit Erlaubnisvorbehalt[54] gibt es gleichwohl keine freie Nutzung personenbezogener Daten.

41 BT-Drucksache 18/1362 v. 2.5.2014, S. 5: http://dipbt.bundestag.de/dip21/btd/18/013/1801362.pdf.

42 So aber Gola/Schomerus, BDSG, § 3 Rn 10.

43 Entwurf einer Verordnung zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (allgemeine Datenschutzverordnung), Kom(2012) 11 endgültig: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:DE:HTML; konsolidierte Fassung: http://www.delegedata.de/datenschutz-grundverordnung-konsolidierte-fassung/; zur Datenschutzverordnung insgesamt Gola/Schulz, RDV 2013, 1; Schwartmann, RDV 2012, 55; Eckhardt, CR 2012, 195; Schneider, ITRB 2012, 180.

44 Ebenso Pohle/Zoch, CR 2014, 409 (410).

45 Ebenso Weichert, SVR 2014, 201 (204).

46 BT-Drucksache 18/1362 v. 2.5.2014, S. 5: http://dipbt.bundestag.de/dip21/btd/18/013/1801362.pdf.

47 BT-Drucksache 18/706 v. 5.3.2014, S. 11: http://dipbt.bundestag.de/dip21/btd/18/007/1800706.pdf.

48 VDA: http://www.vda.de.

49 Abrufbar unter http://www.lda.bayern.de/lda/datenschutzaufsicht/lda_daten/Muster-Information_Fahrzeugdatenspeicher.pdf.

50 Kritisch dazu auch Pohle/Zoch, CR 2014, 409 (410).

51 Ausführlich Weichert, SVR 2014, 201 (204).

52 BT-Drucksache 18/1362 v. 2.5.2014, S. 3: http://dipbt.bundestag.de/dip21/btd/18/013/1801362.pdf.

53 BVerfG, Urt. v. 15.12.1983 – 1 BvR 209/83, 1 BvR 269/83, 1 BvR 362/83, 1 BvR 420/83, 1 BvR 440/83, 1 BvR 484/83, NJW 1984, 419 = Volkszählungsurteil.

54 Dazu Gola/Schomerus, BDSG, § 4 Abs. 1 Rn. 1 f.

Denn gleich einem Eigentümer ist der Betroffene i.S.d. § 3 Abs. 1 BDSG vorbehaltlich eines Erlaubnistatbestands berechtigt, jeden Dritten von dem Umgang mit seinen personenbezogenen Daten auszuschließen. Anderenfalls liefe das Verbot mit Erlaubnisvorbehalt ins Leere, woran auch im Entwurf in Art. 6 der Datenschutzverordnung[55] festgehalten wird. Die Zuordnung personenbezogener Daten aus Kfz und intelligenten Verkehrssystemen richtet sich deshalb allein danach, wer Betroffener i.S.d. § 3 Abs. 1 BDSG und wer verantwortliche Stelle i.S.d. § 3 Abs. 7 BDSG ist (dazu sogleich unten Ziff. 3.4).

3.4 Betroffener und verantwortliche Stellen

Betroffen vom Umgang mit personenbezogenen Daten im und aus dem Kfz können Halter, Fahrer, Insassen und ggf. Dritte sein (siehe oben Ziff. 3.2). Zur Feststellung des Betroffenen i.S.d. § 3 Abs. 1 BDSG bedarf es insoweit einer Betrachtung der Daten (dazu oben Ziff. 3.1) im konkreten Einzelfall (zu Anwendungsfällen aus der Praxis unten Ziff. 4). Dies gilt insbesondere, wenn ein Kfz, wie zumeist, durch verschiedene Fahrer oder Insassen genutzt wird, etwa bei einer vom Arbeitgeber gestatteten Privatnutzung eines betrieblichen Kfz durch den Beschäftigten und dessen Familie (*zu den Rechtsfolgen einer solchen zugelassenen Privatnutzung im TMG unten Ziff. 3.5.3.2*).

Ungleich schwieriger ist die Ermittlung der verantwortlichen Stelle i.S.d. § 3 Abs. 7 BDSG. Entscheidend ist, wer die Herrschaft über die im oder aus dem Kfz erhobenen personenbezogenen Daten innehat[56], wer also i.S.d. Art. 2 lit. d) der Richtlinie 95/46/EG vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (*Datenschutz-Richtlinie = DSRL*)[57] „über Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet“[58].

Verantwortliche Stelle dürfte beim Umgang mit personenbezogenen Daten nur in Ausnahmefällen der Betroffene selbst sein, etwa wenn es um Daten aus Servicefunktionen (*dazu oben Ziff. 3.1*) im Infotainment-System (*zum Begriff oben Ziff. 2.4*) geht, über deren Verwendung der Betroffene einschließlich deren Löschung i.S.d. § 3 Abs. 4 Nr. 5 BDSG selbst (mit-) entscheiden kann[59]. Soweit die Bundesregierung davon ausgeht, dass Kfz dem Nutzer „regelmäßig über die elektronische Menüführung die Löschung dieser Daten“ erlauben[60], ist nicht bekannt, auf welcher Tatsachenbasis diese Aussage getroffen worden ist. Die Betriebsanleitungen und Datenschutzerklärungen der Anbieter solcher Dienste verhalten sich regelmäßig weder zum Vorhandensein einer Löschfunktion noch zu deren Wirkweise. Im Übrigen dürften dem Betroffenen im Regelfall die notwendigen Systeme (Software, Hardware) und Kenntnisse fehlen, um Daten für Fahrzeug- oder Servicefunktionen zu beherrschen.

Zumeist dürfte verantwortliche Stelle deshalb derjenige sein, der die zum Umgang mit personenbezogenen Daten im Kfz vorhandenen Anwendungen oder Dienste intelligenter Verkehrssysteme (*zu den Begriffen oben Ziff. 2.2*) bereitgestellt hat oder hierauf bei einem physischen oder Remote-Zugang zum Kfz zugreifen kann[61]. Das ist wegen der Daten aus im Kfz verbauten Steuergeräten regelmäßig der Hersteller oder die mit der Durchführung von Arbeiten am Kfz beauftragte Werkstatt, bei Telematik-Boxen (*dazu oben Ziff. 2.3*) der für deren Einbau verantwortliche Arbeitgeber, Flottenbetreiber oder Versicherer. Geht es um die Übermittlung von Daten C2I/C2X aus dem Kfz an externe infrastrukturelle Anwendungen oder Dienste intelligenter Verkehrssysteme, wird regelmäßig der Dienstleister die verantwortliche Stelle sein. Dabei können sich die verantwortlichen Stellen wiederum Auftragsdatenverarbeiter i.S.d. § 11 BDSG[62] bedienen oder die Verwendung der personenbezogenen Daten in Cloud-Applikationen[63] vornehmen.

Wesentliches Element der datenschutzrechtlichen Bewertung des Umgangs mit personenbezogenen Daten im Connected Car ist deshalb die sorgfältige und differenzierte Aufarbeitung des zugrunde liegenden Sachverhalts bezogen auf die Beteiligten, die verwendete Technik und die betroffenen Anwendungen und Dienste intelligenter Verkehrssysteme, woran es bislang zumeist fehlt.

3.5 Anwendbares Datenschutzrecht

Spezialgesetze für den Umgang mit personenbezogenen Daten im Zusammenhang mit intelligenten Verkehrssystemen gibt es mit Ausnahme des IVG nicht (*zum IVSG oben Ziff. 2.2 und unten Ziff. 3.5.2*). Die Bundesregierung hält solche auch nicht für erforderlich, weil es sich hier um ein Querschnittsthema handele, welches „allgemein und technikneutral geregelt werden“ könne[64].

3.5.1 Grenzüberschreitende Sachverhalte

Für die Bestimmung des anwendbaren Datenschutzrechts bei grenzüberschreitenden Sachverhalten ist auf § 1 Abs. 5 BDSG

55 Dazu oben Fn. 43.

56 BT-Drucksache 18/1362 v. 2.5.2014, S. 4: http://dipbt.bundestag.de/dip21/btd/18/013/1801362.pdf.

57 Http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:DE:HTML.

58 Gola/Schomerus, BDSG, § 3 Rn. 48; anders Weichert, SVR 2014, 201 (205), der jede Zweckveranlassung eines Umgangs mit personenbezogenen Daten genügen lässt.

69 Zu beachten ist, dass bei einem ausschließlich persönlichen oder familiären Umgang mit personenbezogenen Daten das BDSG gemäß § 1 Abs. 2 Nr. 3 BDSG keine Anwendung findet, dazu Schulz/Roßnagel/David, ZD 2012, 510 (513).

60 BT-Drucksache 18/1362 v. 2.5.2014, S. 2: http://dipbt.bundestag.de/dip21/btd/18/013/1801362.pdf.

61 Ausschließlich auf die Zugriffsmöglichkeit stellt ab Kamps, Internationales Verkehrswesen 2014, 18.

62 Denkbar ist, dass die Anwendungen oder Dienste intelligenter Verkehrssysteme im Auftrag des Betroffenen von einem Dritten beherrscht werden, wovon ohne Begründung die Bundesregierung ausgeht, BT-Drucksache 18/1362 v. 2.5.2014, S. 3: http://dipbt.bundestag.de/dip21/btd/18/013/1801362.pdf. Dann handelt es sich bei Abschluss eines Vertrags gemäß § 11 Abs. 2 S. 2 BDSG um eine Auftragsdatenverarbeitung i.S.d. § 11 Abs. 1 BDSG mit der Folge, dass der Betroffene selbst verantwortliche Stelle i.S.d. § 3 Abs. 7 BDSG ist. Ebenso ist denkbar, dass eine Auftragsdatenverarbeitung zwischen dem den Umgang mit personenbezogenen Beherrschenden und einem Dritten abgeschlossen ist, etwa zwischen Flottenbetreiber und Arbeitgeber. Ausführlich zur Auftragsdatenverarbeitung Kremer, ITRB 2014, 60; Kremer/Sander, ITRB 2014, 187.

63 Zum Datenschutz beim Cloud Computing Selzer, DuD 2014, 470; Borges, DuD 2014, 165; Kühling/Biendl, CR 2014, 150; Göpel, RDV 2013, 292.

64 BT-Drucksache 18/1362 v. 2.5.2014, S. 5: http://dipbt.bundestag.de/dip21/btd/18/013/1801362.pdf; kritisch Weichert, SVR 2014, 241 (247).

oder den diesen wegen seiner Harmonisierungswirkung überlagernden Art. 4 Abs. 1 DSRL als die entscheidenden Kollisionsnormen abzustellen, ohne dass es Besonderheiten zu beachten gilt[65].

3.5.2 Intelligente Verkehrssysteme Gesetz

Die besonderen Herausforderungen intelligenter Verkehrssysteme haben 2010 zur Verabschiedung der IVS-RL und 2013 in Deutschland zum IVSG geführt (Details oben Ziff. 2.2).

3.5.2.1 Erlaubnistatbestände für Intelligente Verkehrssysteme

§ 3 Satz 2 IVSG enthält einen völlig missglückten datenschutzrechtlichen Erlaubnistatbestand, wenn es dort heißt: „Personenbezogene Daten dürfen nur erhoben, verarbeitet oder genutzt werden, soweit dies durch eine bundesgesetzliche Regelung ausdrücklich zugelassen oder angeordnet wird."

§ 3 Satz 2 IVSG soll Art. 10 IVS-RL umsetzen. Art. 10 Abs. 1 IVS-RL schreibt fest, dass bei Intelligenten Verkehrssystemen die DSRL (*siehe oben Ziff. 3.4*) zu beachten ist. Art. 10 Abs. 3 IVS-RL konkretisiert dies dahingehend, dass „soweit angemessen" die Verwendung anonymer Daten bei Anwendungen und Diensten intelligenter Verkehrssysteme zu fördern ist und mit personenbezogenen Daten nur dann umgegangen werden darf, wenn dies für den Betrieb der Anwendungen und Dienste erforderlich ist. Im Übrigen sind gemäß Art. 10 Abs. 4 IVS-RL die Bestimmungen über die Einwilligung im Datenschutzrecht einzuhalten.

Vor diesem Hintergrund[66] und der gebotenen europarechtskonformen Auslegung von § 3 Satz 2 IVSG[67] ist dieser kein eigenständiger, die Einwilligung ausschließender gesetzlicher Erlaubnistatbestand i.S.d. § 4 Abs. 1 BDSG, sondern zunächst nur ein in seiner Wirkung deklaratorischer Verweis auf alle bundesgesetzlichen Erlaubnistatbestände insbesondere im BDSG, TMG und TKG. Konstitutiv verbietet § 3 Satz 2 IVSG jedoch den Rückgriff auf landesgesetzliche Regelungen als Erlaubnistatbestand für den Umgang mit personenbezogenen Daten zum Betrieb intelligenter Verkehrssysteme und hierauf basierender Anwendungen und Dienste[68].

3.5.2.2 Besondere Datenarten im IVSG

Das IVSG definiert in § 2 besondere Datenarten. Straßendaten i.S.d. § 2 Nr. 6 IVSG sind „Daten über Merkmale der Straßeninfrastruktur einschließlich fest angebrachter Verkehrszeichen oder ihrer geregelten Sicherheitsmerkmale", Verkehrsdaten i.S.d. § 2 Nr. 7 IVSG „vergangenheitsbezogene Daten und Echtzeitdaten zum Straßenverkehrszustand" und Reisedaten i.S.d. § 2 Nr. 8 IVSG „Daten wie Fahrpläne und Tarife öffentlicher Verkehrsmittel als erforderliche Grundlage für die Bereitstellung von Reiseinformationen vor und während der Reise zur Erleichterung der Planung, Buchung und Anpassung der Reise". Allen diesen Datenarten ist gemein, dass es sich nicht um personenbezogene Daten i.S.d. § 3 Abs. 1 BDSG handelt, so dass diese hier keiner weiteren Betrachtung bedürfen.

3.5.3 Weitere Spezialgesetze

Vorrangig gegenüber dem BDSG können als Spezialgesetze gemäß § 1 Abs. 3 S. 1 BDSG insbesondere TMG und TKG auf den Umgang mit personenbezogenen Daten im Kfz und den anderen intelligenten Verkehrssystemen Anwendung finden[69]. Die Subsidiarität des BDSG greift aber nur soweit, wie eigene, zum BDSG deckungsgleiche Erlaubnistatbestände zum Umgang mit personenbezogenen Daten in TKG oder TMG vorhanden sind[70], dies jedoch auch dann, wenn sich dadurch eine Erleichterung zugunsten der verantwortlichen Stelle gegenüber dem BDSG ergibt[71]. Weil das TKG keine eigenständigen, von § 1 Abs. 5 BDSG abweichenden Regelungen enthält und § 1 Abs. 5 TMG ausdrücklich klarstellt, dass dort keine „Regelungen im Bereich des internationalen Privatrechts" getroffen sind, ist das bereichsspezifische Datenschutzrecht im TKG und TMG stets anwendbar, wenn auch das BDSG international Anwendung findet (*dazu oben Ziff. 3.5.1*)[72].

3.5.3.1 Anwendbarkeit des TKG

Die Anwendbarkeit der §§ 91 ff. TKG setzt nach § 91 Abs. 1 S. 1 TKG voraus, dass „geschäftsmäßig Telekommunikationsdienste" erbracht oder an der Erbringung solcher Dienste mitgewirkt wird. „Telekommunikationsdienste" sind dabei nach § 3 Nr. 24 TKG „in der Regel gegen Entgelt erbrachte Dienste, die ganz oder überwiegend in der Übertragung von Signalen über Telekommunikationsnetze bestehen", wobei die Geschäftsmäßigkeit gemäß § 3 Nr. 10 TKG bei einem „nachhaltigen Angebot (...) für Dritte mit oder ohne Gewinnerzielungsabsicht" vorliegt. Ebenfalls unter die Telekommunikationsdienste fallen die sog. telekommunikationsgestützten Dienste nach § 3 Nr. 25 TKG, die keinen vom Telekommunikationsdienst räumlich und zeitlich trennbaren Leistungsfluss auslösen, sondern bei denen die Inhaltsleistung noch während der Telekommunikationsverbindung erfüllt wird. Abgrenzungskriterium gegenüber Telemediendiensten nach § 1 Abs. 1 S. 1 TMG ist im Kern der technische Vorgang des Übertragens von Inhalten im Gegensatz zum Angebot der Inhalte als solche, sog. Schichtenmodell[73].

65 Zur Harmonisierungswirkung der DSRL und der Bestimmung des anwendbaren Rechts am Beispiel von Social Media Diensten ausführlich Kremer, RDV 2014, 73 (75). Zur neuen extensiven Auslegung des Begriffs der Ausführung von Datenverarbeitungen in einer Niederlassung in Art. 4 Abs. 1 lit. a) DSRL EuGH, Urteil v. 13.5.2014 – C-131/12 = K&R 2014, 512, dazu Karg, ZD 2014, 359.

66 Siehe auch Erwägungsgrund 12 IVS-RL, zur Notwendigkeit der Berücksichtigung der Erwägungsgründe bei Auslegung einer Richtlinie EuGH, Urteil v. 10.4.2014 – C-435/12, Urteil v. 21.10.2010 – C-467/08.

67 Zur Harmonisierungswirkung der DSRL siehe Kremer, RDV 2014, 73 (75).

68 Ob die mit dem Ausschluss landesgesetzlicher Erlaubnistatbestände einhergehende Beschränkung der Gesetzgebungskompetenz der Länder aus Art. 70 Abs. 1 GG verfassungsrechtlich zulässig ist, bedarf ggf. noch besonderer Prüfung.

69 Ausführlich Weichert, SVR 2014, 201 (203).

70 Eckhardt, in: Spindler/Schuster, Recht der elektronischen Medien, § 91 TKG Rn. 2.

71 Gola/Schomerus, BDSG, § 1 Rz. 24.

72 Stadler, ZD 2011, 57 (58).

73 Eckhardt, in: Spindler/Schuster, Recht der elektronischen Medien, § 91 TKG Rz. 5; Holznagel/Ricke, in: Spindler/Schuster, Recht der elektronischen Medien, § 3 TKG Rz. 35.

Wird eine Anwendung intelligenter Verkehrssysteme über Mobilfunk oder andere Funktechniken realisiert (ohne dass sich dies auf eine Ad hoc-Kommunikation zwischen zwei Systemen beschränkt[74]), liegt schon begrifflich eine Übertragung von Signalen über Telekommunikationsnetze i.S.d. § 3 Nr. 27 TKG vor. Die Entgeltlichkeit und Geschäftsmäßigkeit wird dabei regelmäßig gegeben sein. Damit ist keine vom Anwender zu zahlende Vergütung gemeint, vielmehr wird auf eine Teilnahme am Wirtschaftsleben durch den Anbieter der Dienste intelligenter Verkehrssysteme abgestellt. Dies hat zur Folge, dass auf den Umgang mit personenbezogenen Daten im Zusammenhang mit der Signalübertragung bei intelligenten Verkehrssystemen nicht das BDSG, sondern die §§ 91 ff. TKG anzuwenden sind[75].

Ein Telekommunikationsdienst ist auch dann gegeben, wenn der Dienst intelligenter Verkehrssysteme (zum Begriff oben Ziff. 2.2) selbständig für den Kfz-Nutzer das Veröffentlichen und Verteilen von Nachrichten oder sonstigen Informationen innerhalb des jeweiligen Dienstes oder an andere Anwendungen und Dienste übernimmt. In diesem Fall dient die Funktionalität überwiegend der Verbreitung von Inhalten, also deren technischer Übertragung; ohne die Übertragung wäre die Funktionalität für den Nutzer wertlos[76]. Eine derartige Verteilung von Informationen findet sich heute z.B. in Infotainment-Systemen (zum Begriff oben Ziff. 2.4), welche die Nutzung von Twitter, Facebook oder E-Mail-Diensten im Kfz erlauben, aber auch in Navigationsgeräten zur Optimierung der Routenplanung in Echtzeit oder standortbasierten Diensten im Fuhrparkmanagement.

Sind die §§ 91 ff. TKG anwendbar, wird der Umgang mit personenbezogenen Daten gegenüber dem BDSG erheblich beschränkt. Ohne Einwilligung dürfen dann im Wesentlichen Verkehrsdaten i.S.d. § 3 Nr. 30 TKG für den Aufbau von Verbindungen gemäß § 96 Abs. 1 TKG, zur Entgeltermittlung und Entgeltabrechnung gemäß § 97 TKG sowie zum Umgang mit Störungen und Missbrauchsfällen gemäß § 100 TKG, Bestandsdaten i.S.d. § 3 Nr. 3 TKG zur Begründung, Durchführung und Beendigung von Vertragsverhältnissen sowie Standortdaten i.S.d. § 3 Nr. 19 TKG nur anonymisiert gemäß § 98 TKG verwendet werden. Inhaltsdaten sind, soweit das Fernmeldegeheimnis greift, ohnehin jeglichem Zugriff durch den Diensteanbieter entzogen[77] und unterfallen mangels Spezialgesetz im TKG dem BDSG[78].

3.5.3.2 Anwendbarkeit des TMG

Nach § 1 Abs. 1 S. 1 TMG sind Telemediendienste durch eine Negativabgrenzung zu bestimmen. Hiernach ist jeder elektronische Informations- und Kommunikationsdienst, der kein ganz in der Übertragung von Signalen bestehender Telekommunikationsdienst nach § 3 Nr. 24 TKG, kein telekommunikationsgestützter Dienst nach § 3 Nr. 25 TKG und auch kein Rundfunk nach § 2 RStV[79] ist, ein Telemediendienst. Damit fallen u.a. folgende Funktionalitäten in den Anwendungsbereich des TMG:[80] Datendienste (Verkehr, Wetter, Umwelt, Börse), Empfehlungs- und Ratgeberdienste, Bestellungs-, Buchungs- und Maklerdienste, einschließlich Shops und Handelsplattformen, Presse und Nachrichtendienste sowie On-Demand- und Streaming-Dienste, soweit es sich dabei nicht um Rundfunk handelt.

Viele der vorgenannten Funktionalitäten werden durch Dienste intelligenter Verkehrssysteme (*zum Begriff oben Ziff. 2.2*) dynamisch und nicht nur als stationäre, lokal im Kfz installierte Software bereitgestellt, so dass auf diese Dienste vorrangig gegenüber dem BDSG die §§ 11 ff. TMG anzuwenden sind[81]. Funktionalitäten, die nicht ganz, sondern nur überwiegend in der Erbringung von Telekommunikationsdiensten bestehen, können sowohl unter die §§ 91 ff. TKG als auch unter die §§ 11 ff. TMG fallen. Besteht ein Dienst aus mehreren Funktionalitäten, die z.T. unter das TKG, z.T. unter das TMG fallen, sind derartige „zusammengesetzte Dienste" einzeln nach ihren Funktionalitäten und nicht nach dem Schwerpunkt des Dienstes zu behandeln[82].

Sind die § 11 ff. TMG anwendbar, ist der Anbieter des Dienstes zur Bereitstellung einer Datenschutzerklärung gemäß § 13 Abs. 1 TMG verpflichtet[83]. Daneben beschränken die §§ 14, 15 TMG den Umgang mit personenbezogenen Daten zur Erbringung von Telemediendiensten ähnlich wie die §§ 91 ff. TKG (*dazu oben Ziff. 3.5.3.1*). Außerhalb der Begründung, Durchführung oder Beendigung eines Vertragsverhältnisses sowie dessen Abrechnung bedarf der Umgang mit personenbezogenen Daten aus Telemedien nahezu immer der Einwilligung des Betroffenen. Dies ist insbesondere im Beschäftigungsverhältnis misslich, wenn der Arbeitgeber dem Arbeitnehmer die (auch) private Nutzung eines betrieblichen Kfz als Anwendung intelligenter Verkehrssysteme gestattet hat und damit über das betriebliche Kfz Dienste intelligenter Verkehrssysteme in Form von Telemedien in Anspruch genommen werden können. Wegen § 11 Abs. 1 Nr. 1 TMG, der den Rückgriff auf das BDSG im Dienst- und Arbeitsverhältnis nur bei der ausschließlich betrieblichen Nutzung von Telemedien gestattet, kann der Arbeitgeber bei derartig gestatteter Privatnutzung einen nach dem BDSG zulässigen, aber nach dem TMG unzulässigen Umgang mit personenbezogenen Daten nur über eine Einwilligung des oder der Betroffenen (*dazu unten Ziff. 3.6.3*) oder eine Betriebsvereinbarung legimitieren, letzteres jedoch nur, wenn sich die Betriebsvereinbarung wegen § 12 Abs. 1, Abs. 2 TMG ausdrücklich auch auf Telemedien bezieht[84].

74 Schulz/Roßnagel/David, ZD 2012, 510 (512).

75 BMW ist bei der Bundesnetzagentur (http://www.bnetza.de) bereits als Telekommunikationsdiensteanbieter registriert: http://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Anbieterpflichten/Meldepflicht/TKDiensteanbieterPDF.pdf?__blob=publicationFile&v=24.

76 Zur vergleichbaren Situation bei Apps Kremer, CR 2012, 438 (441).

77 Zum Fernmeldegeheimnis nach § 88 TKG und Art. 10 GG am Beispiel E-Mail Sander, CR 2014, 176.

78 Weichert, SVR 2014, 201 (203).

79 Zur Abgrenzung Heckmann in jurisPK-Internetrecht, Kap. 1 Rz. 42 ff.

80 Weitere Beispiele bei Heckmann in jurisPK-Internetrecht, Kap. 1 Rz. 59 ff.; Holznagel/Ricke in Spindler/Schuster, Recht der elektronischen Medien, § 1 TMG Rz. 10.

81 Ebenso die Bundesregierung, BT-Drucksache 18/1362 v. 2.5.2014, S. 4: http://dipbt.bundestag.de/dip21/btd/18/013/1801362.pdf; kritisch Schulz/Roßnagel/David, ZD 2012, 510 (512).

82 Mit Nachweisen zur anderen Ansicht Kremer, CR 2012, 438 (441).

83 Zur Datenschutzerklärung und deren Inhaltskontrolle als AGB Kremer, RDV 2014, 73, 82.

84 Zur Abgrenzung von TMG und BDSG ausführlich Sander, CR 2014, 176 (181).

3.6 Art und Weise des Umgangs mit personenbezogenen Daten

Beim Umgang mit personenbezogenen Daten aus und im Kfz (*zur Herleitung oben Ziff. 3.2*) kann man zwischen einem geheimen Vorgehen, einem Vorgehen mit Wissen des Betroffenen und einem Vorgehen mit Einwilligung des Betroffenen differenzieren[85]. Die datenschutzrechtliche Zulässigkeit beurteilt sich dabei jeweils nach dem anwendbaren Datenschutzrecht (*dazu oben Ziff. 3.5*).

3.6.1 Geheimer Umgang

Der geheime Umgang bezieht sich auf solche personenbezogenen Daten, die ohne Wissen oder Einwilligung des Betroffenen erhoben, verarbeitet und genutzt werden. Hierbei handelt es sich regelmäßig um Daten für Fahrzeugfunktionen (*zum Begriff oben Ziff. 3.1*), auf die der Betroffene regelmäßig mangels Herrschaft über die verwendeten Systeme (Hardware/Software) keinen Zugriff hat und worüber er nicht durch eine Datenschutzerklärung der verantwortlichen Stelle (*dazu oben Ziff. 3.4*) aufgeklärt wird.

3.6.2 Umgang mit Wissen des Betroffenen

Der Umgang mit personenbezogenen Daten mit Wissen des Betroffenen erfasst alle Fälle, in denen der Betroffene entweder von der verantwortlichen Stelle (*dazu oben Ziff. 3.4*) über eine Datenschutzerklärung (*zur Notwendigkeit bei Telemedien im Kfz oben Ziff. 3.5.3.2*) über den Umgang mit personenbezogenen Daten in Kenntnis gesetzt worden oder dieser für den Betroffenen offenkundig ist. Letzteres ist bei solchen Anwendungen und Diensten intelligenter Verkehrssysteme der Fall, die vom Betroffenen aktiv in Betrieb genommen und die Erhebung personenbezogener Daten kenntlich machen. Hierunter fallen z.B. Daten aus Servicefunktionen (*zum Begriff oben Ziff. 3.1*) im Infotainment-System, etwa wenn der Betroffene sein Smart Device (*dazu oben Ziff. 2.4*) mit dem Kfz koppelt und sodann über das Kfz telefoniert, E-Mails versendet oder soziale Netzwerke nutzt oder aber auf Informationen aus Kamerasystemen im Kfz zurückgreift.

3.6.3 Umgang mit Einwilligung des Betroffenen

Der Umgang mit personenbezogenen Daten mit Einwilligung des Betroffenen setzt wegen der Informiertheit und Bestimmtheit der Einwilligung nach § 4a Abs. 1 BDSG[86] stets das Wissen des Betroffenen über die Erhebung, Verarbeitung und Nutzung seiner personenbezogenen Daten voraus (*dazu oben Ziff. 3.6.2*). Kennzeichnendes Merkmal ist insoweit die Zustimmung des Betroffenen zum Umgang mit seinen personenbezogenen Daten, die als Erlaubnistatbestand i.S.d. § 4 Abs. 1 BDSG den anderenfalls erfolgenden Grundrechtseingriff rechtfertigt (*dazu oben Ziff. 3.3*). Derartige Einwilligungen werden in der Praxis bislang nahezu ausschließlich für Daten aus Servicefunktionen beim Kauf eines Kfz eingeholt, aber nur in Ausnahmefällen bei einer späteren Nutzungsüberlassung des Kfz an den Arbeitnehmer oder für Daten aus Fahrzeugfunktionen (*zu den Begriffen oben Ziff. 3.1*). Ein Beispiel hierfür sind die zur Inanspruchnahme eines Telematik-Tarifs (*dazu unten Ziff. 4.3*) erforderlichen Einwilligungen in die Installation der Telematik-Box (*zum Begriff oben Ziff. 2.3*) und die Verwendung der hiermit erhobenen personenbezogenen Daten zur Bestimmung des Versicherungstarifs.

4. Anwendungsfälle aus der Praxis

Im Folgenden werden einzelne Anwendungsfälle zum Umgang mit personenbezogenen Daten im und aus dem Kfz beschrieben und datenschutzrechtlich bewertet. Daneben gibt es eine Vielzahl weiterer Anwendungsfälle, z.B. bei der Vertragsanbahnung, der Bereitstellung von Serviceangeboten, der Fernsteuerung von Kfz und in Straf- und Ordnungswidrigkeitenverfahren, deren Darstellung jedoch den Rahmen dieses Beitrags gesprengt hätte[87].

4.1. Intelligente Verkehrssteuerung

Bei der intelligenten Verkehrssteuerung geht es um den Umgang mit Daten zur Ermöglichung eines verkehrsoptimierten Verhaltens von Fahrer und Kfz.

4.1.1 Beispiele intelligenter Verkehrssteuerung

Bei der intelligenten Verkehrssteuerung können etwa Angaben über die Entfernung zur Ampel, die Restdauer der dortigen Grünphase und etwaige Geschwindigkeitsbegrenzungen oder Verkehrshindernisse auf dem verbleibenden Weg bis zur Ampel in einer Kommunikation C2C und C2X (*dazu oben Ziff. 2*) zu einem Fahren mit der „grünen Welle“, einem verbrauchsreduzierten Heranrollen an die Ampel oder einer Änderung der Ampelphasen genutzt werden. Ähnlich können Angaben zum Wetter wie Temperatur und Niederschlagsmenge in der Kommunikation C2C und C2X zur adaptiven Verkehrssteuerung und Unfallvermeidung genutzt werden, wenn etwa das vorausfahrende Kfz die nachfolgenden Kfz vor Glätte warnt oder infrastrukturelle intelligente Verkehrssysteme (*zum Begriff oben Ziff. 2.2*) im Kfz vor einem Unfall auf der Fahrstrecke warnen.

4.1.2 MDM Mobilitäts Daten Marktplatz

Die Einführung der intelligenten Verkehrssteuerung ist ein Schwerpunkt im sog. IVS Aktionsplan „Straße“ der Bundesregierung[88]. Ein Element ist die Etablierung des MDM Mobilitäts Daten Marktplatz mit Unterstützung des Bundeswirtschaftsministeriums.[89] Der MDM soll „die Profile aller bundesweit ver-

85 Nach Mielchen in: 52. Deutscher Verkehrsgerichtstag 2014, 241 (246); Mielchen, SVR 2014, 80 (81).

86 Dazu Gola/Schomerus, BDSG, § 4a Rn. 26 ff.

87 Zur Kommunikation zwischen Kfz und Fußgänger ausführlich Schulz/Roßnagel/David, ZD 2012, 510 (513).

88 Details im IVS Aktionsplan „Straße“, September 2012: http://www.bmvi.de/SharedDocs/DE/Anlage/VerkehrUndMobilitaet/Strasse/ivs-aktionsplan-strasse-broschuere.pdf?__blob=publicationFile; Information an die EU-Kommission, August 2012: http://www.bmvi.de/SharedDocs/DE/Anlage/VerkehrUndMobilitaet/Strasse/ivs-massnahmen.pdf?__blob=publicationFile; Bericht zu Status und Rahmenbedingungen für intelligente Verkehrssysteme in Deutschland, 2011: http://ec.europa.eu/transport/themes/its/road/action_plan/doc/2011_its_initial_report_germany.pdf.

89 MDM Mobilitäts Daten Marktplatz: http://www.mdm-portal.de.

fügbaren Online-Verkehrsdaten zentral vereinen" und als „Metadatenplattform […] mehr Transparenz für die Akteure im neu entstehenden Markt [schaffen] und […] die Kooperation [fördern]".[90] Beim noch bis Ende 2015 kostenfrei nutzbaren MDM sollen Datenanbieter unter Angabe von Metadaten ihre Straßendaten, Verkehrsdaten und Reisedaten i.S.d. IVSG (*dazu oben Ziff. 3.5.2.2*) bewerben, Kontakt zu Datenabnehmern herstellen und sodann die angebotenen Daten standardisiert übertragen können[91].

4.1.3 Datenschutzrechtliche Bewertung

Bei den auf dem MDM angebotenen Daten dürfte es sich regelmäßig nicht um personenbezogene Daten handeln, weil diese entweder ihrem Wesen nach als Straßendaten, Verkehrsdaten und Reisedaten keinen Personenbezug aufweisen (*dazu oben Ziff. 3.5.2.2*) oder aber nur in anonymisierter Form zum Handel angeboten werden. Solange es nicht durch die Kombination verschiedener Datenpakete mittels Big Data[92] zur Wiederherstellung eines Personenbezugs kommt, ist die Nutzung dieser Daten datenschutzrechtlich unbeachtlich (*zu anderen Nutzungsschranken oben Ziff. 3.3*).

Fehlt es beim Umgang mit personenbezogenen Daten zu Zwecken der intelligenten Verkehrssteuerung an einer Anonymisierung, erlauben diese Daten regelmäßig die Erstellung von Fahr- und Verhaltensprofilen der Betroffenen, was ein schwerwiegender Eingriff in das Persönlichkeitsrecht ist, der durch keinen gesetzlichen Erlaubnistatbestand gerechtfertigt werden kann, insbesondere dann nicht, wenn auch besondere Arten personenbezogener Daten i.S.d. § 3 Abs. 9 BDSG betroffen sind (*dazu oben Ziff. 3.2*). Damit ist regelmäßig eine Einwilligung der Betroffenen für einen datenschutzrechtlich zulässigen Umgang erforderlich (*zur Einwilligung unten Ziff. 5.3*).

4.2 Automatische Notrufsysteme

Die bislang von verschiedenen Herstellern freiwillig angebotenen automatischen Notrufsysteme (wie seit 2006 BMW Assist)[93] werden mit Einführung des EU-weiten, auf Mobilfunktechnik basierenden eCall-Dienstes rechtlich voraussichtlich zum 1.10.2015 verpflichtend, spätestens jedoch zum 1.10.2017[94]. Grundlage hierfür sind die IVS-RL (*oben Ziff. 2.2*), die delegierte Verordnung 305/2013 vom 26.11.2012 zur Ergänzung der Richtlinie 2010/40/EU in Bezug auf die harmonisierte Bereitstellung eines interoperablen EU-weiten eCall-Dienstes (*eCall-VO*)[95] und der Beschluss Nr. 585/2014 von europäischem Parlament und Rat vom 15.5.2014 über die Einführung des interoperablen EU-weiten eCall-Dienstes[96].

4.2.1 eCall-Dienst und Mindestdatensatz

Im Fall eines Unfalls löst das Kfz über ein bordeigenes Gerät i.S.d. Art. 2 lit. g) ISV-RL automatisch ohne Mitwirkung der Insassen eine eCall-Transaktion i.S.d. Art. 2 lit. i) ISV-RL aus, welche über das öffentliche Mobilfunknetz den sog. Mindestdatensatz (MSD) i.S.d. Art. 2 lit. j) ISV-RL an die zuständige eCall-Notrufabfragestelle i.S.d. Art. 2 lit. f) ISV-RL übermittelt und zugleich eine Tonverbindung zwischen dem verunfallten Kfz und derselben eCall-Notrufabfragestelle herstellt. Bestandteil des MSD sind die sich aus der DIN EN 15722 ergebenden Daten, im Einzelnen Unfallort, Unfallzeitpunkt, Fahrtrichtung, Fahrzeugkennung mit Fahrzeugtyp und Treibstoffart sowie die Anzahl der angelegten Sicherheitsgurte[97]. Da die Fahrzeugkennung mit der FIN (*dazu oben Ziff. 3.1*) die Ermittlung des Halters zulässt, handelt es sich beim MSD insgesamt um personenbezogene Daten i.S.d. § 3 Abs. 1 BDSG[98].

4. 2.2 Datenschutzrechtliche Bewertung

Mit Inkrafttreten der zugehörigen Verordnung beruht der Umgang mit personenbezogenen Daten zur Realisierung des eCall-Dienstes auf einer Rechtsvorschrift i.S.d. § 4 Abs. 1 BDSG als Erlaubnistatbestand[99], bei deren Erstellung die Vorgaben der Art. 29 Gruppe im Working Paper 125 aus dem Jahr 2006[100] berücksichtigt worden sind[101].

Derzeit wäre der eCall-Dienst ohne Einwilligung der Betroffenen (*zur Einwilligung unten Ziff. 5.3*) jedenfalls über § 28 Abs. 1 Satz 1 Nr. 2 BDSG gerechtfertigt, weil dem Interesse an Verkürzung der Reaktionszeiten der Notdienste und einer Lebensrettung nach einem Unfall[102] keine überwiegenden schutzwürdigen Interessen der Betroffenen entgegenstehen.

Eine Möglichkeit zur Deaktivierung des eCall-Dienstes ist für eine datenschutzgerechte Ausgestaltung nicht erforderlich.[103] Dem Gesetzgeber steht es frei, als Erlaubnistatbestand i.S.d. § 4 Abs. 1 BDSG auch eine Verpflichtung zum Umgang mit personenbezogenen Daten zu normieren, wenn dies durch den Schutzzweck gerechtfertigt ist[104].

90 Http://www.mdm-portal.de/projekt.html.

91 Http://service.mdm-portal.de/mdm-portal-application/.

92 Dazu oben Fn. 3.

93 Http://www.pressebox.de/pressemitteilung/bmw-ag-0/Automatischer-Notruf-mit-Ortung-in-allen-BMW-Automobilen-erhaeltlich/boxid/61214.)

94 Der genaue Zeitpunkt hängt vom Inkrafttreten der „Verordnung über Anforderungen für die Typgenehmigung zur Einführung des bordeigenen eCall-Systems in Fahrzeuge und zur Änderung von Richtlinie 2007/46/EG", die derzeit nur als Vorschlag COM(2013)316 final (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2013:0316:FIN:DE:PDF) vorliegt und beraten wird, zum Stand des Verfahrens http://ec.europa.eu/prelex/detail_dossier_real.cfm?CL=de&DosId=202791; weitere Details bei Lüdemann/Sengstacken, RDV 2014, 177; Pohle/Zoch, CR 2014, 409 (412).

95 Http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:091:0001:0004:DE:PDF.

96 Http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=OJ:JOL_2014_164_R_0002&from=DE.

97 Ausführlich Lüdemann/Sengstacken, RDV 2014, 177 (178).

98 Zur Kritik an der Einbeziehung der FIN in den MSD Pohle/Zoch, CR 2014, 409 (414).

99 Ausführlich Lüdemann/Sengstacken, RDV 2014, 177 (178).

100 Artikel 29-Gruppe: Working document on data protection and privacy implications in eCall initiative v. 26.9.2006 (http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2006/wp125_en.pdf).

101 Zur Kritik an der verpflichtenden Einführung des eCall-Dienstes Mielchen, ITRB 2014, 110; zu Details der datenschutzrechtlichen Regelungen auf EU-Ebene Pohle/Zoch, CR 2014, 409 (413).

102 Vgl. Erwägungsgrund 6 der Verordnung Nr. 305/2013.

103 Ebenso Pohle/Zoch, CR 2014, 409 (416).

104 Eine Datenverwendungspflicht ergibt sich etwa aus § 25h Abs. 2 S. 1 KWG, die noch durch einen positiv formulierten Erlaubnistatbestand in § 25h Abs. 2 S. 2 KWG ergänzt wird. Zu Rechtsvorschriften als Erlaubnistatbestand Gola/Schomerus, BSDG, § 4 Rn. 7.

4.2.3 Zusatzdienste als Ergänzung des eCall-Dienstes

Datenschutzrechtlich problematisch können jedoch die ggf. neben dem verpflichtenden eCall-Dienst weiterhin möglichen Zusatzdienste sein, die vom Hersteller des Kfz oder Dritten angeboten werden. Denkbar sind insbesondere die Zusammenführung des MSD mit Gesundheitsdaten von Fahrer und Insassen, die aus Sensoren im Kfz gewonnen werden (*dazu oben Ziff. 2.1 und Ziff. 3.2*). Hierfür greifen die gesetzlichen Grundlagen des eCall-Dienstes nicht, so dass es für diese Zusatzdienste eines eigenen Erlaubnistatbestands bedarf, wobei es sich regelmäßig um die Einwilligung des/der Betroffenen handeln wird, wenn diese denn überhaupt zu ermitteln sind.[105]

4.3 Telematik-Tarife in der Kfz-Versicherung

Ein Telematik-basierter Tarif wird derzeit in Deutschland nicht mehr angeboten. Das bislang einzige Angebot, der S-Drive Telematik-Sicherheits-Service Sparkassen Direktversicherung AG[106], war auf 1.000 bereit vergriffene Einheiten beschränkt.

4.3.1 Funktionsweise und Umgang mit personenbezogenen Daten

S-Drive basiert auf einer Trennung der Erhebung und Verarbeitung personenbezogener Daten von deren Nutzung durch den Versicherer zur Bemessung eines Prämienvorteils in der Kfz-Versicherung, die wiederum nur ein Teil des dem Kunden angebotenen Leistungspakets ist[107]. Durch einen Dienstleister werden im ersten Schritt von einer im Kfz installierten Telematik-Box (*zum Begriff oben Ziff. 2.3*) Daten zur Fahrt und zum Fahrverhalten erhoben, ohne dass der Dienstleister jedoch die Kundendaten kennt. Die aus dem Kfz gewonnenen Rohdaten werden im zweiten Schritt mit Kartendaten angereichert und zu Scores i.S.d. § 28b BDSG[108] verarbeitet, bestehend aus einem Gesamtscore und vier Teil-Scores zum Fahrverhalten, zur Geschwindigkeit, zum Anteil der Nachtfahrten und zum Anteil der Stadtfahrten[109].

Auf die Daten zu ihren Fahrten, Scores und Ereignisse haben ausschließlich die S-Drive nutzenden Kunden Zugang über ein Webportal oder eine App (*zu Smart Devices oben Ziff. 2.4*). Der Versicherer erhält ausschließlich die Score-Werte und die im jeweiligen Zeitraum gefahrenen Kilometer mitgeteilt, um hieraus fahrdatenbasiert den etwaigen Nachlass auf den Versicherungstarif zu errechnen. Die Kommunikation erfolgt dabei über eine dem Versicherer und dem Dienstleister jeweils bekannte Kunden-Identifikationsnummer. Im Fall eines von der Telematik-Box ermittelten Unfalls wird außerdem ein Unfallreport an die Deutsche Assistance zur Einleitung von Rettungsmaßnahmen übermittelt.

4.3.2 Datenschutzrechtliche Bewertung

Die Trennung der Erhebung von Fahrt- und Fahrverhaltensdaten ohne Kenntnis des jeweiligen Fahrers von der Nutzung der ausschließlich durch Scores und Angabe einer Gesamtfahrleistung repräsentierten Daten vermeidet zunächst, dass Dienstleister und Versicherer jeweils über einen vollständigen Datensatz (Kundendaten, Fahrtdaten, Fahrverhaltensdaten) verfügen, obwohl dieser mit Blick auf § 3a BDSG zur Zweckerreichung überhaupt nicht erforderlich ist. Es darf allerdings nicht verkannt werden, dass die beim Dienstleister vorhandenen Rohdaten nicht anonymisiert, sondern nur pseudonymisiert i.S.d. § 3 Abs. 6a BDSG sind, so dass der Dienstleister durch Heranziehung weiterer Datenquellen diese wieder personalisieren kann. Ebenso erlauben die dem Versicherer übermittelten Scores zumindest noch die Bildung von Risikoprofilen des jeweiligen Kunden, weil ein schlechter Score aufgrund von Nachtfahrten weniger risikobehaftet ist als ein vergleichbar schlechter Score aus dem Fahrverhalten und der Geschwindigkeit.

Ungeachtet dessen wird die oben beschriebene Verfahrensweise bei einer hinreichenden Datenschutzerklärung (*Unfallmeldung und Datenaufbereitung für den Kunden sind Telemediendienste, dazu oben Ziff. 3.5.3.2*) unter Einführung der notwendigen technischen und organisatorischen Maßnahmen i.S.d. § 9 BDSG datenschutzrechtlich wegen der der Trennung verschiedener Datenquellen gemäß § 28 Abs. 1 S. 1 Nr. 1 BDSG ohne Einwilligung des Fahrers[110] (*zur Einwilligung unten Ziff. 5.3*) zulässig sein[111], wenn die sich aus § 28b BDSG für das Scoring und aus § 6a BDSG für automatisierte Einzelfallentscheidungen geltenden Vorgaben beachtet werden[112]. Auch andere Ausgestaltungen sind auf dieser gesetzlichen Grundlage denkbar.

4.4 Einsatz- und Verhaltenssteuerung

4.4.1 Beispiele zur Einsatz- und Verhaltenssteuerung

Über GPS, RFID[113] oder andere Systeme ermittelte Standortdaten von Kfz, Auflegern, Anhängern, Containern oder Ladungen können einerseits zur Einsatzplanung zwecks Routenplanung oder Nachverfolgung eingesetzt werden, andererseits zur Verhaltenssteuerung, um eine automatisierte Erfassung der betrieblichen und privaten Nutzung eines Kfz oder die Einhaltung vom Arbeitgeber vordefinierter dienstlicher Routen oder effizienter Fahrprofile zu gewährleisten[114]. Die durch solche Loca-

105 Zu Zusatzdiensten und den Schwächen einer Einwilligungslösung Lüdemann/Sengstacken, RDV 2014, 177 (179).

106 Https://www.sparkassen-direkt.de/telematik.html.

107 Schaubilder: http://www.sparkassen-direkt.de/fileadmin/pdf/getrennte.datenkreise.pdf und https://www.sparkassen-direkt.de/fileadmin/pdf/datenfluss.im.ueberblick.pdf.

108 Zum Scoring BGH, Urteil v. 28.1.2014 – VI ZR 156/13 = RDV 2014, 154; Joos, RDV 2014, 157; Gürtler/Kriese, RDV 2010, 47; Behm, RDV 2010, 61.

109 Merkblatt: https://www.sparkassen-direkt.de/fileadmin/pdf/Merkblatt07112013.pdf.

110 Zu den Problemen bei mehreren Betroffenen Lüdemann/Sengstacken, RDV 2014, 177 (180).

111 Ebenso Pohle/Zoch, CR 2014, 409 (411); Weichert, SVR 2014, 241 (246).

112 Soweit im Zusammenhang mit S-Drive von einer durch den Landesbeauftragten für Datenschutz und Informationssicherheit Nordrhein-Westfalen (LDI NRW) erfolgten Prüfung des Verfahrens gesprochen wird, lässt sich diese Angabe nicht nachvollziehen. Eine öffentliche Stellungnahme oder Empfehlung des LDI NRW gibt es nicht.

113 Http://de.wikipedia.org/wiki/RFID, dazu Löw, ZD 2013, 309; Dreyer, ZD 2012, 20; Kesten, RDV 2008, 97.

114 Mit dem sog. Fiskaltaxameter ist dies technisch möglich, dazu http://taxi-magazin.de/taxi/topics/fiskaltaxameter-hamburgs-weg-in-die-schoene-neue-taxiwelt.php.

tion Based Services erlangten Vorteile in Effizienz und Wirtschaftlichkeit der Leistungserbringung haben jedoch zur Folge, dass Bewegungsprofile der betroffenen Fahrer aus den Rohdaten erstellt werden und Fahrer ggf. in Echtzeit auch außerhalb ihrer Arbeitszeit überwacht werden können.

4.4.2 Datenschutzrechtliche Bewertung

Ein gesetzlicher Erlaubnistatbestand für die Erfassung von Standortdaten[115] (*zu Standortdaten bei Anwendung des TKG oben Ziff. 3.5.3.1*) wird sich nur in Ausnahmefällen aus § 28 Abs. 1 S. 1 Nr. 1, Nr. 2 BDSG ableiten lassen, etwa wenn es um die Erfüllung gesetzlicher Vorgaben bei Geldtransporten, die Ressourcen- und Routenplanung bei Logistikern oder die Erbringung von Notfallleistungen im Facility Management geht. Mit Blick auf die Eingriffsintensität von Bewegungsprofilen[116] bedarf es dabei jedoch einer besonders strengen Zweckbindung einschließlich einer unverzüglichen Löschung der angefallenen Daten nach Zweckerledigung und des Verzichts auf die Zusammenführung mit anderen Datenquellen. Ferner ist sicherzustellen, dass im Privatbereich keine Standortdaten erhoben werden, etwa indem die Systeme nach Beendigung der Arbeitszeit deaktiviert werden können. Im Übrigen lässt sich eine nicht anonymisierte Einsatz- und Verhaltenssteuerung nur über eine Einwilligung der Betroffenen realisieren (*zur Einwilligung unten Ziff. 5.3*).

5. Herausforderungen für Unternehmen und Datenschützer

Die Ausführungen zum Stand der Technik (*oben Ziff. 2)*, zum Personenbezug der Daten im und aus dem Kfz sowie deren Zuordnung (*oben Ziff. 3.2 und 3.3*), dem anwendbaren Datenschutzrecht (*oben Ziff. 3.5*) und den Anwendungsfällen aus der Praxis (*oben Ziff. 4*) zeigen die Komplexität des Datenschutzes beim „Connected Car" und den intelligenten Verkehrssystemen. Daraus ergeben sich exemplarisch die nachfolgend beschriebenen besonderen Herausforderungen für Unternehmen und Datenschützer.

5.1 Beschäftigtendatenschutz

§ 32 BDSG ist und bleibt auf absehbare Zeit die einzige Regelung zum Beschäftigtendatenschutz[117]. Die Bundesregierung will vor einem eigenen Tätigwerden zunächst das weitere Gesetzgebungsverfahren auf EU-Ebene bis zur Verabschiedung der allgemeinen Datenschutzverordnung abwarten[118], obwohl im Entwurf in § 82 Datenschutzverordnung[119] ausdrücklich eine Öffnungsklausel zu Gunsten des nationalen Gesetzgebers vorgesehen ist. Für den Umgang mit personenbezogenen Daten durch Anwendungen und Dienste intelligenter Verkehrssysteme (*zum Begriff oben Ziff. 2.2*) im Beschäftigungsverhältnis bleibt es deshalb beim Nebeneinander von § 28 Abs. 1 S. 1 Nr. 2, Nr. 3 BDSG und § 32 BDSG und der ungeklärten Frage zur Freiwilligkeit der Einwilligung eines Arbeitnehmers[120].

5.2 Beteiligung von Beschäftigtenvertretungen

Werden Anwendungen und Dienste intelligenter Verkehrssysteme (*zum Begriff oben Ziff. 2.2*) genutzt, ist dies regelmäßig mit der Einführung und Anwendung technischer Einrichtungen verbunden, die unabhängig von einer entsprechenden Intention des Arbeitgebers zur Überwachung von Verhalten und Leistung der Arbeitnehmer i.S.d. § 87 Abs. 1 Nr. 6 BDSG geeignet ist (*zur Speicherung von Daten im und aus dem Kfz oben Ziff. 2.6*)[121]. Dies ist selbst dann der Fall, wenn Erhebung, Verarbeitung und Nutzung der Daten aus der technischen Einrichtung zeitlich versetzt erfolgen oder die Überwachung nur ein (ggf. sogar nicht gewollter) Nebeneffekt der technischen Einrichtung ist[122]. Es verwundert nicht, dass keiner der zuvor beschriebenen Anwendungsfälle (*dazu oben Ziff. 4*) ohne Systeme (Hardware/Software) auskommt, die als eine solche technische Einrichtung zu qualifizieren sind.

Ist ein Betriebsrat vorhanden, bedürfen Einführung und Anwendung der technischen Einrichtung in diesen Fällen gemäß § 87 Abs. 1 Nr. 6 BetrVG dessen Zustimmung. Entsprechendes gilt für Personalvertretungen. Wird die Zustimmung im Zusammenhang mit einer Betriebsvereinbarung erteilt, kann diese eine Rechtsvorschrift i.S.d. § 4 BDSG und damit ein Erlaubnistatbestand für den Umgang mit personenbezogenen Daten sein[123], ohne dass jedoch das Schutzniveau des BDSG durch die Betriebsvereinbarung in der Summe unterschritten werden darf[124].

5.3 Einwilligung der Betroffenen

Viele praktische Anwendungsfälle (*dazu oben Ziff. 4*) machen ganz oder teilweise den Rückgriff auf eine Einwilligung des oder der Betroffenen erforderlich, wenn nicht mit anonymisierten Daten umgegangen wird (*dazu oben Ziff. 3.2*). Dabei ist die Einwilligung, obwohl mit Blick auf den mit jedem Umgang mit personenbezogenen Daten zunächst einhergehenden Grundrechtseingriff naheliegend (*dazu oben Ziff. 3.3*), wegen der Schwächen in der Praxis der denkbar schwächste Erlaubnistatbestand.

Neben den bekannten Problemen zur Form, Informiertheit, Bestimmtheit und Widerruflichkeit der Einwilligung[125] sowie deren Freiwilligkeit im Beschäftigungsverhältnis (*dazu oben Ziff. 5.1*) ist bei Anwendungen und Diensten intelligenter Verkehrssysteme (*zum Begriff oben Ziff. 2.2*) die Ermittlung der Betroffenen und deren Ansprache zwecks Einholung der Einwilligung eine Herausforderung[126]. Neben dem Halter und Fahrer

115 Ausführlich Weichert, SVR 2014, 201 (206).

116 Dazu Weichert, SVR 2014, 241.

117 Zum Verlauf des Gesetzgebungsverfahren im Beschäftigtendatenschutz nach Einführung des § 32 BDSG http://gesetzgebung.beck.de/node/1002468, zum Beschäftigtendatenschutz insgesamt Wybitul, NZA 2014, 225; Hornung/Knieper, ZD 2014, 383; Pötters/Traut, RDV 2013, 132; Gola, RDV 2012, 60; Thüsing, RDV 2011, 163.

118 BT-Drucksache 18/1122 v. 10.4.2014, S. 3: http://dip21.bundestag.de/dip21/btd/18/011/1801122.pdf.

119 Dazu Fn. 43.

120 Dazu Gola/Schomerus, BDSG, § 4a Rn. 65 f.

121 Ausführlich Kania, Erfurter Kommentar zum Arbeitsrecht, § 87 Rn. 48 ff.

122 Grundlegend BAG, Beschluss v. 10.7.1979 – 1 ABR 50/78 zum Fahrtenschreiber.

123 Gola/Schomerus, BDSG, § 4 Rn. 10 f.

124 Grundlegend BAG, Beschluss v. 27.5.1986 – 1 ABR 48/84 = RDV 1986, 199.

125 Hierzu Lüdemann/Sengstacken, RDV 2014, 177 (181); Weichert, SVR 2014, 241 (243).

126 Lüdemann/Sengstacken, RDV 2014, 177 (180).

können eben auch Insassen und Dritte wie Familienangehörige und Fuhrparkverantwortliche vom Umgang mit personenbezogenen Daten betroffenen sein. Dies gilt insbesondere dann, wenn das Kfz zu verschiedenen Zwecken (betrieblich, privat) genutzt wird.

5.4. Technische und organisatorische Maßnahmen zur Datensicherheit

Anwendungen und Dienste intelligenter Verkehrssysteme (*zum Begriff oben Ziff. 2.2*) bedürfen besonderer technischer und organisatorischer Maßnahmen gemäß § 9 BDSG nebst Anlage. Dies gilt insbesondere für die Weitergabekontrolle (Nr. 4 Anlage zu § 9 BDSG) und die Eingabekontrolle (Nr. 5 Anlage zu § 9 BDSG).

Anders als den Hersteller des Kfz oder den Betreiber einer Telematik-Box (*dazu oben Ziff. 2.3*) stellt dies Arbeitgeber und Fuhrparkbetreiber jedoch vor enorme Herausforderungen, verlangt die Einbindung der Kfz in das betriebliche Datensicherheitskonzept doch Kenntnis von dem im Einzelnen stattfindenden Umgang mit personenbezogenen Daten im Kfz, der jedoch bislang kaum oder gar nicht dokumentiert ist und von den Herstellern der Systeme (Hardware/Software) als Betriebsgeheimnis vor Zugriffen Dritter geschützt wird und dem Zugriff durch Dritte entzogen ist[127]. Wie soll aber ein Arbeitgeber oder Fuhrparkbetreiber seinen Verpflichtungen aus § 9 BDSG etwa durch Verschlüsselung der Daten im Kfz nachkommen, wenn ihm hierzu sowohl Zugang als auch technische Möglichkeiten fehlen?

Dieser offensichtliche Widerspruch zwischen den Pflichten der verantwortlichen Stelle und deren tatsächlichen Möglichkeiten lässt sich derzeit nur lösen, wenn die Hersteller oder Betreiber der Anwendungen und Dienste intelligenter Verkehrssysteme selbst die erforderlichen technischen und organisatorischen Maßnahmen treffen, die für einen datenschutzkonformen Umgang mit personenbezogenen Daten erforderlich sind.

6. Fazit

„Connected Car" und intelligente Verkehrssysteme bringen alle Zutaten für den Alptraum eines jeden Datenschützers mit:

- *schlecht oder nicht dokumentierte Hardware und Software,*
- *fehlendes technisches Verständnis für die Personenbeziehbarkeit der erhobenen Daten,*
- *Schwierigkeiten bei Ermittlung und Ansprache der Betroffenen,*
- *eine Vielzahl von nebeneinander und miteinander agierenden verantwortlichen Stellen,*
- *Einsatz von Big-Data-Technologien, und*
- Umgang mit personenbezogenen Daten in der Cloud.

Solange im Datenschutz am Verbot mit Erlaubnisvorbehalt festgehalten wird, bedarf es deshalb vor Einführung und Anwendung intelligenter Verkehrssysteme und der hierauf beruhenden Anwendungen und Dienste einer sorgfältigen Ermittlung von Sachverhalt, (Rechts-)Beziehungen der Beteiligten und deren datenschutzrechtlicher Zulässigkeit.

Viel wäre schon gewonnen, wenn Hersteller und Dienstleister den Empfehlungen des 52. Verkehrsgerichtstags[128] nachkommen, insbesondere:

- *verständliche und dokumentierte Information der Betroffenen bei Erwerb und Nutzung des Kfz über den Umgang mit personenbezogenen Daten im und aus dem Kfz und die damit verfolgten Zwecke,*
- *Einräumung technischer und rechtlicher Möglichkeiten zur Kontrolle und Unterbindung des Umgangs mit personenbezogenen Daten im und aus dem Kfz („privacy by default"[129] und „privacy by design"), sowie*
- *Bestimmung und Umsetzung der technischen und organisatorischen Maßnahmen zur Datensicherheit.*

Hierbei handelt es sich um datenschutzrechtliche Selbstverständlichkeiten, die freilich bislang vielfach ignoriert werden.

127 Kritisch auch Weichert, SVR 2014, 241 (244).
128 Zusammenfassung bei Born, NZV 2014, 154 (158).
129 Dazu Pohle/Zoch, CR 2014, 409 (411).

Sascha Kremer
Sascha Kremer ist Fachanwalt für Informationstechnologie-Recht und Partner bei LLR LegerlotzLaschet Rechtsanwälte in Köln (www.llr.de). Zugleich ist er Geschäftsführer der LLR DSC GmbH (www.llrdsc.de) und als externer Datenschutzbeauftragter tätig. Er unterrichtet als Lehrbeauftragter an der Heinrich-Heine-Universität Düsseldorf und der Hochschule Bonn-Rhein-Sieg. Spezialisiert ist er auf das Informationstechnologie-Recht nebst den Bezügen zum Gewerblichen Rechtsschutz (insb. Urheberrecht, Wettbewerbsrecht) und das Datenschutzrecht, ebenso auf die praktische Umsetzung des Datenschutzes und der IT-Sicherheit in Unternehmen.

Benjamin Rüdiger

Smart Home – intelligentes Wohnen ohne Privatsphäre?

Verschiedene Anbieter verkaufen das intelligente Wohnen zum Nachrüsten für das eigene Zuhause. Welche Systeme stecken dahinter und was wissen Hersteller über die Menschen, die diese Systeme in den eigenen vier Wänden nutzen?

I. Einleitung

Was versteht man überhaupt unter dem Begriff Smart Home? Welche Möglichkeiten eröffnen sich hier für den Nutzer bzw. welche Vorteile bietet Smart Home?

Unter Smart Home wird das intelligente Vernetzen und Steuern der in einem Haushalt vorhandenen Elektronik verstanden. Ziel ist es, dem Nutzer durch Energieeinsparung und Komfortgewinn einen Mehrwert zu bieten.

Heutzutage gehört es zum Standard eines jeden Haushaltes, dass die Heizungsanlage über einen Außenfühler und Innenthermostate gesteuert wird, um die gewünschte Raumtemperatur zu erreichen. Smart Home Systeme gehen noch viel weiter. Sie ermöglichen eine komplexe Steuerung der Heizung, z.B. das Hinterlegen unterschiedlicher und individueller Heizgewohnheiten. Gleichzeitig können Smart Home Systeme die Raumtemperatur sowie die Luftfeuchtigkeit überwachen und sogar erkennen, ob ein Fenster geöffnet wurde. In diesem Fall würde der Heizvorgang durch das Schließen der Heizthermostate sofort unterbrochen.

Außerdem ist es möglich, alle Vorgänge aus der Ferne über das eigene Smartphone oder via Internet von jedem Rechner aus zu überwachen und zu steuern. Der Vorteil liegt auf der Hand: Der Nutzer kann kurz vor Feierabend aus dem Büro bequem die Heizung zu Hause ansteuern und die gewünschte Raumtemperatur eingeben, also individuell heizen.

II. Was leisten nachrüstbare Smart Home Systeme?

All das, was früher zu Beginn eines Neubaus mit viel Verkabelung früh bedacht werden musste, kann heute über den Einbau von Schaltern, Steckdosen, Bewegungsmeldern und weiteren Sensoren durch den Nutzer selbst nachgerüstet werden. Im Gegensatz zu dem bereits beim Neubau eingeplanten Smart Home System, welches meistens das zusätzliche Verlegen von Kabeln erforderlich macht, bieten nachrüstbare Smart Home Systeme jedem Nutzer die Möglichkeit, in den Genuss einer intelligenten Steuerung der Hauselektronik bzw. der im Haushalt vorhandenen elektronischen Geräte zu kommen, ohne zusätzlich Kabel verlegen zu müssen. Über ein hausinternes Funknetzwerk kommunizieren alle verbauten Smart Home Endgeräte, also Schalter, Steckdosen, Sensoren etc. miteinander. Das Herzstück dieses Netzwerks bildet die Smart Home Zentrale, bei der alle Fäden zusammenlaufen. Sie wird einfach an den eigenen Internetanschluss sowie die Steckdose angeschlossen und kommuniziert per Funk mit den verbauten Smart Home Endgeräten.

Letztere verfügen – soweit erforderlich – in der Regel über eine eigene Stromversorgung (Batterie), so dass sich ein weiterer Stromanschluss erübrigt. Der Nutzer muss sie über die Funkverbindung nur in das Smart Home System einbinden. Konfiguriert wird das Smart Home System über den eigenen Computer, auf dem die Software des Herstellers installiert wird, oder noch einfacher über eine vom Hersteller betriebene Internetplattform, die sich mit der Smart Home Zentrale verbindet. Über die Software bzw. die Internetplattform lassen sich dann auch alle Smart Home-Schalter, Steckdosen und Sensoren einbinden, individuell zuordnen bzw. konfigurieren.

III. Smart Home Systeme sind flexibel und individuell einsetzbar

Der Nutzer kann zum Beispiel einen Türsensor an der Haus- bzw. Wohnungseingangstür anbringen. Werden dann noch ein paar Schalter und/oder Steckdosen durch Smart Home Schalter und Steckdosen ersetzt, kann z.B. das folgende Szenario konfiguriert werden: Mit dem Öffnen der Tür innerhalb eines bestimmten Zeitfensters (z.B. abends) werden verschiedene Lampen und elektronische Geräte ein- oder ausgeschaltet. Dabei kann der Nutzer auch bestimmen, welchen Dimmungsgrad er sich für welche Lampe wünscht, in welcher Reihenfolge und mit welchem Zeitabstand die Geräte ein- oder wieder ausgeschaltet werden sollen.

Das zuvor beschriebene Szenario dürfte eines der unkompliziertesten sein. Angesichts der Entwicklung der Hauselektronik (z.B. internetfähige Waschmaschinen, Trockner, Kühlschränke etc.) im Allgemeinen sowie der von den Herstellern für Smart Home Systeme angebotenen Erweiterungen (z.B. Bewegungsmelder, Rauchmelder, Kameras, Auslesegeräte für Stromzähler, Rollladensteuerung etc.) kann man sich unendlich viele mögliche Szenarien vorstellen.

Zwei weitere Szenarien zeigen, wie flexibel und individuell einsetzbar Smart Home Systeme sind: Das eigene Heim kann aus dem Urlaub derart gesteuert werden, dass es dort immer noch bewohnt aussieht. Auch der Garten kann, je nach Wetterlage (Verknüpfung mit einem Wetterdienst), weiterhin nach Bedarf bewässert werden. All das lässt sich über eine App auf dem Smartphone bequem und zuverlässig steuern.

Wer seine eigenen vier Wände in Abwesenheit überwachen möchte, kann dies durch die Verknüpfung von Tür- und Fenstersensoren mit Bewegungsmeldern tun. Abonniert der Nutzer zusätzlich einen sog. Mehrwertdienst, erhält er eine SMS an die hinterlegte Telefonnummer, die ihn darüber informiert, welcher Sensor soeben ausgelöst hat. Diese Funktion steht bei einzelnen Herstellern auch für Rauchmelder zur Verfügung. Der Konfiguration des Smart Home Systems sind, je nach Hersteller, kaum Grenzen gesetzt. Der Nutzer entscheidet, was wann passieren soll, indem er einzelne Smart Home Endgeräte einander so zuordnet, dass das gewünschte Szenario zum gewünschten Zeitraum ausgelöst wird.

Verfügt der Nutzer über einen Energiespeicher, z.B. eine Photovoltaikanlage auf dem Dach seines Hauses, so kann er

diese ebenfalls in sein Smart Home System einbinden, wie folgendes Beispiel veranschaulicht: Der Nutzer kann in Abwesenheit, z.B. vom Büro aus, die Wasch- oder Spülmaschine einschalten, wenn die eigene Photovoltaikanlage dafür die nötige Energie liefert. Eine unnötige Energieentnahme aus dem öffentlichen Energienetz entfällt dann. Da es jedoch unkomfortabel ist, selbst darauf achten zu müssen, wann die Photovoltaikanlage die erforderliche Energie liefert, kann auch hierfür eine entsprechende Konfiguration hinterlegt werden (z.B. Trockner einschalten, wenn Energie aus Photovoltaikanlage vorhanden oder Batteriespeicher voll ist). Als Batteriespeicher kann auch das eigene Elektroauto dienen, sofern vorhanden. Der Nutzer muss nur die Ladesäule mit in das Smart Home System einbinden. Ist das Elektroauto dann an die Ladesäule angeschlossen, prüft Smart Home, wieviel Energie zur Verfügung steht. Smart Home wird auch sicherstellen, dass nicht zu viel Energie entnommen wird, wenn es weiß, wann der Nutzer das Elektroauto wieder benötigt und für welche Strecke. All das kann der Nutzer seinem Smart Home System „beibringen".

IV. Erstinstallation und Konfiguration des Smart Home Systems

Hat der Nutzer das Smart Home System gekauft, muss er es zu Hause installieren. Wie bereits dargestellt, liegt der Mehrwert eines Smart Home Systems darin, den eigenen Haushalt sowie alle durch das Smart Home System zur Verfügung stehenden Funktionen ständig von jedem Ort aus steuern und überwachen zu können. Hierzu bieten einzelne Hersteller von Smart Home Systemen eine Internetplattform (nachfolgend Back-End genannt) an, über die das Smart Home System konfiguriert und gesteuert werden kann.

Zunächst wird zu diesem Zweck die Smart Home Zentrale vom Nutzer im Back-End registriert. Die Registrierung erfolgt im Rahmen der Einrichtung eines Benutzerkontos im Back-End, welches mittels Kennwort geschützt ist. Zuletzt werden die Smart Home Endgeräte (Schalter, Steckdosen, Sensoren etc.) über die Smart Home Zentrale in das Back-End eingebunden.

Über eine grafische Benutzeroberfläche kann nun das gesamte Smart Home System inklusive der Endgeräte mit persönlichen Einstellungen und Szenarien konfiguriert werden. Schaltvorgänge, Betriebszustände der Smart Home Endgeräte, Energieverbräuche und -einspeisungen können angezeigt werden.

V. Wo sind Smart Home Systeme erhältlich und welche Daten werden beim Kauf eines Smart Home Systems gespeichert?

Die Smart Home Systeme werden von den Herstellern im Internet oder im Fachhandel zum Kauf angeboten. Im Fachhandel kann der Nutzer das Smart Home System inklusive Zubehör kaufen, ohne seinen Namen und seine Anschrift zu hinterlassen.

Bei einem Kauf über das Internet ist es hingegen erforderlich, dass der Nutzer den Herstellern bzw. Anbietern der Smart Home Systeme seine Namens- und Anschriftsdaten mitteilt, die dann auch gespeichert werden. Nur wenige Hersteller ermöglichen dem Nutzer den Kauf im Internet, ohne dass dieser ein persönliches Benutzerkonto anlegen muss.

Bei einem Kauf im Internet fällt aus Sicht des Nutzers auf, dass hier bereits Daten erhoben werden, die einer späteren anonymen Nutzung des Smart Home Systems im Wege stehen.

Um dem Nutzer dennoch eine möglichst anonymisierte bzw. zumindest pseudonymisierte Nutzung seines Smart Home Systems anbieten zu können, müssen die Hersteller darauf achten, welche Daten sie an welcher Stelle erheben und wie lange diese gespeichert werden. Bereits bei der Entwicklung und dem späteren Verkauf der Smart Home Systeme sollten sie sich in Bezug auf folgende Aspekte festlegen:

- Sollen Kauf- und Nutzungsdaten überhaupt miteinander verknüpft werden?
- Wie lange sollen Kauf- und Nutzungsdaten überhaupt gespeichert werden?
- Zu welchen Zwecken werden die Kaufdaten verarbeitet? Sollen diese auch für weitere Produktempfehlungen erhoben werden?
- Wie weitreichend sollen die Zwecke für die Nutzungsdaten sein? Werden diese nach Wegfall der Zweckbindung, also direkt nach dem Aussenden eines Steuerimpulses, wieder gelöscht?
- Wie werden insbesondere die Nutzungsdaten geschützt?
- Gibt es Möglichkeiten der Anonymisierung oder Pseudonymisierung der Kauf- und Nutzungsdaten?

Im Zusammenhang mit all diesen Fragen zeigt sich, dass eine Trennung der IT-Systeme für den Verkauf (Webshop) und die spätere Nutzung des Smart Home Systems (Back-End) datenschutzrechtlich von Vorteil ist. Die Nutzungsdaten dürften einem sehr hohen Schutz unterliegen. Nur wenige Mitarbeiter sollten überhaupt Zugriffsrechte für das IT-System der Nutzungsdaten und damit für das „Herz" des Smart Home Systems erhalten.

VI. Datenerhebung bei Kauf und Erstregistrierung des Smart Home Systems

Hat der Nutzer sein Smart Home System nach seinen Vorstellungen konfiguriert, kann er es ab sofort zur intelligenten Steuerung aller in seinem Haushalt vorhandenen elektrischen Geräte nutzen. Ab diesem Zeitpunkt entscheidet sich durch die vom Hersteller vorgegebenen Prozesse, wie genau der Nutzer für den Hersteller zu identifizieren ist.

An dieser Stelle könnten die Hersteller von Smart Home Systemen den Gedanken „privacy by design" aufgreifen und umsetzen, um dem Nutzer eine möglichst anonymisierte bzw. pseudonymisierte Nutzung des Smart Home Systems zu ermöglichen. Folgende Fragen spielen in diesem Zusammenhang eine wichtige Rolle:

- Werden die IT-Systeme, welche die Kaufdaten (Namens- und Anschriftsdaten, Bankverbindungsdaten, gekaufte Produkte etc.) des Nutzers aus einem ggf. vorhandenen Webshop speichern, von denjenigen für den Betrieb des Back-End und den dort entstehenden Nutzungsdaten getrennt?
- Werden bei der Registrierung Namens- und Anschriftendaten oder andere Daten des Nutzers erhoben, die es den Herstellern ermöglichen, diese Registrierungsdaten mit den

ggf. vorhandenen Daten aus dem Verkauf des Smart Home Systems zu verbinden?

- Kann der Nutzer einen Benutzernamen frei wählen?

VII. Welche Möglichkeiten zur anonymisierten bzw. pseudonymisierten Nutzung von Smart Home Systemen gibt es heute bereits?

Das Trennen der IT-Systeme für den Verkauf von denjenigen, die das Smart Home System steuern, ist technisch möglich und trägt dazu bei, dem zuvor erwähnten Grundgedanken „privacy by design" gerecht zu werden. Eine Verknüpfung beider IT-Systeme dürfte nur dann erforderlich werden, wenn der Nutzer Mehrwertdienste (z.B. SMS-Benachrichtigung etc.) bestellt.

Darüber hinaus könnte es sein, dass die Hersteller das Back-End ebenfalls kostenpflichtig anbieten. Doch selbst in diesem Fall sollten die Hersteller die IT-Systeme so gestalten, dass z.B. die Bezahlung von Mehrwertdiensten und die anschließende Freischaltung die Grundsätze der Datensparsamkeit einhalten.

Eine Möglichkeit, in den genannten Fällen so wenig Daten wie möglich zu erheben, ist die Vergabe eindeutiger Seriennummern für das Smart Home System bzw. die Smart Home Zentrale und alle Smart Home Endgeräte. Solche eindeutigen Seriennummern ermöglichen dann den weitestgehend anonymen bzw. pseudonymen Verkauf von Mehrwertdiensten: Der Nutzer müsste den Mehrwertdienst nur für die Seriennummer seiner Smart Home Zentrale kaufen, ohne seine Namens- und Anschriftendaten anzugeben. Durch technische Maßnahmen ließe sich zudem der Bezahlprozess von der späteren Freischaltung des Mehrwertdienstes trennen. Auf diese Weise wäre die anonymisierte bzw. pseudonymisierte Nutzung des Smart Home Systems weiterhin sichergestellt.

Die Hersteller sollten den Kunden ihrer Webshops sowohl die Variante einer personenbezogenen Registrierung anbieten als auch eine Registrierung ohne jegliche Angabe von Namens- und Anschriftsdaten.

Die zuvor genannten Möglichkeiten für die anonymisierte bzw. pseudonymisierte Nutzung des Smart Home Systems müssten von den Herstellern bereits bei der Entwicklung ihrer Smart Home Systeme bedacht und berücksichtigt werden.

VIII. Wie werden diese Möglichkeiten umgesetzt?

Hersteller sollten darauf achten, das Back-End weitestgehend autark zu betreiben. Kann der Nutzer sich mit einem von ihm frei wählbaren Benutzernamen bzw. einer von ihm frei wählbaren E-Mail-Adresse anmelden, so kann er selbst entscheiden, wie sehr Benutzername oder E-Mail-Adresse seinem tatsächlichen Namen entsprechen.

Erst wenn der Nutzer einen Mehrwertdienst in Anspruch nähme (z.B. SMS-Benachrichtigung bei Alarm durch Brandmelder), müssten die Daten aus dem Webshop (Kauf und Bezahlung des Mehrwertdienstes) mit den Daten aus dem Back-End verknüpft werden. Für die Freischaltung des Mehrwertdienstes wäre dies nur kurzzeitig erforderlich. Außerdem müsste ausschließlich die Information an das Back-End übermittelt werden, welcher Mehrwertdienst für welche Smart Home Zentrale mit welcher Seriennummer bereitgestellt wird. Im Anschluss an diese Datenübermittlung müsste keine weitere Verbindung zwischen den IT-Systemen Webshop und Back-End bestehen.

IX. Welche Daten werden bei der Nutzung von Smart Home Systemen verarbeitet?

Mit der Erstinstallation und der anschließenden Nutzung des Smart Home Systems fallen nicht nur Daten für die Registrierung im Smart Home System an. Wie bereits dargestellt, kann der Nutzer verschiedene Szenarien, also persönliche Einstellungen, vornehmen, die alle im Back-End gespeichert werden. Darüber hinaus werden die für den Betrieb des Smart Home Systems erforderlichen Daten, die mit jedem Schaltvorgang entstehen, im Back-End gespeichert. Das Smart Home System (und damit das Back-End) muss also ständig Daten über den Zustand der angeschlossenen Geräte und Sensoren bereithalten. Diese kann der Nutzer sich auf Wunsch anzeigen lassen, sie ermöglichen das Steuern der Geräte oder lösen ggf. die automatisierten Schaltvorgänge aus, die der Nutzer konfiguriert hat. Durch die Nutzung des Smart Home Systems fallen also die meisten Daten an:

- *Benutzernamen und Kennwörter des Nutzers und möglicher Mitnutzer.* Diese sind für die Anmeldung am Back-End erforderlich und müssen für die Dauer der Nutzung des Smart Home Systems gespeichert werden.
- *Namen für Räume, Smart Home Endgeräte und Szenarien.* Der Nutzer sowie mögliche Mitnutzer können hier individuelle Bezeichnungen wählen. Diese Daten werden ständig benötigt.
- *Steuerimpulse.* Für jeden Schaltvorgang werden Steuerimpulse erzeugt, die den Schaltvorgang überhaupt erst ermöglichen. Diese sind für den Nutzer selbst nicht sichtbar. Da die Steuerimpulse nach Abschluss des Schaltvorgangs nicht mehr benötigt werden, sind diese unmittelbar danach wieder zu löschen.
- *Protokolldaten von Schaltvorgängen.* Sofern der Hersteller es anbietet, kann der Nutzer sich sogenannte Protokolldateien über erfolgte Schaltvorgänge erstellen lassen. Dies bietet sich zum Beispiel bei Tür- und Fenstersensoren an. So ist ersichtlich, wann ggf. ein Fenster geöffnet wurde oder ob ein Fenster geöffnet ist. Protokolldateien sollten dem Nutzer so zur Verfügung gestellt werden, dass sie von ihm selbst gelöscht werden können.
- *Fehlerprotokolle.* Kommt es zu einer Fehlfunktion des Smart Home Systems, werden bei einigen Herstellern Fehlerdateien erzeugt. Diese bieten dem Nutzer die Möglichkeit, sich mit dem Hersteller in Verbindung zu setzen, um dann Unterstützung bei der Fehlersuche zu erhalten. Es gibt Hersteller, die solche Fehlerdateien aus Datenschutzgründen bereits heute schon nur auf der Smart Home Zentrale und damit zunächst unzugänglich für den Hersteller selbst speichern. Stellt der Nutzer einen Fehler fest, kann er selbst die Fehlerdatei auslesen und dem Hersteller zusenden.
- *Weitere Daten.* Diese Auflistung ist nicht abschließend, da die ständige Weiterentwicklung der Smart Home Systeme neue Funktionen zur Verfügung stellt und damit ggf. auch neue Daten verarbeitet werden.

X. Können Daten, die bei der Nutzung von Smart Home Systemen erhoben, verarbeitet und genutzt werden, auch wieder gelöscht werden?

Was geschieht mit den Daten des Nutzers, wenn er sich dazu entscheidet, das Smart Home System nicht mehr selbst zu nutzen, sondern es zu verkaufen?

In diesem Fall werden Daten zur persönlichen Konfiguration sowie aus der Nutzung des Smart Home Systems gespeichert sein, die nun einer dritten Person zur Verfügung stehen könnten.

Hat der Nutzer die Pflicht, diese Daten zu löschen, oder müssen die Hersteller einen Prozess anbieten, der die Löschung der Daten ermöglicht bzw. sogar sicherstellt?

Vor dem Hintergrund der aktuell laufenden Datenschutzdiskussionen rund um das Thema „privacy by design" täten die Hersteller von Smart Home Systemen gut daran, einen Minimalstandard zu implementieren, welcher im Falle eines Besitzerwechsels des Smart Home Systems die Datenlöschung vorsieht.

XI. Wie und wann könnte eine derart automatisierte Löschung von Daten erfolgen?

Es gibt Smart Home Systeme, bei denen der Nutzer mit der Registrierung im Back-End den Benutzernamen und das Kennwort erst nach Eingabe einer – von der Smart Home Zentrale automatisch generierten und im Display erscheinenden – Ziffern- und Buchstabenfolge vergeben kann. Dieser Schritt, der bei der Erstregistrierung des Smart Home Systems vollzogen wird, könnte im Falle eines Besitzerwechsels genauso gut die Datenlöschung sicherstellen. Möchte der neue Besitzer des Smart Home Systems seinerseits die Erstregistrierung im Back-End vornehmen, muss er vor der Vergabe von Benutzername und Kennwort ebenso zuerst die auf dem Display der Smart Home Zentrale erscheinende, neue Ziffern- und Buchstabenfolge im Back-End eingeben. Das Back-End stellt nun fest, dass die eindeutige Seriennummer der Smart Home Zentrale mit einer neue Ziffern- und Buchstabenfolge verknüpft wird. Das Back-End bekommt also die Aufforderung, dass der Registrierungsschritt neu durchlaufen werden soll bzw. dass ein neues Benutzerkonto angelegt werden soll. Somit werden alle zuvor erfolgten Registrierungen sowie die in diesem Zusammenhang erstellten Benutzerkonten überschrieben. Auf diese Weise könnten alte Daten einer Löschroutine zugeführt werden.

Der Nutzer, der sich nun neu registriert hat, kann beim Durchlaufen des beschriebenen Prozesses nicht nur einen eigenen Benutzernamen und ein eigenes Kennwort eingeben. Durch diesen Prozess wird gleichzeitig sichergestellt, dass der neue Nutzer nicht auf die Daten des Vorbesitzers bzw. auf die Daten aus einer anderen Registrierung zugreifen kann.

Unabhängig von einem möglichen Besitzerwechsel sollte dem Nutzer die Möglichkeit zur Datenlöschung ständig eingeräumt werden.

XII. Anonymisierung, Pseudonymisierung und „privacy by design". Was ist möglich, was ist nötig?

Bisher wurde aufgezeigt, wie und wo Smart Home Systeme verkauft, welche Daten dabei erhoben werden und wie der Nutzer die Erstregistrierung des eigenen Smart Home Systems vornehmen kann. Die Möglichkeiten einer anonymen oder pseudonymen Nutzung von Smart Home Systemen sind deshalb so wichtig, weil sich durch die dabei gespeicherten und verarbeiteten Daten genaue Rückschlüsse auf die Lebensgewohnheiten des Nutzers ziehen lassen. Sie zeigen auch, wann wer zu Hause ist und wann nicht.

Es mag durchaus vertretbar sein, dass die Hersteller von Smart Home Systemen ihre Kunden in gewisser Art und Weise kennen möchten, um ihnen – passend zu bereits erworbenen Smart Home Systemen – neue Produkte anbieten zu können. Hierfür ist allerdings die Kenntnis der Nutzungsdaten aus dem Smart Home Back-End nicht zwingend erforderlich. Ein weiteres Argument spricht gegen das Speichern von personenbezogenen Daten im Back-End: Kriminalität im Internet! Immer mehr IT-Systeme werden von gezielten Hackerangriffen erfasst. Kriminelle könnten sich z.B. darauf spezialisieren, das Back-End auszuspionieren, um dann genau zu den Zeiten einzubrechen, zu denen garantiert niemand zu Hause ist.

Zusammenfassend sind unter Berücksichtigung des Gedankens der Datensparsamkeit folgende Maßnahmen für eine bestmögliche Anonymisierung bzw. Pseudonymisierung der Nutzungsdaten zu nennen:

- Trennung von Webshop und Back-End.
- Registrierung im Back-End über einen vom Nutzer frei wählbaren Benutzernamen bzw. eine frei wählbare e-Mail-Adresse.
- Dauerhafte Speicherung von Daten und Schaltvorgängen bzw. Erstellen von Protokollen über Schaltvorgänge nur dann, wenn der Nutzer diese Funktion selbst aktiv eingeschaltet hat. Bei der Auslieferung von Smart Home Systemen an den Nutzer sollte diese Funktion deaktiviert sein.
- Fehlerdateien sollten physisch nur auf der Smart Home Zentrale gespeichert werden. Somit kann der Nutzer selbst entscheiden, wann er die Fehlerdatei ggf. an den Hersteller schickt, um Unterstützung bei der Fehlersuche zu erhalten.
- Hinweise für ggf. zugelassene Mitnutzer, wer welche Daten einsehen kann.
- Überschreiben von Szenarien oder Protokolldateien, wenn das Smart Home System den Besitzer wechselt.

Es muss damit gerechnet werden, dass die Smart Home Systeme auch von solchen Nutzern eingesetzt werden, die im eigenen Haushalt einfach und bequem Energie einsparen möchten, ohne sich mit jeder technischem Möglichkeit auseinanderzusetzen. Diese Gruppe von Nutzern sollte für die Hersteller von Smart Home Systemen der Maßstab sein. Der Grundsatz der Datensparsamkeit bzw. der Datenvermeidung wird nämlich nur dann gewahrt, wenn das Smart Home System mit einer Grundeinstellung ausgeliefert wird, die das massenhafte und dauerhafte Speichern von Schaltvorgängen verbie-

tet, es sei denn, der Nutzer wünscht dies ausdrücklich und aktiviert eine entsprechende Funktion.

Ebenso wichtig ist in diesem Zusammenhang auch, dass der Nutzer bereits vor der Nutzung des Smart Home Systems mit Hilfe einer gut verständlichen Datenschutzerklärung bei der Registrierung darüber informiert wird, was er zum Schutz seiner Privatsphäre tun kann (z.B. nicht den echten Namen und Vornamen als Benutzernamen nutzen). Doch auch während der Nutzung sollte der Nutzer bei relevanten Prozessschritten (z.B. Aktivierung der Protokollierung von Schaltvorgängen) darüber informiert werden, welche Daten wie lange gespeichert werden und wie diese wieder gelöscht werden können.

XIII. Wie wichtig ist Datensicherheit bei Smart Home Systemen?

Sobald die Smart Home Zentrale mit dem Internet und somit dem Back-End verbunden ist, über welches – zumindest für kurze Zeit – alle Schaltvorgänge laufen, besteht die Möglichkeit, Einstellungen zu verändern oder Schaltvorgänge zu unterbinden bzw. auszulösen.

Nicht zu vergessen sind an dieser Stelle alle eingebundenen Smart Home Endgeräte, die über Funk mit der Smart Home Zentrale kommunizieren. Diese Funkverbindungen wären ggf. der einfachste und ideale Angriffspunkt, um dem Nutzer Schaden zuzufügen. Je nach Umfang des vom Nutzer installierten Smart Home Systems kann bereits an dieser Stelle mit entsprechender krimineller Energie in das Smart Home System und damit in dessen Steuerung eingegriffen werden.

Geht man zudem davon aus, dass die Möglichkeiten der Smart Home Systeme und der in Zukunft einzubindenden Smart Home Geräte immer größer werden, könnte im Falle eines Missbrauchs auch der Schaden größer werden.

Die Hersteller sollten daher die folgenden Aspekte gut durchdenken und bei der Grundausstattung und Grundeinstellung von Smart Home Systemen berücksichtigen:

- Das Back-End, über das alle Steuerimpulse laufen und in dem die Einstellungen des Nutzers gespeichert werden, sollte nur in einem Rechenzentrum mit entsprechend hohen Schutzstandards betrieben werden.
- Die Smart Home Zentrale muss automatisch eine verschlüsselte Internetverbindung zum Rechenzentrum aufbauen.
- Die Funkverbindungen zwischen der Smart Home Zentrale und den Smart Home Endgeräten müssen ebenfalls verschlüsselt werden.
- Bei der Registrierung der Smart Home Zentrale im Back-End muss ein komplexes Passwort erzwungen werden.
- Beim Einbinden neuer Smart Home Endgeräte muss ein Standardprozess sicherstellen, dass die richtigen Smart Home Endgeräte eingebunden werden; also eben nicht die Endgeräte eines Nachbarn, der zufällig das Smart Home System des gleichen Herstellers verwendet.

XIV. Big Data-Analysen bei Smart Home Systemen

Hersteller von Smart Home Systemen sowie deren Datenschützer sollten sich vor einer geplanten Big Data-Analyse unbedingt eine Reihe von Fragen stellen, um bei der Durchführung der Analyse dann entsprechend datenschutzkonforme Lösungen zu finden:

- Welchen Mehrwert kann der Hersteller mit den Daten aus dem Webshop oder dem Back-End von Smart Home Systemen erzielen?
- Kann der Hersteller die Ziele bzw. den Zweck der Datenanalyse beschreiben und absehen?
- Verfügt der Hersteller über die im Aufsatz beschriebene Trennung der IT-Systeme (Webshop und Back-End)?
- Mit welchen Daten aus welchem IT-System können die gewünschten Ziele am besten erreicht werden?
- Können Zweck und Ziel derart beschrieben werden, dass eine evtl. erforderliche Einwilligung des Nutzers für die Datenanalyse ausreichend ist?

Diese Fragen zeigen auf, welche datenschutzrechtlichen Herausforderungen an eine Big Data-Analyse gestellt werden.

Bei vielen Big Data-Analysen stehen Zweck und Ziel vor der dann erfolgenden Datenverarbeitung noch nicht fest. Hersteller und Unternehmen mit Kundendaten führen Big Data-Analysen durch, um Auffälligkeiten bzw. Merkmale des eigenen Kundenkreises überhaupt erst herauszufiltern. Erst dann erfolgen die nächsten Schritte wie z.B. eine Datenanreicherung oder die gezielte Ansprache der Kunden.

In einem solchen Fall liegt die datenschutzrechtliche Herausforderung in der datenschutzkonformen Machbarkeit. Mag die Big Data-Analyse der Kaufdaten aus dem IT-System für den Webshop noch einfach zu rechtfertigen sein, kann dies mit den Daten aus dem Back-End durchaus schwierig werden, da es sich nicht nur im Listendaten, sondern ggf. um besonders schutzwürdige Daten handelt. Wie ist also am besten vorzugehen, um bei einer Datenanalyse einen datenschutzkonformen Weg zu wählen?

Fokussieren wir uns auf die datenschutzrechtlich größere Herausforderung, also auf die Big Data-Analyse von Daten aus dem Back-End, sind folgende Aspekte datenschutzrechtlich zu prüfen:

- Es kann nicht für jeden Datensatz eines jeden Nutzers im Back-End die 100%ige Anonymität sichergestellt werden. Es wird Nutzer geben, die ggf. ihre personenbezogene E-Mail-Adresse (vorname.nachname@xy.de) als Benutzernamen einsetzen.
- Auch wenn das Back-End autark betrieben wird und bewusst auf das Erheben von personenbezogenen Daten verzichtet wird, dürfte in den meisten Fällen die Möglichkeit bestehen, mit wenig Aufwand den Personenbezug über eindeutige Zuordnungskriterien (Seriennummer der Smart Home Zentrale bzw. Smart Home Endgeräte) des evtl. gesondert betriebenen Webshops herzustellen. Diese Möglichkeit führt zu dem Ergebnis, dass die im Back-End gespeicherten Daten als pseudonymisierte Daten zu betrachten sind.
- Big Data-Analysen mit pseudonymisierten Daten bedürfen der Einwilligung des Nutzers.
- Die Anforderungen an eine Einwilligung machen es erforderlich, dem Nutzer den vorgesehenen Zweck der Datenverarbeitung zu nennen. Zweck und Ziel der Big Data-Analyse müssen also vor der Datenerhebung festgelegt und verständlich erklärt werden.

Wenn all diese Schritte wohl überlegt und gezielt dargestellt wurden, kann die entsprechende Einwilligungserklärung eine Big Data-Analyse ermöglichen. Sofern der Hersteller jedoch neue Geschäftsideen und/oder Geschäftskooperationen entwickeln möchte, steht das Entwickeln vor allen anderen zu verfolgenden Schritten. Dies bedeutet, dass der Hersteller ggf. Zweck und Ziel seiner geplanten Datenanalyse noch nicht genau beschreiben kann, bevor er eben diese Daten nicht analysiert hat. Dies ist eine datenschutzrechtliche Problematik, die bei Big Data-Analysen nicht selten vorkommen dürfte.

Für solche Fälle könnten die folgenden Lösungsansätze datenschutzrechtliche Ansatzpunkte darstellen, um auch ein solches Vorhaben nicht unmöglich erscheinen zu lassen:

- Das gezielte Analysieren von Daten aus dem Back-End könnte mit „Testusern" durchgeführt werden, die von Anfang an in eine solche umfangreiche Auswertung einwilligen bzw. nur zu diesem Zweck das Smart Home System nutzen. Die Testuser werden also in einer etwas umfangreicher gestalteten Vereinbarung darüber informiert, dass der Hersteller die Daten für das Entwickeln von Geschäftsideen und Geschäftskooperationen analysiert. Im Gegensatz zu der Einwilligung des Nutzers, der das Smart Home System bereits nutzt, wird der Testuser von Anfang an über die umfangreiche Datenauswertung auf „Feldebene" informiert und kann über eine entsprechende Vereinbarung mit dem Hersteller seine Einwilligung erklären.
- Vorhandene Daten aus dem Back-End könnten auch derart anonymisiert werden, dass die Rückführbarkeit auf die einzelne Person unmöglich wird (jegliche Zuordnungskriterien durch nicht rückführbare Hashwerte ersetzen). Dies führt jedoch häufig nicht zu dem gewünschten Ergebnis, da die Rückführbarkeit zur Person erforderlich ist, um Geschäftsideen und Geschäftskooperation erfolgreich an der Zielgruppe auszurichten.

Das Thema „Big Data" dürfte also ebenfalls oder vielleicht insbesondere im Bereich von Smart Home interessant für die Hersteller sein. Dabei sollten allerdings nicht ausschließlich die Vorteile für den Hersteller betrachtet werden, sondern es sollte auch das Ziel verfolgt werden, den Nutzer an dem Mehrwert von Smart Home Systemen teilhaben zu lassen. Je nach Umfang und Ausstattung des Smart Home Systems könnten die folgenden Aspekte sowohl für den Hersteller als auch für den Nutzer von Vorteil sein. Sie können auch dem Thema Big Data zugeordnet werden, wenn weitere Datenanalysen oder Geschäftskooperationen geplant werden:

- Durch das Erheben von Stromverbrauchsdaten und die anschließende grafische Aufbereitung für den Nutzer könnte gezielt nach „Stromfressern" gesucht werden. Der Nutzer könnte sich seine Energieverbrauchsdaten auf die Minute genau anzeigen lassen und sehen, was er zur jeweiligen Zeit im Haushalt gemacht hat und wieviel Energie dabei verbraucht wurde (z.B. Staubsauger).
- Es könnten Ziele zur Energieeinsparung „erzwungen" werden. Hierzu könnte der Betroffene seinen Stromverbrauch pro Monat oder Tag als eigenes Ziel angeben. Droht eine Überschreitung dieses Ziels, könnte durch das Auslesen der Stromverbrauchsdaten bestimmt werden, welche Energieverbraucher für den Monat oder Tag nicht mehr eingeschaltet werden (z.B. Gartenbeleuchtung) sollten. Das Smart Home System würde die entsprechenden Geräte nur einschalten, wenn der Energieverbrauch den vom Nutzer eingegebenen Wert nicht überschreitet.

Je nach Umfang und Ausstattung des Smart Home Systems lassen sich viele weitere Ideen entwickeln, die in die genannte Richtung gehen. Für die Hersteller von Smart Home Systemen ist es wichtig, den Datenschutz früh genug in ihre Überlegungen bzw. in die Entwicklung ihrer Produkte einzubinden, um die Daten eben auch für diese Zwecke und die sich daraus ggf. ableitenden Geschäftsideen (z.B. Produktempfehlung für einen effizienteren Staubsauger etc.) nutzen zu können.

Big Data für die Energiewende? Dies ist keine Vision, sondern bereits heute möglich und in Nachbarländern schon tägliche Praxis.

XV. Fazit mit einem Blick in die Zukunft

Sicherlich werden Smart Home Systeme in Zukunft mehr und mehr unser Leben in die Komfortzone rücken. Wenn Freunde zu Besuch kommen, wird der Gang durch das Wohnzimmer, um Beleuchtung und Musik richtig einzustellen, von einem kurzen Bedienen der Smart Home App auf dem eigenen Smartphone abgelöst werden. Wir werden mit dem eigenen Smartphone die bequeme Kontrolle über Raumtemperatur, offene Fenster oder Türen sowie über smarte Geräte im eigenen Haushalt haben, angefangen beim Babyphone, über die Gartenbeleuchtung bis hin zur Videoüberwachung der Haustür. Alles, was sich elektronisch steuern und überwachen lässt, kann vom Smart Home System erledigt werden, wenn wir es ihm „beibringen" oder ihm unsere Gewohnheiten verraten. Die Smart Home Systeme werden uns sicherlich auch bei den Zielen zur Energieeinsparung unterstützen.

Dabei sollten die Hersteller aber keinesfalls ausschließlich Komfortgewinn und Energieeinsparung als Ziele vor Augen haben. Das Recht auf informationelle Selbstbestimmung des Nutzers sollte durch „privacy by design" sichergestellt werden können. Auch die Gewährleistung des Datenschutzes sollte nicht auf den Nutzer allein abgewälzt werden, der sich im schlechtesten Fall durch komplexe Menüs klicken muss, um die Privatsphäreeinstellungen zu aktivieren. Aufgrund der besonders sensiblen Nutzungsdaten aus Smart Home Systemen tragen Hersteller hier eine besondere Verantwortung.

Benjamin Rüdiger
Benjamin Rüdiger berät seit über 10 Jahren Unternehmen aus der Energiewirtschaft zu datenschutzrechtlichen Fragestellungen. Bevor er stellvertretender Konzern-Datenschutzbeauftragter bei RWE wurde, war er u.a. als Datenschutzbeauftragter von verschiedenen RWE-Töchtern tätig. Er spezialisierte sich dabei auf das Thema Kundendatenschutz und Elektromobilität und referiert hierzu bei Verbänden der Energiewirtschaft.

Kurzbeiträge

Aus den aktuellen Berichten der Aufsichtsbehörden (15): Datenschutz in der Arztpraxis

Ausgewählt und kommentiert von Prof. Peter Gola, Königswinter*

Allgemeines

Patientendaten zählen bereits dann zu den speziellen Datenschutz genießenden Gesundheitsdaten (besondere Arten personenbezogener Daten gemäß § 3 Abs. 9 BDSG), wenn nur eine indirekte Aussage über die Gesundheit dadurch gemacht wird, dass jemand bei einem Arzt in Behandlung ist. Zudem unterliegen sie der besonderen Schweigepflicht des § 203 Abs. 1 Nr. 1 StGB. Neuen bereichsspezifischen Datenschutz enthalten zudem die mit dem Gesetz zur Verbesserung der Rechte von Patientinnen und Patienten vom 20.2.2013 (BGBl. I, S. 277; vgl. Reif, RDV 2013, 193) in das BGB eingefügten Vorschriften der §§ 630a–630h über den „Behandlungsvertrag". Aber auch hier sehen die Aufsichtsbehörden, da der Gesetzgeber ihre Vorschläge (Beschluss des Düsseldorfer Kreises vom 23.5.2012; u.a. Anlage 13 zum XI. TB, 2011/3.2013, des LfD Sachsen-Anhalt) weitgehend nicht berücksichtigte, noch Datenschutzmängel (LDA Brandenburg, TB 2012/2013, Ziff. 6.1; LfD Sachsen-Anhalt XI TB, 2011/3,2013, Ziff. 10.1.8).

Die elektronische Patientenakte

§ 630f Abs. 1 S. 1 BGB sieht vor, dass die die Behandlung dokumentierende Patientenakte in Papierform oder in elektronisch geführt werden kann. Damit ergeben sich für die elektronische Speicherung die gleichen Fragen der Gewährleistung der Richtigkeit und Vertraulichkeit, wie sie bei der Digitalisierung von Personalakten erörtert werden (HessDSB 42. TB, 2013, Ziff. 4.9.1.2). § 630f Abs. S. 2 BGB schreibt dazu vor, dass Berichtigungen und Änderungen von Eintragungen nur zulässig sind, wenn neben dem ursprünglichen Inhalt erkennbar bleibt, wann sie vorgenommen worden sind. Auch hier stellt sich Frage der Vernichtung von Originalunterlagen mit der Konsequenz des Wegfalls des Urkundenbeweises nach § 419 ZPO. So kann beispielsweise beim Einscannen ohne weiteres ein neues „Dokument" entstehen, das sich aus dem Inhalt und der Unterschrift verschiedener Dokumente zusammensetzt. Zumindest muss durch eine möglichst fälschungssichere, dem Gericht nachweisbare Organisation der elektronischen Dokumentation das Prozessrisiko minimiert werden.

Das Foto in der Patientenakte

Zur ordnungsmäßen Dokumentation der Behandlung in der Patientenakte ist es regelmäßig nicht erforderlich, ein bei dem Beginn der Behandlung gefertigtes Foto des Patienten der Patientenakte beizufügen (HessDSB, 42. TB, 2013, Ziff. 4.9.1). Der Eingriff in das Recht am eigenen Bild kann nicht durch den Wunsch nach späterer Identifikation des Patienten und zur Vermeidung von Verwechslungen begründet werden (LfDI Mecklenburg-Vorpommern, 11. TB, 2012/2013, Ziff. 6.6.1) und ist daher von der freiwilligen und widerrufbaren, den Anforderungen des § 4a BDSG entsprechenden, d.h. dem Patienten freigestellten, Einwilligung abhängig (HessDSB, 42. TB, 2013, a.a.O.). Eine Ablehnung der Behandlung kommt jedenfalls im Hinblick auf den zuvor genannten Speicherungsgrund nicht in Betracht. Anders kann es sein, wenn bestimmte Krankheitsbilder per Foto dokumentiert werden sollen. So hat es der HessDSB (42. TB, 2013, Ziff. 4.9.1.5) als zulässig angesehen, wenn der Arzt bei einem Hausbesuch behandlungsbegleitende Fotos auf seinem Mobiltelefon oder iPad speichert, um sie alsbald auf den Praxisrechner zu überspielen.

Vorlage des Personalausweises und Aufnahme einer Kopie in die Patientenakte

Regelmäßig nicht als erforderlich sieht es der BlnBDI (JB 2013, Ziff. 8.7) an, dass ein Patient sich vor Abschluss des Behandlungsvertrages durch Vorlage des Personalausweises identifizieren soll. Ohne Vorliegen besonderer Anhaltspunkte ist ein solches Verlangen unzulässig. Ausreichend ist, dass sich die Person mit ihrer Krankenversichertenkarte ausweist. Ohne auf die Zulässigkeit nach dem Personalausweisgesetz einzugehen, wird in jedem Falle die Anfertigung einer Kopie des Ausweises und deren Ablage in der Patientenakte als unzulässig verneint.

Mitnahme von Krankenhauspatientendaten in die neue eigene Praxis

Nicht beanstandet es der HessDSB (42. TB, 2013, Ziff. 4.9.1.6), wenn ein liquidationsberechtigter Krankenhausarzt, der sich selbständig macht, die Patientenunterlagen über die von ihm erbrachten und abgerechneten Leistungen nunmehr in seiner Praxis aufbewahrt und den Patienten über seinen neuen Wirkungsort und die dort angebotenen Therapien informiert. Der DSB äußert sich jedoch nicht zu der Rechtsgrundlage, die die diesbezügliche Nutzung der Patientenakte rechtfertigt. Wahrscheinlich stellt er noch auf die Zweckbestimmung des ehemaligen Behandlungsvertrages (§ 28 Abs. 1 S. 1 Nr. 1 BDSG) ab, wenn er wie folgt ausführt: „Letztlich dürfen Patientendaten in dem Umfang genutzt werden, wie dies dem Behandlungsvertrag zwischen Arzt und Patient dient. .... Das Schreiben trug

* Der Autor ist Ehrenvorsitzender der Gesellschaft für Datenschutz und Datensicherheit e.V., Bonn.

dazu bei, über die neue Wirkungsstätte des Arztes zu informieren, damit bei Bedarf eine Weiterbehandlung erfolgen kann". Das setzt aber voraus, dass der Behandlungsvertrag zumindest noch Nachwirkungen hat. Eher zutreffend ist es, dieses Schreiben als nach § 28 Abs. 3 BDSG zulässige Werbung zu bewerten.

Übersendung von Patientendaten per Telefax

Eine Übermittlung personenbezogener Daten per Telefax birgt Risiken hinsichtlich der Wahrung der Vertraulichkeit der übermittelten Daten (vgl. die von verschiedenen Aufsichtsbehörden erhältliche Orientierungshilfe Datenschutz und Telefax). Diesen ist auch speziell bei der Übersendung von Arzt zu Arzt Rechnung zu tragen (LfDI Mecklenburg-Vorpommern, 11. TB, 2012/2013, Ziff. 6.6.1). Der Berliner BDI (JB 2013, Ziff. 5.13) führt dazu wie folgt aus: „Beim Faxversand ist zu bedenken dass jeder, der Zugang zum Empfangsgerät hat, Einblick in die übermittelten Daten nehmen kann. Eine aus datenschutzrechtlicher Sicht sichere Anonymisierung vor dem Versand birgt jedoch bei dem Empfänger häufig die gerade im Gesundheitswesen ggf. schwerwiegende Gefahr einer Verwechselung mit sich. Um somit datenschutz- und berufsrechtliches Fehlverhalten durch unbefugtes Offenbaren zu vermeiden, sollten in der Regel folgende schriftlich zu fixierende Kommunikationsregeln beachtet werden:

- Personenbezogene Gesundheitsdaten sollten nur dann gefaxt werden, wenn eine schnelle Übermittlung erforderlich ist; soweit risikolos möglich, sollten die Unterlagen anonymisiert werden.
- Vor dem Versenden muss geprüft werden, ob die Faxnummer des Empfängers noch aktuell ist.
- Es muss sichergestellt sein, dass die richtige Faxnummer des Empfängers eingegeben wurde; regelmäßig sollten daher die gespeicherten Kurzwahlnummern auf Richtigkeit überprüft werden. Zur Absicherung sollte hierbei das Vier-Augen-Prinzip eingehalten werden.
- Das eigene Faxgeräte muss so aufgestellt sein, dass nur Berechtigte Einblick in und Zugriff auf eingehende Faxe haben.
- Im Zweifel oder z.B. bei einem längere Zeit nicht angewählten Empfänger sollte vor dem Versenden (telefonisch) geklärt werden, ob und dass auch beim Empfänger die datenschutz- und berufsrechtlichen Anforderungen eingehalten werden und das Fax angekündigt wird.
- Um sicher zu gehen, dass der allein Berechtigte das Fax in Empfang nimmt, sollte mit dem Empfänger vor der Versendung bei Bedarf ein bestimmter Übermittlungszeitpunkt vereinbart werden.
- Die Faxvorlage darf nach dem Versenden nicht im Faxgerät liegengelassen werden.

Schweigepflichtentbindungserklärungen in AGBs

Mit dem Passus im Anmeldebogen: „ Es gelten unsere allgemeinen Geschäftsbedingungen (AGB, siehe Aushang)" können keine nach § 4a BDSG erforderlichen schriftliche Einwilligungserklärungen eingeholt werden. Das gilt umso mehr, wenn zugleich mehrere nach unterschiedlichen Kriterien zu betrachtende Einverständnisse erteilt werden sollen, wie ein von dem HessDSB (42. TB, 2013, Ziff. 4.9.1.3) zu beurteilender Fall belegt. Dabei ging es nicht nur um die Übermittlung von Behandlungsdaten an andere an der Behandlung beteiligte Ärzte, Krankenhäuser oder medizinische Labore, sondern zum einen um die „ausdrückliche" Einwilligung, zu informations-, termin-, recall- und medizinischen Zwecken von der Praxis schriftlich, fernmündlich oder per Telefax, SMS oder E-mail kontaktiert zu werden, und zum anderen um die Weitergabe der Daten zum Zwecke der Rechnungslegung an die der Schweigepflicht unterliegende privatärztliche Verrechnungsstelle XY.

Beide Erklärungen scheitern auch u.a. auch schon daran, dass ihr Inhalt zu pauschal und unbestimmt ist. Ein Patient muss, bevor er sich entscheidet, ob er der Weitergabe seiner Daten an eine ärztliche Verrechnungsstelle zustimmt, eine konkrete Vorstellung haben, wer welche Daten wozu erhält, d.h. er muss u.a. wissen, ob der Arzt für seine Daten weiter verantwortlich bleibt, d.h. ob ein Fall der Auftragsdatenverarbeitung vorliegt oder ob die Rechnungsstelle als Funktionsübernehmer verantwortlich wird (LfD Baden-Württemberg, 31. TB, 2012/2013, Ziff. 7.9).

Gleiches gilt, wenn der Arzt die Möglichkeit haben will, ein Inkassobüro einzuschalten. Inkassounternehmen benötigen, jedenfalls wenn kein Forderungsübergang gewollt ist, zur außergerichtlichen Beitreibung der offenen Forderung keine kompletten Befund- und Therapieberichte, sondern nur die die sich aus der Rechnung ergebenden Informationen über durchgeführte Behandlungsmaßnahmen. Keiner schriftlichen Einwilligung des Patienten zur Einschaltung des Inkassounternehmens bedarf es dann, wenn der Arzt bereits in einem zweiten Mahnschreiben wiederholt die Einschaltung des Inkassobüros angekündigt hat (HessDSB, 42. TB, 2013, Ziff. 4.9.1.4.2).

Zulässig ist es auch, vor der Aufnahme der Behandlung die Einwilligung in eine Bonitätsanfrage einzuholen, wobei ein die Anfrage rechtfertigendes Kreditgeschäft bei gesetzlich Versicherten besteht, wenn z.B. ein Zahnarzt über den gesetzlichen Leistungsumfang hinaus besondere privatärztlich abzurechnende Leistungen vereinbart. Die Einwilligung darf erst eingeholt werden, wenn der Patient über die insoweit auf ihn zukommenden Kosten aufgeklärt ist. Wie der HambBfDI (24. TB, 2012/2013, III. Ziff. 5.6) festhält, darf die Einwilligung nicht durch die Androhung der Behandlungsverweigerung erzwungen werden. Dem Patienten muss ggf. auch angeboten werden, sie durch Vorkasse oder Sicherheitsleistung abzuwehren.

Weitergabe der Patientenakte an einen Praxisnachfolger

Beanstandet hat der HessDSB (42. TB, 2013, Ziff. 4.9.1.3) auch eine wohl vorsorglich eingeholte Erklärung, mit der die Weitergabe der Behandlungsunterlagen an einen möglichen Praxisnachfolger akzeptiert werden sollte. Die Erklärung ist keine „informierte" Einwilligung, da der Umfang der Bewerbungsunterlagen, der Zeitpunkt der Übergabe und insbesondere der konkrete Empfänger noch völlig offen sind.

Aus der digitalen Agenda der Bundesregierung – das geplante IT-Sicherheitsgesetz

RA Levent Ferik, LL.M., Bonn*

I. Vorbemerkung

Das technische Konzept der Vermittlung von IP-Paketen, und damit der wesentliche Unterbau dessen, was heute umgangssprachlich, aber ungenau als Internet bezeichnet wird, stammt bekanntlich aus den frühen sechziger Jahren (1962). Wollte man ein Jahr festmachen, an dem dieses, ehemals einem recht exklusiven Klientel vorbehaltene, Netz seinen Siegeszug durch alle Bevölkerungsschichten begann, und in den darauf folgenden Jahren ein nicht mehr wegzudenkender Bestandteil sowohl des Wirtschaftslebens als auch des sozialen Lebens wurde, dann wäre dies das Jahr 1993, als Marc Andreessen einen Browser namens „Mosaic" veröffentlichte, der bald dem World Wide Web und auch dem gesamten Internet ungekannte Popularität jenseits der bisherigen Nutzerkreise und ein explosionsartiges Wachstum bescherte[1].

Beseelt von der Einsicht, dass die Menschen zunehmend in einer digital vernetzten Welt leben und diese digitale Vernetzung den Arbeitsplatz, die Schule, die Universität sowie das Privatleben betrifft, hat die aktuelle Bundesregierung über 20 Jahre nach dem Siegeszug des Netzes die sog. Digitale Agenda 2014-2014 vorgestellt, um endlich die Grundsätze ihrer Digitalpolitik bekannt zu geben[2].

Abseits der Stellungnahmen zu den sonstigen Grundsätzen und Punkten der Digitalen Agenda hat die Vorstellung des Entwurfs eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) besonders viel Resonanz hervorgerufen.

Die Tatsache allein, dass der Entwurf vom Bundesministerium des Innern (BMI) kommt, zeigt bereits die weitere Erkenntnis, in welch hohem Maß unsere Gesellschaft und wesentliche Teile unseres Gemeinwesens von einer funktionierenden Informationstechnik und sicheren Informationsinfrastrukturen abhängig sind, und wie sehr die Beeinträchtigung dieser Vernetzung oder schlimmstenfalls ein gezielter Angriff auf diese Infrastruktur auch die innere Sicherheit Deutschlands gefährden könnte.

II. Altes und Neues

Das BMI hatte bereits am 12. März 2013 den Referentenentwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme[3] vorgestellt. Der damalige Bundesinnenminister Dr. Hans-Peter Friedrich konnte drei Schwerpunkte zur Verbesserung der IT-Sicherheit in dem vorgestellten Entwurf festmachen.

Die Betreiber kritischer Infrastrukturen sollten zum einen zu einer Verbesserung des Schutzes der von ihnen eingesetzten Informationstechnik und zur Verbesserung ihrer Kommunikation mit dem Staat bei IT-Vorfällen verpflichtet werden. Zum anderen sollten gleichzeitig Telemediendienstanbieter, denen eine Schlüsselrolle für die Sicherheit des „Cyberraumes" zugestanden wurde, stärker als bis dahin für diese ihnen zugewiesene Schlüsselrolle zur Verantwortung gezogen werden können. Darüber hinaus sah es der damalige Bundesinnenminister als erforderlich an, das BSI in seinen Aufgaben und Kompetenzen zu stärken, um die gewünschten Resultate tatsächlich erzielen zu können.

Der jüngste Entwurf des BMI scheint an einigen Stellen ambitionierter[4]. Sprach die Bundesregierung im Koalitionsvertrag[5] noch lediglich darüber, Mindestanforderungen an die IT-Sicherheit für Kritische Infrastrukturen zu schaffen, soll nun nicht nur der Schutz der Verfügbarkeit, Integrität und Vertraulichkeit der datenverarbeitenden Systeme verbessert werden, sondern, über die Optimierung der CIA Triade hinaus, sowohl die IT-Sicherheit der Unternehmen verbessert als auch der Schutz der Bürgerinnen und Bürger hinsichtlich des Netzes, in dem sie sich bewegen, gestärkt werden. Abweichend vom alten Entwurf soll in diesem Zusammenhang nicht nur das BSI, sondern auch das BKA eine Stärkung erfahren. Der Anspruch ist nicht geringer, als dass die IT-Systeme und digitalen Infrastrukturen Deutschlands die sichersten weltweit werden sollen.

III. Adressaten und Maßnahmen

Enthielt der Koalitionsvertrag 2014[6] lediglich die vage Maßgabe, die Betreiber kritischer Infrastrukturen durch Kooperation und gesetzliche Vorgaben anhalten zu wollen, die Widerstandsfähigkeit (Resilienz) und Schutzmaßnahmen zu verbessern, konkretisiert der Entwurf diese Vorgabe. Vor allem Betreiber sogenannter kritischer Infrastrukturen, z.B. aus dem Energie-, Wasser-, Transport- oder Finanzwesen, sollen Sicherheitsvorfälle unter Mitwirkung von Warn- und Alarmierungskontakten zukünftig an das Bundesamt für Sicherheit in der Informationstechnik (BSI) melden. Unter die Definition passen gemäß der zu ergänzenden Absätze 10 und 11 des BSI-Gesetzes alle Unternehmen, die von hoher Bedeutung für das Funktionieren des Gemeinwesens sind und durch deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe oder erhebliche Störungen der öffentlichen Sicherheit eintreten würden.

* Rechtsanwalt Levent Ferik, LL.M. ist stellvertretender Geschäftsführer der Gesellschaft für Datenschutz und Datensicherheit (GDD) e.V.

1 Wikipedia: http://de.wikipedia.org/wiki/NCSA_Mosaic.

2 Digitale Agenda 2014-2017, http://www.bmwi.de/DE/Themen/Digitale-Welt/digitale-agenda.html.

3 Im Folgenden: IT-Sicherheitsgesetz.

4 BMI: http://www.bmi.bund.de/SharedDocs/Downloads/DE/Gesetzestexte/Entwuerfe/Entwurf_IT-Sicherheitsgesetz.pdf.

5 Koalitionsvertrag für die 18. Legislaturperiode, S. 104, https://www.cdu.de/sites/default/files/media/dokumente/koalitionsvertrag.pdf.

6 Koalitionsvertrag für die 18. Legislaturperiode, S. 104, https://www.cdu.de/sites/default/files/media/dokumente/koalitionsvertrag.pdf.

Der Entwurf sieht Änderungen in fünf verschiedenen Themenfeldern vor:

1. Verbesserung der IT-Sicherheit bei Unternehmen – insbesondere bei kritischen Infrastrukturen

Betreiber kritischer Infrastrukturen sollen verpflichtet werden, binnen zwei Jahren nach Inkrafttreten der Rechtsverordnung angemessene organisatorische und technische Vorkehrungen und sonstige Maßnahmen zum Schutz derjenigen informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind. Diese Vorkehrungen sollen dann mindestens alle zwei Jahre hinsichtlich der Erfüllung der Anforderungen einer Überprüfung unterzogen werden. Das Gesetz spricht insoweit von der Möglichkeit, die Anforderungen auf geeignete Weise nachzuweisen. Als gangbare Möglichkeit werden Sicherheitsaudits, Prüfungen und Zertifizierungen genannt[7].

Nach § 8b Abs. 5 BSIG-E sind Betreiber kritischer Infrastrukturen nur dann unter Nennung des Betreibernamens unverzüglich zu einer Meldung an das BSI verpflichtet, wenn die Beeinträchtigung der informationstechnischen Systeme, Komponenten oder Prozesse zu einem Ausfall oder einer Beeinträchtigung der Kritischen Infrastruktur führen würde.

Nach § 8b Abs. 4 BSIG-E kann die Meldung durch die Betreiber kritischer Infrastrukturen anonym erfolgen, soweit die Beeinträchtigungen der informationstechnischen Systeme, Komponenten oder Prozesse (lediglich) Auswirkungen auf ihre eigene Funktionsfähigkeit haben können. Angaben zu den technischen Rahmenbedingungen sowie zur Branche des Betreibers müssen jedoch enthalten sein.

2. Schutz der Bürgerinnen und Bürger in einem sicheren Netz

Der angestrebte Schutz soll unter anderem durch die Erhöhung der Sicherheitsstandards bei öffentlichen Telekommunikationsnetzen und den Anbietern von Telemediendiensten erreicht werden[8]. Zusätzlich sollen Telekommunikationsanbieter nicht nur über Cyberangriffe informieren, sondern die Nutzer auch mit Lösungsvorschlägen zur Behebung bzw. Abwehr des Angriffs versorgen. Konkrete, zumindest beispielhaft genannte Erläuterungen wie diese Doppelstrategie in der Praxis aussehen kann, enthält der Entwurf nicht. Als weiteres Element, den Schutz der Bürger in diesem Bereich voranzutreiben, sollen Telemediendiensteanbieter ihren Nutzern sichere Authentifizierungsverfahren anbieten.

3. Schutz der IT des Bundes

Um auch die Bundesregierung selbst stärker in die Pflicht zu nehmen und als Reaktion auf die quantitativ wie qualitativ zugenommenen Angriffe auf Regierungsnetze, sieht der Entwurf eine Erweiterung der Möglichkeiten für verbindliche Vorgaben für die IT des Bundes durch das BSI vor. Hierzu wird die bestehende Regelung für die Regierungsnetze auf die IT des Bundes als Ganzes ausgeweitet.

4. Stärkung des BSI

Der gewachsenen Bedeutung des BSI soll unter anderem durch eine klarere Regelung seiner Warnbefugnisse und seine Etablierung als internationale Zentralstelle Rechnung getragen werden. Um die Erfüllung der im Gesetz vorgesehenen Aufgaben erfolgreich zu verwirklichen, sieht der Entwurf beim BSI einen zusätzlichen Aufwand von insgesamt 133 zusätzlichen Planstellen vor. Weiterhin geht der Entwurf davon aus, dass für die Wahrnehmung der Aufgabe als zentrale Meldestelle für die Sicherheit in der Informationstechnik für die Betreiber kritischer Infrastrukturen der Ausbau des BSI-Lagezentrums auf einen 24/7 Betrieb unausweichlich sein wird[9].

5. Zuständigkeitserweiterung des BKA

Die bestehende Zuständigkeit des Bundeskriminalamts für die polizeilichen Aufgaben auf dem Gebiet der Strafverfolgung soll im Bereich der Cyberdelikte ausgeweitet werden. Gerade bei Angriffen auf bundesweite Einrichtungen sei eine solche klare Zuständigkeitsregelung notwendig. Konkret wird die Zuständigkeit des Bundeskriminalamts für die polizeilichen Aufgaben auf dem Gebiet der Strafverfolgung über die bereits bestehende Zuständigkeit für Straftaten nach § 303b StGB (Computersabotage) hinaus auf Straftaten nach den §§ 202a, 202b, 202c, 263a und 303a StGB ausgedehnt.

IV. Kritik

Obwohl der Referentenentwurf des BMI zunächst innerhalb der Bundesregierung abgestimmt und darauf folgend den beteiligten Kreisen für eine weitere Diskussion überlassen werden soll, hat er bereits unmittelbar nach seiner Veröffentlichung verschiedenste Stellen und Verbände zu ersten Stellungnahmen animiert.

Der BITKOM begrüßt generell die Verbesserungen am IT-Sicherheitsgesetz und nimmt es wohlwollend zur Kenntnis, dass in Bezug auf die Meldepflicht von schwerwiegenden IT-Sicherheitsvorfällen die Hinweise der IT-Industrie weitgehend berücksichtigt worden seien, und bewertet es positiv, dass die Wirtschaft in die konkrete Ausgestaltung des Gesetzes einbezogen werden soll[10].

Die Planungssicherheit sieht der BITKOM hinsichtlich der Frage des Adressatenkreises nachteilig betroffen und wünscht sich hier mehr Klarheit darüber, welche Unternehmen das geplante Gesetz adressieren soll. Darüber hinaus wird angeregt, kleinen und mittelständischen Unternehmen beim Aufspüren von Sicherheitslücken eine bessere Unterstützung zuteil werden zu lassen. Die Forderung nach Anwendung derselben, im Entwurf geforderten Meldepflichten und Sicherheitsstandards

7 Gesetzesbegründung zum Entwurf, Seite 13.

8 Infoblatt des BMI zum IT-Sicherheitsgesetz, S. 2, http://www.bmi.bund.de/SharedDocs/Downloads/DE/Gesetzestexte/Entwuerfe/Infoblatt_IT-Sicherheitsgesetz.pdf?__blob=publicationFile.

9 Referentenentwurf des BMI zum IT-Sicherheitsgesetz, S. 5.

10 BITKOM, http://www.bitkom.org/files/documents/BITKOM-Presseinfo_Entwurf_IT-Sicherheitsgesetz_19_08_2014.pdf.

auch für den Staat stützt der BITKOM darauf, dass dieser der größte Betreiber kritischer Infrastrukturen sei.

Der BITKOM rechnet vor, dass die beabsichtigte Meldepflicht für schwere IT-Sicherheitsfälle für die deutsche Wirtschaft Kosten in Höhe von bis zu 1,1 Milliarden Euro pro Jahr verursachen dürfte. Ausgaben für die Einhaltung höherer Sicherheitsstandards in dreistelliger Millionenhöhe kämen hinzu.

Eine extrem detaillierte Betrachtung der Kosten hatte auch der Bundesverband der Deutschen Industrie e.V (BDI) bereits nach Erscheinen des Referentenentwurfs vom 12. März 2013 in seiner von der KPMG durchgeführten Studie „IT-Sicherheit in Deutschland. Handlungsempfehlungen für eine zielorientierte Umsetzung des IT-Sicherheitsgesetzes" aufgestellt[11]. In seinem Positionspapier[12] „Erwartungen der deutschen Industrie an ein IT-Sicherheitsgesetz" gelangt der BDI zu einem niederschmetternden Ergebnis:

„Der BDI setzt sich nachdrücklich für eine Stärkung der IT-Sicherheit, den Ausbau des staatlichen IT-Lagebilds sowie für einen verbesserten Informationsaustausch zwischen Industrie und Amtsseite ein. Nach Auffassung der deutschen Industrie wird das IT-Sicherheitsgesetz (ITSiG) keines dieser Ziele erreichen."

Der Verband der deutschen Internetwirtschaft e.V. (eco)[13] befürwortet nach eigenen Angaben grundsätzlich die Pläne des Innenministers, Deutschland zum führenden Standort im Bereich IT-Sicherheit auszubauen, rät jedoch davon ab, ein IT-Sicherheitsgesetz als nationalen Alleingang auszugestalten. Nationale Alleingänge seien nicht hilfreich, wenn die im Entwurf genannten Betreiber kritischer Infrastrukturen teilweise europa- bzw. weltweit tätig seien. Die Bundesregierung sollte besser eine europaweite Regelung im Rahmen der geplanten NIS-Richtlinie[14] anstreben, um den betroffenen Unternehmen unnötig hohe Kosten zu ersparen.

Das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD) stört sich daran, dass dem Gesetzentwurf nur beiläufig zu entnehmen sei, dass der Schutz des allgemeinen Persönlichkeitsrechts allgemein und des Datenschutzes speziell ein zentrales Anliegen von IT-Sicherheit ist. Mehr IT-Sicherheit gehe nicht ohne die Einbeziehung und Stärkung der unabhängigen Datenschutzbeauftragten[15].

Der Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V. glaubt daran, dass der auf kritische IT-Strukturen ausgerichtete Gesetzesentwurf insgesamt zur Steigerung der IT-Sicherheit und damit zum Schutz der personenbezogenen Daten der Bürgerinnen und Bürger in Deutschland beitragen kann, und verweist als Beleg darauf, dass die Einführung von Meldepflichten sich im Bereich von Datenschutzverletzungen als Arbeitsinstrument bewährt hat[16].

Die Ausführung des Referentenentwurfs hinsichtlich des prognostizierten Mehraufwands durch Erfüllungskosten sieht zwar auch der BvD, ergänzt jedoch richtigerweise, dass dies faktisch nur dort zu Mehrkosten führen wird, wo bislang noch kein hinreichendes Niveau an IT-Sicherheit bzw. keine entsprechenden Meldewege etabliert sind. Weiter gibt der BvD zu bedenken, dass bei der Etablierung von Mitteilungspflichten der Verfassungsgrundsatz, dass sich niemand selbst belasten muss, Berücksichtigung finden muss.

Der Umstand, dass der Entwurf eine weitere gesetzgeberische Aktivität zum Schutz der Daten der Bürgerinnen und Bürger vermissen lässt, sieht der BvD als einen der Kritikpunkte an dem Entwurf. Als weiterer Kritikpunkt werden die neuen gesetzlichen Befugnisse zum Speichern und Verarbeiten von Nutzerdaten gesehen, die sich im Entwurf im Bereich der Neuerungen zum TMG verbergen. Mit der Kritik, in dem jetzigen Gesetzentwurf werde für jeden Anbieter von Telemediendiensten die Möglichkeit geschaffen, Nutzerdaten in erheblicher Menge vorsorglich zu erheben und zu speichern, steht der BvD nicht allein.

Sowohl der Arbeitskreis Vorratsdatenspeicherung[17] als auch die Piraten[18] haben die Sorge, dass mit dem geplanten Vorhaben bei allen Anbietern von Telemediendiensten Strukturen zum Vorhalten von umfangreichen Nutzerdaten geschaffen werden. Der sich im Gesetzentwurf befindliche Gedanke, Daten von Nutzern zum Erkennen von Störungen zu erheben, entspreche dem Gedanken der Vorratsdatenspeicherung. Unabdingbar seien dafür jedoch strenge Regelungen zur Zweckbindung dieser Daten und die zeitliche Befristung der Erhebung und Verwendung.

V. Gemeinsamer Kritikpunkt: „Versteckte Vorratsdatenspeicherung" (?)

Die Befürchtung einer „versteckten Vorratsdatenspeicherung" wird von diversen Beteiligten geäußert, so dass es sich lohnt, diesen Aspekt noch näher zu beleuchten. Die Gemüter erhitzen sich dabei an den geplanten Änderungen zum Telemediengesetz. Konkret sieht der Entwurf eine neue Regelung in Form des § 15 Abs. 9 TMG-E vor[19].

„Soweit erforderlich, darf der Diensteanbieter Nutzungsdaten zum Erkennen, Eingrenzen oder Beseitigen von Störungen seiner für Zwecke seines Telemedienangebotes genutzten technischen Einrichtungen erheben und verwenden. Absatz 8 Satz 2 gilt entsprechend."

Als Begründung für die geplante Einführung dieser Norm nennt der Gesetzgeber folgende Erwägung:

11 Studie des BDI: http://www.bdi.eu/download_content/SicherheitUndVerteidigung/Anlage_Studie_BDI_Final.pdf.

12 Positionspapier der BDI vom 25.08.2014 „Erwartungen der deutschen Industrie an ein IT-Sicherheitsgesetz", http://www.bdi.eu/download_content/SicherheitUndVerteidigung/Positionspapier_Sicherheitsgesetz_25_02.pdf.

13 Positionspapier des eco e.V. zum IT-Sicherheitsgesetz: http://www.eco.de/2014/news/eco-lehnt-it-sicherheitsgesetz-als-nationalen-alleingang-ab.html.

14 Europäische Kommission: COM(2013) 48 final: http://eeas.europa.eu/policies/eu-cyber-security/cybsec_directive_de.pdf.

15 ULD, https://www.datenschutzzentrum.de/presse/20140820-it-sicherheitsgesetz.htm.

16 Pressemitteilung BvD e.V. vom 22.08.2014 https://www.bvdnet.de/system-ordner/tt-news/detailansicht/article/bvd-unterstuetzt-it-sicherheitsgesetz-grundsaetzlich-und-regt-verbesserungen-an.html.

17 AKVorratsdatenspeicherung: http://www.vorratsdatenspeicherung.de/content/view/748/79/.

18 Piraten Partei: https://www.piratenpartei.de/2014/08/21/it-sicherheitsgesetz-bka-carepaket-enthaelt-auch-vorratsdatenspeicherung/.

19 Referentenentwurf des BMI zum IT-Sicherheitsgesetz, S. 18.

„Diensteanbieter müssen die Möglichkeit haben, eine Infektion der von ihnen angebotenen Telemedien mit Schadprogrammen zu erkennen, um entsprechende Schutzmaßnahmen ergreifen zu können. Hier bestand bislang eine Lücke im Bereich der Erlaubnistatbestände des Telemediengesetzes, denn auch die Telemedienanbieter brauchen eine entsprechende Ermächtigung, beispielsweise um Angriffe (Denial of Service, Schadprogramme, Veränderung ihrer Werbeangebote von außerhalb) abwehren zu können. Zur Erkennung und Abwehr bestimmter Angriffe gegen Webseiten und andere Telemedien ist die Erhebung und kurzfristige Speicherung und Auswertung der Nutzungsdaten erforderlich. Diese soll durch den neuen § 15 Absatz 9 TMG, der sich an § 100 Absatz 1 TKG anlehnt, geschaffen werden. Dabei ist auch eine Weiterentwicklung der Angriffsmethoden zu berücksichtigen."

Nimmt man zur Kenntnis, dass gem. § 15 Abs. 1 TMG zu den in der Regelung erwähnten Nutzungsdaten „Merkmale zur Identifikation des Nutzers, Angaben über Beginn und Ende sowie des Umfangs der jeweiligen Nutzung und Angaben über die vom Nutzer in Anspruch genommenen Telemedien" gehören, die nach der Gesetzesbegründung erhoben und gespeichert werden sollen, ist es keine große Überraschung, dass der erste reflexartige Gedanke in Richtung Vorratsdatenspeicherung geht.

Richtigerweise kommen Teile der Blogosphäre hier zum Schluss, dass bei der Formulierung „Erkennen von Störungen" eine proaktive Speicherung der Daten gemeint sein muss und die Diensteanbieter mit der Speicherung nicht so lange warten müssen, bis ein Angriff stattgefunden hat und seine Auswirkungen eingetreten sind[20].

Ob sich der Vorwurf einer versteckten Vorratsdatenspeicherung auch nach der ersten Aufregung um die geplante Änderung langfristig halten wird, wird sicher davon abhängen, welcher Zeitraum sich hinter der Angabe „kurzfristig" verbirgt. Einen Fingerzeig, welche Fristen in diesem Bereich tolerierbar sein könnten, dürfte jüngst der BGH gegeben haben, der bei der Speicherung von dynamischen IP-Adressen 7 Tage als unbedenklich einstufte[21]. Die teilweise vorgetragene Kritik, dass „der IT-Gesetzesentwurf keine Speicherfristen vorsehe", scheint zumindest an dieser Stelle etwas voreilig und ungenau[22].

VI. Fazit

Die Zahlen sprechen dafür, dass die Einführung eines IT-Sicherheitsgesetzes nicht nur eine gute Idee, sondern eine erforderliche staatliche Maßnahme darstellt.

Die Durchdringung des Gemeinwesens und die Abhängigkeit des Gemeinwesens von einer funktionierenden und sicheren IT-Landschaft kann durch Zahlen des Statistischen Bundesamts und anderer Institutionen und Verbände gut nachgewiesen werden.

87 % der deutschen Unternehmen nutzen einen Internetzugang, wobei 37 % der Unternehmen den direkten Kontakt zu den Kunden über soziale Medien suchen[23]. Allein auf Cloud-Dienste soll eine Bruttowertschöpfung von 78,8 Mrd. EUR entfallen[24]. In Deutschland würden zwar 26 Prozent der Menschen ihren Fernseher weggeben, aber nur 14 Prozent ihr Smartphone[25], wobei 76 % der Deutschen auf einen privaten Internetanschluss zurückgreifen können. 50,4 Millionen Menschen besitzen in Deutschland ein Smartphone. Ein Leben ohne Internet scheint ohne Aufgabe der lieb gewordenen Lebensweise kaum vorstellbar und würde zudem viele wirtschaftliche Prozesse erschweren.

Die IT des Bundes stärker zu schützen, erscheint ebenfalls konsequent wie sinnvoll. Informationstechnik und Kommunikation eröffnen auch in diesem Bereich neue Möglichkeiten und müssen im Bereich der Verwaltung weiter modernisiert werden, um mit der Privatwirtschaft Schritt zu halten. Allein die steigende Zahl der Computer- und Internetkriminalität[26] und der gezielten Angriffe auf IT-Systeme[27] zeigt die Notwendigkeit, den Schutz dieser Systeme als wichtigen Bestandteil einer digitalen Agenda zu führen.

Wenn der Bundesinnenminister zum Gesetzesentwurf erklärt: „Wir müssen sicherer werden als bisher. Wer ein Risiko setzt für andere, trägt dafür auch die Verantwortung. Wer Kritische Infrastrukturen betreibt[28]", der muss sie sicher betreiben ", dann trifft er den Kern dieses Erfordernisses.

Was für andere wichtige Dinge zur Förderung und Aufrechterhaltung des Gemeinwesens gilt, muss auch für die IT-Sicherheit gelten. Eine schnelle Infrastruktur in Form von Breitbandnetzen ist nicht weniger wichtig für das wirtschaftliche Wachstum als der Ausbau und die Wartung von Autobahnen. Wer eine Gefahr auf dieser Autobahn in Form einer Baustelle für andere Verkehrsteilnehmer schafft, muss natürlich Sorge dafür tragen, dass Dritte keinen Schaden nehmen.

Wenn der Betreiber eines Kernkraftwerks sich gegen Katastrophenszenarien wappnen und mit dem Katastrophenschutz beschäftigen sollte, warum sollten sich Betreiber von kritischen Infrastrukturen nicht mit Szenarien beschäftigen, die sowohl die Datensicherheit als auch den Datenschutz betreffen? Die Forderung des Bundesinnenministers scheint also eine Übertragung der sonst üblichen Verkehrssicherungspflichten vom Analogen ins Digitale zu sein.

Allein an Ungenauigkeiten und Ungereimtheiten des Entwurfs, die bereits in den ersten Stellungnahmen anklingen,

20 Delegedata.de, http://www.delegedata.de/2014/08/it-sicherheitsgesetz-telemedienanbieter-duerfen-anlasslos-speichern/.

21 BGH Az.: III ZR 391/13, http://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&nr=68350&Blank=1.pdf.

22 Piraten Partei: https://www.piratenpartei.de/2014/08/21/it-sicherheitsgesetz-bka-carepaket-enthaelt-auch-vorratsdatenspeicherung/

23 Statistisches Jahrbuch 2013, S. 513.

24 BITKOM, http://www.bitkom.org/files/documents/BITKOM_PK_Industrie_4.0_07_04_2014.pdf.

25 SPON: http://www.spiegel.de/netzwelt/web/studie-deutsche-verzichten-lieber-auf-fernseher-als-auf-smartphone-a-979244.html.

26 BITKOM, http://www.bitkom.org/de/presse/8477_79284.aspx.

27 BKA, Bundeslagebild Cybercrime 2013, S. 5, http://www.bka.de/nn_224082/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2013,templateId=raw,property=publicationFile.pdf/cybercrimeBundeslagebild2013.pdf.

28 Pressemitteilung BMI, http://www.bmi.bund.de/SharedDocs/Kurzmeldungen/DE/2014/08/einleitung-ressortabstimmung-it-sicherheitsgesetz.html.

dürfte noch zu arbeiten sein. Unsicherheiten scheinen dahingehend zu bestehen, dass Unternehmen nicht genau einschätzen können, ob sie als Betreiber einer kritischen Infrastruktur in Frage kommen. Die im Rahmen einer Verordnung geplante Regelung könnte hier Abhilfe schaffen. Leichte Zweifel ruft ebenfalls die Frage auf, wie realistisch es sein kann, dass die Unternehmen von der Möglichkeit einer anonymen Meldung beim BSI Gebrauch machen?

Sind die vorgesehenen zwei Jahre, die den Unternehmen für die Festlegung von Mindeststandards für die jeweilige Branche eingeräumt werden, und die das BSI dann absegnen soll, in einer Zeit der rasanten Weiterentwicklung im Bereich der IT-Sicherheit nicht zu lang?

Auch wenn die Zweckbindung bei § 15 Abs. 7 TMG-E gegeben ist, die auf das Erkennen und die Abwehr von Störungen beschränkt sein soll, müssen nicht Vorkehrungen getroffen werden, um eine spätere zweckfremde Verwendung bspw. durch Sicherheitsbehörden auszuschließen?

Diese und andere Fragen werden in einer breiten öffentlichen Debatte zu erörtern sein, um die vom BMI gewünschten wirksamen und sachgerechten Lösungen im Hinblick auf das geplante IT-Sicherheitsgesetz zu finden.

Rechtsprechung

Recht auf Vergessen in Suchmaschinen (Ls)

(**Europäischer Gerichtshof**, Urteil vom 15. Mai 2014 – C-131/12 – Google Spain und Google)

1. **Art. 2 Buchst. b und d der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr ist dahin auszulegen, dass die Tätigkeit einer Suchmaschine, die darin besteht, von Dritten ins Internet gestellte oder dort veröffentlichte Informationen zu finden, automatisch zu indexieren, vorübergehend zu speichern und schließlich den Internetnutzern in einer bestimmten Rangfolge zur Verfügung zu stellen, sofern die Informationen personenbezogene Daten enthalten, als „Verarbeitung personenbezogener Daten" im Sinne von Art. 2 Buchst. b der Richtlinie 95/46 einzustufen ist und dass der Betreiber dieser Suchmaschinen als für diese Verarbeitung „Verantwortlicher" im Sinne von Art. 2 Buchst. d der Richtlinie 95/46 anzusehen ist.**

2. **Art. 4 Abs. 1 Buchst. a der Richtlinie 95/46 ist dahin auszulegen, dass im Sinne dieser Bestimmung eine Verarbeitung personenbezogener Daten im Rahmen der Tätigkeiten einer Niederlassung ausgeführt wird, die der für die Verarbeitung Verantwortliche im Hoheitsgebiet eines Mitgliedstaats besitzt, wenn der Suchmaschinenbetreiber in einem Mitgliedstaat für die Förderung des Verkaufs der Werbeflächen der Suchmaschine und diesen Verkauf selbst eine Zweigniederlassung oder Tochtergesellschaft gründet, deren Tätigkeit auf die Einwohner dieses Staates ausgerichtet ist.**

3. **Art. 12 Buchst. b und Art. 14 Abs. 1 Buchst. a der Richtlinie 95/46 sind dahin auszulegen, dass der Suchmaschinenbetreiber zur Wahrung der in diesen Bestimmungen vorgesehenen Rechte, sofern deren Voraussetzungen erfüllt sind, dazu verpflichtet ist, von der Ergebnisliste, die im Anschluss an eine anhand des Namens einer Person durchgeführte Suche angezeigt wird, Links zu von Dritten veröffentlichten Internetseiten mit Informationen zu dieser Person zu entfernen, auch wenn der Name oder die Informationen auf diesen Internetseiten nicht vorher oder gleichzeitig gelöscht werden, und gegebenenfalls auch dann, wenn ihre Veröffentlichung auf den Internetseiten als solche rechtmäßig ist.**

4. **Art. 12 Buchst. b und Art. 14 Abs. 1 Buchst. a der Richtlinie 95/46 sind dahin auszulegen, dass im Rahmen der Beurteilung der Anwendungsvoraussetzungen dieser Bestimmungen u.a. zu prüfen ist, ob die betroffene Person ein Recht darauf hat, dass die Information über sie zum gegenwärtigen Zeitpunkt nicht mehr durch eine Ergebnisliste, die im Anschluss an eine anhand ihres Namens durchgeführte Suche angezeigt wird, mit ihrem Namen in Verbindung gebracht wird, wobei die Feststellung eines solchen Rechts nicht voraussetzt, dass der betroffenen Person durch die Einbeziehung der betreffenden Information in die Ergebnisliste ein Schaden entsteht. Da die betroffene Person in Anbetracht ihrer Grundrechte aus den Art. 7 und 8 der Charta verlangen kann, dass die betreffende Information der breiten Öffentlichkeit nicht mehr durch Einbeziehung in eine derartige Ergebnisliste zur Verfügung gestellt wird, überwiegen diese Rechte grundsätzlich nicht nur gegenüber dem wirtschaftlichen Interesse des Suchmaschinenbetreibers, sondern auch gegenüber dem Interesse der breiten Öffentlichkeit am**

Zugang zu der Information bei einer anhand des Namens der betroffenen Person durchgeführten Suche. Dies wäre jedoch nicht der Fall, wenn sich aus besonderen Gründen – wie der Rolle der betreffenden Person im öffentlichen Leben – ergeben sollte, dass der Eingriff in die Grundrechte dieser Person durch das überwiegende Interesse der breiten Öffentlichkeit daran, über die Einbeziehung in eine derartige Ergebnisliste Zugang zu der betreffenden Information zu haben, gerechtfertigt ist.

Richtlinie zum grenzüberschreitenden Informationsaustausch bei Verkehrsdelikten (Ls)

(**Europäischer Gerichtshof**, Urteil vom 6. Mai 2014 – C-43/12 –)

1. **Die Richtlinie 2011/82/EU des Europäischen Parlaments und des Rates vom 25. Oktober 2011 zur Erleichterung des grenzüberschreitenden Austauschs von Informationen über die Straßenverkehrssicherheit gefährdende Verkehrsdelikte wird für nichtig erklärt, da sie hauptsächlich der Verkehrssicherheit dient und insoweit aufgrund unzutreffender Rechtsgrundlage (Art. 87 Abs. 2 AEUV) erlassen wurde.**
2. **Die Wirkungen der Richtlinie 2011/82 werden aufrechterhalten, bis innerhalb einer angemessenen Frist, die zwölf Monate ab dem Tag der Verkündung des vorliegenden Urteils nicht überschreiten darf, eine neue, auf die geeignete Rechtsgrundlage, nämlich Art. 91 Abs. 1 Buchst. C. AEUV, gestützte Richtlinie in Kraft tritt.**

(Nicht amtliche Leitsätze)

Keine Auskunft über den anonymen Einmelderin ein Ärztebewertungsportal

(**Bundesgerichtshof**, Urteil vom 1. Juli 2014 – VI ZR 345/13–)

a) **Dem durch persönlichkeitsrechtsverletzende Inhalte einer Internetseite (hier: zur Bewertung von Ärzten) Betroffenen kann ein Unterlassungsanspruch gegen den Diensteanbieter zustehen (vgl. Senatsurteil vom 25. Oktober 2011 – VI ZR 93/10, BGHZ 191, 219). Darüber hinaus darf der Diensteanbieter nach § 14 Abs. 2, § 15 Abs. 5 Satz 4 Telemediengesetz (TMG) auf Anordnung der zuständigen Stellen im Einzelfall Auskunft über Bestands-, Nutzungs- und Abrechnungsdaten erteilen, soweit dies u.a. für Zwecke der Strafverfolgung erforderlich ist.**

b) **Der Betreiber eines Internetportals ist in Ermangelung einer gesetzlichen Ermächtigungsgrundlage im Sinne des § 12 Abs. 2 TMG dagegen grundsätzlich nicht befugt, ohne Einwilligung des Nutzers dessen personenbezogene Daten zur Erfüllung eines Auskunftsanspruchs wegen einer Persönlichkeitsrechtsverletzung an den Betroffenen zu übermitteln.**

Sachverhalt:

Der Kläger macht – soweit im Revisionsverfahren noch von Interesse – einen Auskunftsanspruch gegen die Beklagte geltend.

Die Beklagte betreibt ein Internetportal, das die Bewertung von Ärzten ermöglicht. Der Kläger, der eine Arztpraxis betreibt, entdeckte dort im November 2011 eine Bewertung, in der unter anderem behauptet wurde, bei ihm würden Patientenakten in den Behandlungsräumen in Wäschekörben gelagert, es gebe unverhältnismäßig lange Wartezeiten, Folgetermine seien nicht zeitnah möglich, eine Schilddrüsenüberfunktion sei von ihm nicht erkannt und kontraindiziert behandelt worden. Im Juni 2012 wurden in das Portal weitere, teilweise wortgleiche Beiträge eingestellt. Die Bewertungen wurden jeweils nach entsprechenden Mitteilungen des Klägers von der Beklagten gelöscht. Am 4. Juli 2012 erschien wiederum eine Bewertung mit den bereits zuvor beanstandeten Vorwürfen, die jedenfalls bis November 2012 nicht von der Beklagten gelöscht wurde. Die Beklagte hat nicht bestritten, dass die entsprechenden Behauptungen unrichtig sind.

Das Landgericht hat die Beklagte zur Unterlassung der Verbreitung der vom Kläger beanstandeten Behauptungen, zur Auskunft über Namen und Anschrift des Verfassers der Bewertung vom 4. Juli 2012 und zur Zahlung vorgerichtlicher Anwaltskosten verurteilt. Die dagegen eingelegte Berufung der Beklagten hatte keinen Erfolg. Das Berufungsgericht hat die Revision beschränkt auf den Auskunftsanspruch zugelassen. Mit ihrer Revision verfolgt die Beklagte ihren Antrag auf Abweisung der Klage insoweit weiter.

Das Berufungsgericht hat einen Auskunftsanspruch des Klägers hinsichtlich der bei der Beklagten hinterlegten Anmeldedaten des Verletzers gemäß §§ 242, 259, 260 BGB bejaht. Dieser Anspruch sei auch gegen Dritte als Nicht-Verletzer gegeben. Stelle sich ein Kommentar in einem Blog als rechtswidriger Eingriff in das allgemeine Persönlichkeitsrecht des Betroffenen dar, bestehe gegen den Blogbetreiber bei der Verletzung von Prüfpflichten ein Auskunftsanspruch als Minus zu den Ansprüchen auf Unterlassung und Löschung. § 13 Abs. 6 Satz 1 TMG, wonach ein Diensteanbieter die Nutzung von Telemedien anonym oder unter Pseudonym zu ermöglichen habe, soweit dies technisch möglich und zumutbar sei, schließe den allgemeinen Auskunftsanspruch nicht aus.

Aus den Gründen:

Das Berufungsurteil hält den Angriffen der Revision stand.

1. Allerdings geht das Berufungsgericht zutreffend davon aus, dass nach dem Grundsatz von Treu und Glauben (§ 242 BGB) eine Auskunftspflicht bei jedem Rechtsverhältnis besteht, dessen Wesen es mit sich bringt, dass der Berechtigte in entschuldbarer Weise über Bestehen oder Umfang seines Rechts im Ungewissen und der Verpflichtete in der Lage ist, unschwer die zur Beseitigung dieser Ungewissheit erforderlichen Auskünfte zu erteilen (st. Rspr. seit BGH, Urteil vom 28. Oktober 1953 – II ZR 149/52, BGHZ 10, 385, 386 f.; in jüngerer Zeit etwa BGH, Beschluss vom 20. Februar 2013 – XII ZB 412/11, BGHZ 196, 207 Rn. 30; vgl. auch Senatsurteil vom 28. November 1989 – VI ZR 63/89, VersR 1990, 202 mwN). Für die erforderliche besondere rechtliche Beziehung zwischen Berechtigtem und Verpflichtetem genügt auch ein gesetzliches Schuldverhältnis (BGH, Urteile vom 31. März 1971 – VIII ZR 198/69, WM 1971, 565, 566; vom 5. Juni 1985 – I ZR 53/83, BGHZ 95, 274, 279 – GEMA-Vermutung I; vom 13. Juni 1985 – I ZR 35/83, BGHZ 95, 285, 288 – GEMA-Vermutung II; vom 24. März 1994 – I ZR 42/93, BGHZ 125, 322, 331 – Cartier-Armreif; vom 17. Mai 1994 – X ZR 82/92, BGHZ 126, 109, 113; vom 13. November 2001 – X ZR 134/00, BGHZ 149, 165, 175). Ein derartiges gesetzliches Schuldverhältnis besteht vorliegend aufgrund des aus §§ 823, 1004 BGB folgenden und vom Berufungsgericht rechtskräftig zuerkannten Unterlassungsanspruchs des Klägers gegen die Beklagte (vgl. OLG Dresden, aaO; Kohl, Die Haftung der Betreiber von Kommunikationsforen im Internet und virtuelles Hausrecht, S. 157).

2. In der Rechtsprechung des Bundesgerichtshofs ist zudem anerkannt, dass der Berechtigte unter den vorstehend genannten Voraussetzungen auch die Nennung der Namen Dritter zur Ermittlung der Quelle der Rechtsbeeinträchtigung verlangen kann, um künftige Beeinträchtigungen zu vermeiden; Schuldner des Hauptanspruchs muss daher nicht der Inanspruchgenommene, sondern kann auch ein Dritter sein (BGH, Urteile vom 24. März 1994 – I ZR 42/93, aaO, 330 f.; vom 17. Mai 2001 – I ZR 291/98, BGHZ 148, 26, 30 mwN – Entfernung der Herstellungsnummer II; Teilurteil vom 1. Oktober 2009 – I ZR 94/07, NJW 2010, 2213 Rn. 35 – Oracle).

3. Offen bleiben kann, ob § 13 Abs. 6 Satz 1 TMG, wonach ein Diensteanbieter die Nutzung von Telemedien anonym oder unter Pseudonym zu ermöglichen hat, soweit dies technisch möglich und zumutbar ist, einer Auskunftserteilung über Nutzerdaten entgegensteht (vgl. hierzu einerseits OLG Hamm, CR 2012, 128; andererseits Harting, Internetrecht 5. Aufl., Rn. 2189; Rössel, ITRB 2011, 253, 254; Lauber-Rönsberg, MMR 2014, 10, 13; Siebert, Geheimnisschutz und Auskunftsansprüche im Recht des Geistigen Eigentums, S. 217; zweifelnd OLG Dresden, aaO).

4. Die vom Kläger begehrte Auskunftserteilung scheitert jedenfalls daran, dass die Beklagte gemäß § 12 Abs. 2 TMG nicht zur Herausgabe der zur Bereitstellung des Telemediums erhobenen Anmeldedaten befugt ist. Der Beklagten ist aufgrund dieser Bestimmung die Herbeiführung des geschuldeten Erfolges rechtlich unmöglich (§ 275 Abs. 1 BGB, vgl. BGH, Urteile vom 25. Oktober 2012 – VII ZR 146/11, BGHZ 195 Rn. 33; vom 21. Januar 2010 – Xa ZR 175/07, WM 2010, 410 Rn. 23; zur fehlenden Befugnis zur Auskunftserteilung vgl. auch BGH, Urteil vom 4. April 1979 – VIII ZR 118/78, NJW 1979, 2351, 2353). Es fehlt an der erforderlichen datenschutzrechtlichen Ermächtigungsgrundlage, die die Beklagte zur Erfüllung eines Auskunftsanspruchs des Klägers berechtigten würde (zur Unterscheidung zwischen Auskunftsanspruch und datenschutzrechtlicher Öffnungsklausel vgl. BT-Drucks. 16/3135, S. 2; Schmitz in Hoeren/Sieber/Holznagel, Handbuch Multimedia-Recht, Teil 16.2. Rn. 3, 30, 37, 167, 174 ff. (Stand: Dezember 2009); Hullen/Roggenkamp in Plath, BDSG, § 14 TMG Rn. 17; Zscherpe in Taeger/Gabel, BDSG, 2. Aufl., § 14 TMG Rn. 42).

a) Nach dem Gebot der engen Zweckbindung des § 12 Abs. 2 TMG (hierzu Schmitz, aaO Rn. 34, 109, 130 (Stand: Dezember 2009); Spindler/Nink in Spindler/Schuster, Recht der elektronischen Medien, 2. Aufl., § 12 TMG Rn. 7; FA IT-Recht/Kamps, 2. Aufl., Kap. 20 Rn. 170; vgl. auch BT-Drucks. 13/7385, S. 22, zur Vorgängerregelung des § 3 Abs. 2 TDDSG) dürfen für die Bereitstellung von Telemedien erhobene personenbezogene Daten für andere Zwecke nur verwendet werden, soweit eine Rechtsvorschrift dies erlaubt oder der Nutzer – was hier nicht in Rede steht – eingewilligt hat. Ein Verwenden im Sinne des § 12 Abs. 2 TMG stellt auch die Übermittlung der Daten an Dritte dar (vgl. § 3 Abs. 5, Abs. 4 Satz 2 Nr. 3 BDSG; Heckmann in jurisPK-Internetrecht, 4. Aufl., Kap. 9 Rn. 163 f.; Spindler/Dorschel, CR 2005, 38, 44). Eine Erlaubnis durch Rechtsvorschrift kommt außerhalb des Telemediengesetzes nach dem Gesetzeswortlaut lediglich dann in Betracht, wenn sich eine solche Vorschrift ausdrücklich auf Telemedien bezieht (sog. Zitiergebot; vgl. BT-Drucks. 16/3078, S. 16; Schmitz, aaO Rn. 30, 168, 189, (Stand: Dezember 2009); Bizer/Hornung in BeckRTD-Komm, § 12 TMG Rn. 63, 96; Spindler/Nink, aaO; Heckmann, aaO Rn. 183; Müller-Broich, TMG, § 12 Rn. 4; Hullen/Roggenkamp, aaO, § 12 TMG Rn. 30).

aa) Der aus Treu und Glauben (§ 242 BGB) hergeleitete allgemeine Auskunftsanspruch beinhaltet keine Erlaubnis im Sinne des § 12 Abs. 2 TMG, die sich ausdrücklich auf Telemedien bezieht (vgl. LG München I, CR 2013, 677, 678; AG München, MMR 2011, 417; Spindler/Nink, aaO; Rössel, ITRB 2011, aaO; Müller-Piepenkötter, ITRB 2011, 162, 164; Lauber-Rönsberg, aaO; Schöttler, jurisPR-ITR 7/2007 Anm. 4; zur Vorschrift des § 3 Abs. 2 TDDSG bereits KG, CR 2007, 261, 262; LG Berlin, Urteil vom 27. Oktober 2009 – 27 O 536/09, juris Rn. 49).

bb) Eine Ermächtigung zur Erteilung der begehrten Auskunft ergibt sich auch nicht aus § 14 Abs. 2 TMG. Nach dieser Bestimmung, die nach § 15 Abs. 5 Satz 4 TMG auf Nutzungs- und Abrechnungsdaten entsprechend anwendbar ist, darf zwar der Diensteanbieter auf Anordnung der zuständigen Stellen im Einzelfall Auskunft über Bestandsdaten erteilen, soweit dies für Zwecke der Strafverfolgung, zur Gefahrenabwehr durch die Polizeibehörden der Länder, zur Erfüllung der gesetzlichen Aufgaben der Verfassungsschutzbehörden des Bundes und der Länder, des Bundesnachrichtendienstes oder des Militärischen Abschirmdienstes oder des Bundeskriminalamtes im Rahmen seiner Aufgabe zur Abwehr von Gefahren des internationalen Terrorismus oder zur Durchsetzung der Rechte am geistigen Eigentum erforderlich ist. Eine Ermächtigung zur Auskunftserteilung zu Zwecken des Schutzes von Persönlichkeitsrechten ist darin jedoch nicht enthalten (vgl. LG München I, aaO; BeckRTD-Komm/Dix, § 14 TMG Rn. 53; Roggenkamp/Stadler in jurisPK-Internetrecht, 4. Aufl., Kap. 10 Rn. 538; Spindler, CR 2007, 239, 243; Lauber-Rönsberg, aaO; Kohl, aaO, S. 174).

b) Eine analoge Anwendung von § 14 Abs. 2 TMG, § 15 Abs. 5 Satz 4 TMG scheidet ebenfalls aus, da es an einer planwidrigen Regelungslücke fehlt.

aa) Eine Analogie setzt voraus, dass das Gesetz eine Regelungslücke enthält und der zu beurteilende Sachverhalt in rechtlicher Hinsicht so weit mit dem Tatbestand vergleichbar ist, den der Gesetzgeber geregelt hat, dass angenommen werden kann, der Gesetzgeber wäre bei einer Interessenabwägung, bei der er sich von den gleichen Grundsätzen hätte leiten lassen wie bei dem Erlass der herangezogenen Gesetzesvorschrift, zu dem gleichen Abwägungsergebnis gekommen. Die Unvollständigkeit des Gesetzes muss „planwidrig" sein (vgl. Senatsurteil vom 11. Juni 2013 – VI ZR 150/12, VersR 2013, 1013 Rn. 14; BGH, Urteil vom 14. Dezember 2006 – IX ZR 92/05, BGHZ 170, 187 Rn. 15 mwN).

bb) Wie sich aus der Gesetzesbegründung ergibt, sollte mit der Erweiterung der Auskunftsermächtigung auf Auskünfte zur Durchsetzung der Rechte am geistigen Eigentum in § 14 Abs. 2 bzw. § 15 Abs. 5 Satz 4 TMG die mitgliedstaatliche Verpflichtung zur Sicherstellung bestimmter Auskunftsrechte nach der Richtlinie 2004/48/EG des Europäischen Parlaments und des Rates vom 29. April 2004 zur Durchsetzung der Rechte des geistigen Eigentums (ABl. EU L 157 S. 45) umgesetzt werden (vgl. Begründung der Bundesregierung zu dem Entwurf eines Gesetzes zur Vereinheitlichung von Vorschriften über bestimmte elektronische Informations- und Kommunikationsdienste, BT-Drucks. 16/3078, S. 12 und 16). Die Richtlinie bezieht sich nach Art. 1 und Art. 2 Abs. 1 jedoch nicht auf Persönlichkeitsrechte, sondern dient ausschließlich dem Schutz des geistigen Eigentums, um Innovation und kreatives Schaffen zu fördern, den Arbeitsmarkt zu entwickeln und die Wettbewerbsfähigkeit zu verbessern (vgl. Erwägungsgrund 1 der Richtlinie).

Die Frage, ob dem Betroffenen bei Persönlichkeitsrechtsverletzungen – neben der Möglichkeit, Unterlassungsansprüche gegen den Diensteanbieter geltend zu machen (vgl. insbes. Senatsurteil vom 25. Oktober 2011 – VI ZR 93/10, BGHZ 191, 219 Rn. 18 ff.), – ein Auskunftsanspruch gegen den Diensteanbieter zustehen solle, wurde in den Gesetzesberatungen diskutiert, ohne dass dies zu einer Ausweitung des § 14 Abs. 2 TMG geführt hätte (vgl. das Wortprotokoll der öffentlichen Anhörung des Ausschusses für Wirtschaft und Technologie am 11. Dezember 2006, Protokoll Nr. 16/25, S. 22 ff.). Der Sachverständige von Braunmühl sprach sich

vor dem Ausschuss dafür aus, dass man bei schwerwiegenden Persönlichkeitseingriffen die Daten „der dahinter stehenden Person" erfahren müsse (aaO S. 24). Demgegenüber äußerte der Sachverständige Dr. Bizer, dass es z.B. bei Beleidigungen oder Verleumdungen den Auskunftsanspruch zu Zwecken der Strafverfolgung gebe, der völlig ausreichend sei (aaO, S. 25). Davon, dass der Gesetzgeber die Begrenzung der Auskunftsansprüche auf die Durchsetzung von Rechten am geistigen Eigentum übersehen haben könnte (so Hullen/Roggenkamp, aaO, § 14 TMG Rn. 22), kann unter diesen Umständen nicht ausgegangen werden.

c) Die Beschränkung der Ermächtigung zur Auskunftserteilung auf Inhaber von Rechten am geistigen Eigentum mag zwar wenig nachvollziehbar (Spindler, aaO; Lauber-Rönsberg, aaO, 13 f.) und eine Ausweitung auf Persönlichkeitsrechtsverletzungen – in Anlehnung an § 14 Abs. 2 TMG in Verbindung mit § 101 UrhG, § 19 MarkenG und § 140b PatG – wünschenswert sein (vgl. Kohl, aaO, S. 194 ff.; Lauber-Rönsberg, aaO; Spindler, Persönlichkeitsschutz im Internet – Anforderungen und Grenzen einer Regulierung, in: Verhandlungen des 69. Deutschen Juristentages 2012, Band I, Gutachten F 111 f.; Beschluss Nr. 18 der Abteilung IT- und Kommunikationsrecht des 69. Deutschen Juristentages zum vorgenannten Thema, in: Verhandlungen des 69. Deutschen Juristentages 2012, Band II, O 227). Eine solche Regelung müsste jedoch der Gesetzgeber treffen.

Zur Vererblichkeit von Geldansprüchen wegen Persönlichkeitsrechtsverletzungen

(**Bundesgerichtshof**, Urteil vom 29. April 2014 – VI ZR 246/12 –)

Der Anspruch auf Geldentschädigung wegen Persönlichkeitsrechtsverletzung ist grundsätzlich nicht vererblich.

Sachverhalt:

Die Beklagte ist Gesamtrechtsnachfolgerin der H. B. Zeitschriften Verlag KG (im Folgenden ebenfalls: Beklagte), die im Zeitraum von März 2009 bis August 2010 mehrfach in von ihr herausgegebenen Zeitschriften über den bekannten Entertainer P. A. (im Folgenden: Erblasser) berichtete. Gegenstand der Berichte waren unter anderem die Trauer des Erblassers um seine verstorbene Tochter sowie der Gesundheitszustand des Erblassers. Im Hinblick auf die von ihm in diesem Zusammenhang angenommene Verletzung seines Persönlichkeitsrechts nahm der Erblasser die Beklagte auf Zahlung einer Geldentschädigung in Höhe eines Mindestbetrags von 30.000 € nebst Zinsen in Anspruch. Seine Klage ist beim Landgericht am 11. Februar 2011 eingegangen. Am 12. Februar 2011 verstarb der Erblasser. Im März 2011 ist die Klage zugestellt worden. Der Kläger führt den Prozess als Erbe fort. In den Vorinstanzen ist die Klage erfolglos geblieben. Mit der vom erkennenden Senat zugelassenen Revision verfolgt der Kläger sein Begehren weiter.

Aus den Gründen:

1. Mit Recht ist das Berufungsgericht davon ausgegangen, dass der – unterstellte – Geldentschädigungsanspruch des Erblassers mangels Vererblichkeit nicht auf den Kläger übergehen konnte.

a) Die Frage, ob der Anspruch auf Geldentschädigung wegen Verletzung des Persönlichkeitsrechts vererblich ist, ist höchstrichterlich bislang nicht abschließend geklärt (vgl. Senatsurteil vom 6. Dezember 2005 – VI ZR 265/04, BGHZ 165, 203, 208; BGH, Urteil vom 24. März 2011 – IX ZR 180/10, BGHZ 189, 65 Rn. 39 f.). Im Schrifttum ist die Frage umstritten.

Eine Reihe von Autoren bejaht die Vererblichkeit (z.B. Soergel/Beater, BGB, 13. Aufl., Anh. IV § 823 Rn. 25; Brändel in: Götting/Schertz/Seitz, Handbuch des Persönlichkeitsrechts, § 36 Rn. 24; Cronemeyer, AfP 2012, 10 ff.; Dreier/Specht in Dreier/Schulze, UrhG, 4. Aufl., KUG § 22 Rn. 37 und §§ 33-50 Rn. 21, anders allerdings noch Dreier in der 3. Aufl., KUG § 33-50 Rn. 21; Fechner, Medienrecht, 14. Aufl., Kap. 4 Rn. 157; Kutschera, AfP 2000, 147, 148 f.; Leipold, Erbrecht, 19. Aufl., Rn. 635 Fn. 51; MünchKommBGB/Rixecker, 6. Aufl., Anhang zu § 12 Rn. 237 aE). Begründet wird diese Auffassung zunächst mit der uneingeschränkten Vererblichkeit des Schmerzensgeldanspruchs seit Aufhebung von § 847 Abs. 1 Satz 2 BGB aF zum 1. Juli 1990, aus der entsprechende Konsequenzen auch für den Anspruch auf Geldentschädigung wegen Verletzung des Persönlichkeitsrechts zu ziehen seien (Soergel/Beater, aaO; Cronemeyer, aaO, 11 f.; Kutschera, aaO). Darüber hinaus wird angenommen, die unterschiedliche Behandlung des Schmerzensgeldanspruchs einerseits und des Geldentschädigungsanspruchs wegen Verletzung des Persönlichkeitsrechts andererseits verstoße gegen Art. 3 Abs. 1 GG (Cronemeyer, aaO, 11; Kutschera, aaO, 148). Andere gehen davon aus, eine unberechtigte Besserstellung des Verletzers durch den Tod des Verletzten vor Leistung des Geldersatzes müsse vermieden werden (Dreier/Specht, aaO, KUG § 22 Rn. 37). Überdies löse sich der auf eine Geldzahlung gerichtete Anspruch mit seiner Entstehung von den ideellen Bestandteilen des Persönlichkeitsrechts (Dreier/Specht, aaO).

Die Gegenauffassung (z.B. Burkhardt in: Wenzel, Das Recht der Wort- und Bildberichterstattung, 5. Aufl., Kap. 14 Rn. 140; Damm/Rehbock, Widerruf, Unterlassung und Schadensersatz in den Medien, 3. Aufl., Rn. 1011 ff.; Erman/N. Klass, BGB, 13. Aufl., Anh. § 12 Rn. 320; Müller in: Götting/Schertz/Seitz, Handbuch des Persönlichkeitsrechts, § 51 Rn. 28; Soehring in: Soehring/Hoene, Presserecht, 5. Aufl., § 32 Rn. 23; Löffler/Steffen, Presserecht, 5. Aufl., LPG § 6 Rn. 344) stützt sich auf den Zweck der Geldentschädigung, der darin liege, die – nicht vererblichen (vgl. BGH, Urteile vom 1. Dezember 1999 – I ZR 49/97, BGHZ 143, 214, 220 – Marlene Dietrich; vom 20. März 1968 – I ZR 44/66, BGHZ 50, 133, 137 – Mephisto) – ideellen Bestandteile des allgemeinen Persönlichkeitsrechts zu schützen (so ausdrücklich Burkhard, aaO; Steffen, aaO). Weiter wird darauf verwiesen, die überwiegende Genugtuungsfunktion des Geldentschädigungsanspruchs aus Persönlichkeitsrechtsverletzungen und ihr höchstpersönlicher Bezug zur Individualität des Betroffenen lasse eine Vererblichkeit nicht zu (vgl. Damm/Rehbock, aaO, Rn. 1012; Erman/N. Klass, aaO).

b) Die zuletzt genannte Auffassung trifft im Ergebnis zu. Der Anspruch auf Geldentschädigung wegen Verletzung des Persönlichkeitsrechts ist grundätzlich nicht vererblich.

aa) Unmittelbar aus der nach wie vor zutreffenden Erkenntnis, dass die ideellen Bestandteile des Persönlichkeitsrechts unauflöslich an die Person ihres Trägers gebunden und als höchstpersönliche Rechte unverzichtbar und unveräußerlich, also nicht übertragbar und nicht vererblich sind (vgl. BGH, Urteile vom 24. März 2011 – IX ZR 180/10, BGHZ 189, 65 Rn. 38; vom 1. Dezember 1999 – I ZR 49/97, BGHZ 143, 214, 220 – Marlene Dietrich; vom 20. März 1968 – I ZR 44/66, BGHZ 50, 133, 137 – Mephisto), ergibt sich dies freilich – worauf die Revision zutreffend hinweist – noch nicht. Denn der Geldentschädigungsanspruch hat zwar seine Grundlage im Schutzauftrag aus Art. 1 und Art. 2 Abs. 1 GG (vgl. Senatsurteile vom 6. Dezember 2005 – VI ZR 265/04, BGHZ 165, 203, 204 f.; vom 5. Oktober 2004 – VI ZR 255/03, BGHZ 160, 298, 302; vom 15. November 1994 – VI ZR 56/94, BGHZ 128, 1, 15; jeweils mwN; BVerfGE 34, 269, 292 – Soraya) und dient gerade den vom allgemeinen Persönlichkeitsrecht umfassten ideellen Interes-

sen. Als Geldzahlungsanspruch ist er aber nicht selbst Bestandteil des allgemeinen Persönlichkeitsrechts (vgl. BGH, Urteil vom 24. März 2011 – IX ZR 180/11, BGHZ 189, 65 Rn. 39 f.).

bb) Die Unvererblichkeit ergibt sich aber aus Natur und Zweck des Geldentschädigungsanspruchs selbst.

(1) Der erkennende Senat hat bereits entschieden, dass der Anspruch auf Entschädigung in Geld für die Verletzung des Persönlichkeitsrechts nicht abtretbar ist. Er hat dies „aus der entsprechenden Anwendung der Vorschriften, die für die gesetzlich normierten Fälle ideellen Schadensersatzes gegeben sind", gefolgert. Konkret hat er dabei auf die damals geltenden Regelungen des § 847 Abs. 1 Satz 2 BGB aF und des § 1300 Abs. 2 BGB aF abgestellt (Senatsurteil vom 25. Februar 1969 – VI ZR 241/67, VersR 1969, 519, 521). Die genannten Vorschriften regelten dabei nicht nur die fehlende Abtretbarkeit der Ansprüche aus § 847 Abs. 1 Satz 1 BGB aF bzw. § 1300 Abs. 1 BGB aF, sondern auch ihre grundsätzliche Unvererblichkeit. Grund für den Ausschluss von Abtretbarkeit und Vererblichkeit dieser Ansprüche war, dass sie der Gesetzgeber aufgrund ihres an die Person des Berechtigten gebundenen Charakters für höchstpersönlich erachtete (vgl. für § 847 Abs. 1 Satz 1 BGB aF: Senatsurteile vom 22. Juni 1976 – VI ZR 167/75, NJW 1976, 1890; vom 14. März 1961 – VI ZR 146/60, NJW 1961, 1575; für § 1300 Abs. 2 BGB aF: Palandt/Lauterbach, BGB, 28. Aufl. 1969, § 1300 unter 1). Durch die entsprechende Anwendung der Vorschriften des § 847 Abs. 1 Satz 2 BGB aF und des § 1300 Abs. 2 BGB aF auf den auch zum damaligen Zeitpunkt bereits aus Art. 1 und Art. 2 Abs. 1 GG hergeleiteten (vgl. Senatsurteil vom 19. September 1961 – VI ZR 259/60, BGHZ 35, 363, 366 ff.) Geldentschädigungsanspruch hat der Senat zum Ausdruck gebracht, dass er diesem Anspruch denselben Charakter zumisst.

(2) An dieser Einschätzung und der sich daraus ergebenden Unvererblichkeit des Geldentschädigungsanspruchs hält der Senat – wie bereits im Urteil vom 6. Dezember 2005 (VI ZR 265/04, BGHZ 165, 203, 208) zum Ausdruck gebracht – trotz der inzwischen erfolgten Aufhebung von § 847 Abs. 1 Satz 2 BGB aF und von § 1300 Abs. 2 BGB aF fest. Weder lässt sich der Wille des Gesetzgebers feststellen, auch den Geldentschädigungsanspruch wegen Verletzung des Persönlichkeitsrechts vererblich auszugestalten (a), noch führen Sinn und Zweck des Geldentschädigungsanspruchs unabhängig von einer entsprechenden Entscheidung des Gesetzgebers zur Annahme, der Geldentschädigungsanspruch sei heute vererblich (b).

(a) Unmittelbar hat sich der Gesetzgeber mit der Frage der Vererblichkeit des Geldentschädigungsanspruchs bislang nicht befasst. Eine mittelbare Aussage des Gesetzgebers, der Geldentschädigungsanspruch sei vererblich, lässt sich ebenfalls nicht feststellen.

(aa) Entgegen der Auffassung der Revision ergibt sich ein solcher gesetzgeberischer Wille zunächst nicht aus der Streichung von § 847 Abs. 1 Satz 2 BGB aF und entsprechender Vorschriften in anderen Gesetzen durch das Gesetz zur Änderung des Bürgerlichen Gesetzbuchs und anderer Gesetze vom 14. März 1990 (BGBl. I, S. 478). Anhaltspunkte dafür, dass der Gesetzgeber hier seine bis dahin und auch später (vgl. nur Entwurf eines Zweiten Gesetzes zur Änderung schadensersatzrechtlicher Vorschriften, BR-Drucks. 742/01, S. 58; ferner Gegenäußerung der Bundesregierung zur Stellungnahme des Bundesrates, BT-Drucks. 14/7752, S. 55) geübte Zurückhaltung, den vom erkennenden Senat unmittelbar aus dem Schutzauftrag des Art. 1 und Art. 2 Abs. 1 GG hergeleiteten Geldentschädigungsanspruch in irgendeiner Weise zu regeln, hätte aufgeben und eine Aussage zur Vererblichkeit dieses Anspruchs hätte treffen wollen, sind nicht ersichtlich.

Im Gegenteil sollte mit der Streichung von § 847 Abs. 1 Satz 2 BGB aF und entsprechender Vorschriften im Luftverkehrsgesetz, im Bundesgrenzschutzgesetz sowie im Atomgesetz ein spezifisches Problem im Bereich des Schmerzensgeldes einer Lösung zugeführt werden. Dieses Problem lag ausweislich der Gesetzesmaterialien im „Wettlauf mit der Zeit", dem sich „insbesondere die nächsten Angehörigen" ausgesetzt sahen, wenn sie „gerade bei schwersten Verletzungen mit der Folge der Bewusstlosigkeit des Verletzten und akuter Lebensgefahr" Schmerzensgeldansprüche auch für den Fall des Todes des Verletzten wahren wollten (vgl. Entwurf eines Gesetzes zur Änderung des Bürgerlichen Gesetzbuchs und anderer Gesetze, BT-Drucks. 11/4415, S. 1, 4; Beschlussempfehlung und Bericht des Rechtsausschusses zum genannten Gesetzentwurf, BT-Drucks. 11/5423, S. 1, 4). Auch wenn sich die Reichweite der Gesetzesänderung nicht auf die Fälle schwerster Verletzungen mit der Folge der Bewusstlosigkeit des Verletzten und akuter Lebensgefahr beschränkte, sondern auch leichtere Verletzungen, im Falle des § 34 Bundesgrenzschutzgesetz sogar Ehrverletzungen einschloss, waren mithin doch gerade die Fälle schwerster Körperverletzungen Grund für die Streichung der Unvererblichkeit der genannten Ansprüche. Damit bezweckte die Gesetzesänderung die Beseitigung einer Problemlage, die typischerweise bei Ansprüchen infolge von Körperverletzungen, nicht aber bei Ansprüchen aufgrund der Verletzung des Persönlichkeitsrechts besteht (vgl. auch Damm/Rehbock, Widerruf, Unterlassung und Schadensersatz in den Medien, 3. Aufl., Rn. 1012). Dass der Gesetzgeber mit der Streichung unter anderem des § 847 Abs. 1 Satz 2 BGB aF nicht alle Ansprüche auf Ausgleich immaterieller Nachteile für vererblich erklären wollte, zeigt im Übrigen auch die Regelung des § 1300 Abs. 2 BGB aF. Sie wurde bis zur Abschaffung des Kranzgeldes zum 1. Juli 1998 beibehalten.

(bb) Die Aufhebung des § 1300 Abs. 2 BGB aF im Jahr 1998 lässt offensichtlich keinen Rückschluss auf einen Willen des Gesetzgebers zu, den Geldentschädigungsanspruch wegen Verletzung des Persönlichkeitsrechts vererblich auszugestalten. Die Streichung war notwendige Folge der Abschaffung des Kranzgeldes überhaupt durch das Gesetz zur Neuordnung des Eheschließungsrechts vom 4. Mai 1998 (BGBl. I, S. 833). Grund für die Abschaffung war die Annahme, das Kranzgeld als solches, nicht seine Unvererblichkeit, sei rechtspolitisch überholt (vgl. Entwurf eines Gesetzes zur Neuordnung des Eheschließungsrechts, BR-Drucks. 79/96, S. 37).

(b) Entscheidend gegen die Vererblichkeit des Geldentschädigungsanspruchs spricht seine Funktion.

Bei der Zuerkennung einer Geldentschädigung im Falle einer schweren Persönlichkeitsrechtsverletzung steht regelmäßig der Genugtuungsgedanke im Vordergrund (vgl. etwa Senatsbeschluss vom 10. Januar 2006 – VI ZB 26/05, VersR 2006, 673 Rn. 16; Senatsurteile vom 6. Dezember 2005 – VI ZR 265/04, BGHZ 165, 203, 206; vom 5. Oktober 2004 – VI ZR 255/03, BGHZ 160, 298, 302; vom 15. November 1994 – VI ZR 56/94, BGHZ 128, 1, 15; vom 5. Dezember 1995 – VI ZR 332/94, VersR 1996, 339, 340; vom 4. Juni 1974 – VI ZR 68/73, VersR 1974, 1080, 1082 – Fiete Schulze). Da einem Verstorbenen Genugtuung für die Verletzung seiner Persönlichkeit nicht mehr verschafft werden kann, scheidet nach der Rechtsprechung des erkennenden Senats die Zuerkennung einer Geldentschädigung im Falle der Verletzung des postmortalen Persönlichkeitsschutzes aus (Senatsurteile vom 6. Dezember 2005 – VI ZR 265/04, BGHZ 165, 203, 206 f. mwN; vom 4. Juni 1974 – VI ZR 68/73, VersR 1974, 1080, 1082 – Fiete Schulze). Erfolgt die Verletzung des Persönlichkeitsrechts zwar noch zu Lebzeiten des Verletzten, stirbt dieser aber, bevor sein Entschädigungsanspruch

erfüllt worden ist, verliert die mit der Geldentschädigung bezweckte Genugtuung regelmäßig ebenfalls an Bedeutung. Gründe, vom Fortbestehen des Geldentschädigungsanspruchs über den Tod des Verletzten hinaus auszugehen, bestehen unter diesem Gesichtspunkt im Allgemeinen mithin nicht.

Der von der Revision herangezogene Gedanke der Prävention kann vorliegend zu keiner anderen Beurteilung führen. Zwar trifft es zu, dass der Geldentschädigungsanspruch auch der Prävention dient (Senatsurteile vom 17. Dezember 2013 – VI ZR 211/12, VersR 2014, 381 Rn. 38; vom 6. Dezember 2005 – VI ZR 265/04, BGHZ 165, 203, 207 mwN; vom 5. Oktober 2004 – VI ZR 255/03, BGHZ 160, 298, 302; Müller in: Götting/Schertz/Seitz, Handbuch des Persönlichkeitsrechts, § 51 Rn. 7, 10; jeweils mwN). Der Präventionsgedanke vermag die Gewährung einer Geldentschädigung – auch in dem von der Revision vorliegend für gegeben erachteten Fall der Zwangskommerzialisierung – aber nicht alleine zu tragen (Senatsurteile vom 6. Dezember 2005 aaO mwN; vom 5. März 1974 – VI ZR 228/72, VersR 1974, 756, 758). Dies wirkt sich nicht nur – wie im Falle postmortaler Persönlichkeitsrechtsverletzungen – auf die Beurteilung der Frage aus, ob der Geldentschädigungsanspruch auch unabhängig von seiner Genugtuungsfunktion entstehen kann, sondern auch darauf, ob er – wie im vorliegend zu beurteilenden Fall – bei Fortfall dieser Funktion weiterbestehen kann.

cc) Entgegen der Auffassung der Revision verstößt die Annahme der Unvererblichkeit des Anspruchs auf Geldentschädigung wegen Verletzung des Persönlichkeitsrechts nicht gegen § 1922 BGB. Denn die von § 1922 Abs. 1 BGB vorgesehene Universalsukzession ist von vornherein auf die vererblichen Vermögensgegenstände beschränkt (vgl. Staudinger/Marotzke, BGB, Neubearb. 2008, § 1922 Rn. 53).

dd) Auch der Einwand der Revision, es stelle eine sachlich nicht gerechtfertigte Ungleichbehandlung dar und verstoße deshalb gegen Art. 3 Abs. 1 GG, wenn der Anspruch auf Geldentschädigung anders als der Anspruch auf Schmerzensgeld und andere Immaterialgüterrechte nicht vererblich wäre, geht fehl.

Zwar ist Art. 3 Abs. 1 GG dann verletzt, wenn eine Gruppe von Normadressaten im Vergleich zu anderen Normadressaten in wesentlicher Hinsicht anders behandelt wird, obwohl zwischen beiden Gruppen keine Unterschiede von solcher Art und solchem Gewicht bestehen, dass sie die ungleiche Behandlung rechtfertigen können. Auch liegt eine solche Grundrechtsverletzung nicht nur dann vor, wenn der Gesetzgeber mehrere Personengruppen ohne hinreichenden sachlichen Grund verschieden behandelt, sondern auch dann, wenn die Gerichte im Wege der Auslegung gesetzlicher Vorschriften zu einer derartigen, dem Gesetzgeber verwehrten Differenzierung gelangen (BVerfG, VersR 2000, 897 mwN). Vorliegend scheitert die Annahme einer Verletzung von Art. 3 Abs. 1 GG aber daran, dass für die im Hinblick auf die Frage der Vererblichkeit unterschiedliche Behandlung des Geldentschädigungsanspruchs wegen Verletzung des Persönlichkeitsrechts einerseits und des Schmerzensgeldanspruchs sowie anderer Immaterialgüterrechte andererseits sachliche Gründe bestehen. Denn die Unvererblichkeit des Geldentschädigungsanspruchs hat – wie dargelegt – ihren Grund letztlich in der Genugtuungsfunktion, die bei ihm im Vergleich zu sonstigen Ansprüchen auf Ersatz immaterieller Nachteile und gerade auch im Vergleich zum Schmerzensgeldanspruch in besonderem Maße ausgeprägt ist (vgl. Senatsbeschluss vom 10. Januar 2006 – VI ZB 26/05, VersR 2006, 673 Rn. 14 ff.; Senatsurteile vom 5. Oktober 2004 – VI ZR 255/03, BGHZ 160, 298, 302; vom 26. November 1996 – VI ZR 323/95, VersR 1997, 325, 327).

Soweit die Revision auf die Vererblichkeit des Urheberrechts nach § 28 Abs. 1 UrhG verweist, die sich nicht nur auf die vermögensrechtlichen Elemente des Urheberrechts, sondern auch auf das Urheberpersönlichkeitsrecht bezieht (vgl. BGH, Urteil vom 16. Mai 2013 – I ZR 28/12, WRP 2014, 68 Rn. 25 – Beuys-Aktion; Schulze in Dreier/Schulze, UrhG 4. Aufl., § 28 Rn. 2), ist ihr zuzugeben, dass das Urheberpersönlichkeitsrecht insoweit anders behandelt wird als das allgemeine Persönlichkeitsrecht. Diese Ungleichbehandlung hat ihren sachlichen Grund aber darin, dass das Urheberpersönlichkeitsrecht so mit den vermögensrechtlichen Elementen des Urheberrechts verflochten ist, dass sie sich nicht voneinander trennen lassen (vgl. Schulze, aaO), und sich das Urheberpersönlichkeitsrecht gerade hierin vom allgemeinen Persönlichkeitsrecht unterscheidet. In der unterschiedlichen Ausgestaltung des Urheberpersönlichkeitsrechts als vererbliches und des allgemeinen Persönlichkeitsrechts als grundsätzlich unvererbliches Recht liegt zugleich ein (weiterer) sachlicher Grund für die insoweit unterschiedliche Behandlung auch des Anspruchs auf Ersatz immaterieller Schäden bei Verletzung des Urheberpersönlichkeitsrechts (§ 97 Abs. 2 Satz 4 UrhG) einerseits und des Geldentschädigungsanspruchs wegen Verletzung des (allgemeinen) Persönlichkeitsrechts andererseits. Denn die Entschädigungsansprüche sind mit dem Rechtsgut, dessen Verletzung sie entspringen, eng verknüpft.

c) Entgegen der hilfsweise geäußerten Auffassung der Revision wurde der – unterstellte – Geldentschädigungsanspruch vorliegend auch nicht deshalb vererblich, weil er noch zu Lebzeiten des Erblassers anhängig gemacht wurde. Denn die bloße Anhängigkeit einer auf Geldentschädigung gerichteten Klage ändert nichts daran, dass die von der Geldentschädigung bezweckte Genugtuung mit dem Tod des Verletzten an Bedeutung verliert.

Ob – wie dies etwa § 847 Abs. 1 Satz 2 BGB aF und § 1300 Abs. 2 BGB aF für die Ansprüche auf Schmerzens- bzw. Kranzgeld vorgesehen haben – anderes gilt, wenn der Geldentschädigungsanspruch rechtshängig geworden ist, kann offenbleiben. Denn die Klage wurde der Beklagten erst nach dem Tod des Erblassers zugestellt.

Aus § 167 ZPO ergibt sich nichts anderes. Die dort angeordnete Rückwirkung beschränkt sich – verfassungsrechtlich unbedenklich – auf Fälle, in denen durch die Zustellung eine laufende Frist gewahrt oder die Verjährung neu beginnen oder gehemmt werden soll. Für sonstige Wirkungen der Zustellung gilt sie hingegen nicht (allg. M.; vgl. z.B. BGH, Beschluss vom 22. Juli 2010 – V ZB 178/09, NJW 2011, 528 Rn. 8 mwN; Urteil vom 21. April 1982 – IVb ZR 696/80, NJW 1982, 1812, 1813; Zöller/Greger, ZPO, 30. Aufl., § 167 Rn. 4; MünchKommZPO/Häublein, 4. Aufl., § 167 Rn. 6). Zu diesen sonstigen Wirkungen zählen insbesondere rechtsbegründende und rechtsverstärkende Folgen, die die Vorschriften des materiellen Rechts an die Rechtshängigkeit und damit an die Zustellung der Klageschrift knüpfen (BGH, Beschluss vom 22. Juli 2010 – V ZB 178/09, aaO Rn. 9; Zöller/Greger, aaO). Für § 847 Abs. 1 Satz 2 Halbs. 2 BGB aF hat auch der erkennende Senat eine Anwendung solcher Vorschriften wiederholt abgelehnt, die zur Fristwahrung die Wirkung der Zustellung auf den Zeitpunkt der Einreichung zurückbeziehen (vgl. Senatsurteile vom 22. Juni 1976 – VI ZR 167/75, NJW 1976, 1890 f.; vom 10. Oktober 1961 – VI ZR 40/61, NJW 1961, 2347; vom 14. März 1961 – VI ZR 146/60, NJW 1961, 1575 f.; Palandt/Thomas, BGB, 49. Aufl. 1990, § 847 unter 5 c). Durchgreifende Gründe dafür, diese ständige höchstrichterliche Rechtsprechung aufzugeben, werden von der Revision nicht aufgezeigt und sind auch sonst nicht ersichtlich.

Der Zeitgeschichte zuzuordnende Bilder

(**Bundesgerichtshof**, Urteil vom 8. April 2014 – VI ZR 197/13 –)

Der für die Frage, ob es sich um ein Bild aus dem Bereich der Zeitgeschichte handelt (§ 23 Abs. 1 Nr. 1 KUG), maßgebende Begriff des Zeitgeschehens umfasst alle Fragen von allgemeinen gesellschaftlichen Interessen. Dazu können auch Veranstaltungen von nur regionaler oder lokaler Bedeutung gehören (wie hier ein Mieterfest einer Wohnungsgenossenschaft)

(Nicht amtlicher Leitsatz)

Sachverhalt:

Die Klägerinnen, Großmutter, Tochter und Enkelin, nehmen die Beklagte, eine Wohnungsbaugenossenschaft, auf Zahlung einer Geldentschädigung und von Abmahnkosten wegen einer ohne ihre Einwilligung erfolgten Veröffentlichung und Verbreitung eines Fotos in Anspruch, das die Klägerinnen gemeinsam auf einem von der Beklagten im August 2010 veranstalteten Mieterfest zeigt.

Bei dem jährlich stattfindenden Mieterfest der Beklagten wurden Fotos gefertigt, unter anderem das beanstandete Foto, auf dem im Vordergrund die Klägerinnen zu 1 und 2 zu sehen sind, wie sie die Klägerin zu 3, ein Kleinkind, füttern. Dieses Foto veröffentlichte die Beklagte in ihrer Broschüre „Informationen der Genossenschaft", Ausgabe 2010, neben weiteren neun Fotos, auf denen Teilnehmer des Mieterfestes, einzeln und in Gruppen, zu sehen sind. Die Broschüre wurde in einer Auflage von 2.800 Stück hergestellt und an Genossenschaftsmieter verteilt.

Aus den Gründen:

Nach Auffassung des Berufungsgerichts scheidet ein Anspruch auf Zahlung einer Geldentschädigung der Klägerinnen gegen die Beklagte aus § 823 Abs. 1 BGB i.V.m. Art. 2 Abs. 1, Art. 1 Abs. 1 GG bereits deshalb aus, weil jedenfalls keine schwere Verletzung des allgemeinen Persönlichkeitsrechts der Klägerinnen vorliegt. Ein Anspruch der Klägerinnen auf Erstattung der Abmahnkosten scheitere daran, dass es bereits an der dafür erforderlichen Voraussetzung einer rechtswidrigen Verletzung des allgemeinen Persönlichkeitsrechts der Klägerinnen bzw. ihres Rechts am eigenen Bild aus § 823 Abs. 1 BGB, §§ 22, 23 KUG i.V.m. Art. 2 Abs. 1, Art. 1 Abs. 1 GG fehle. Die Verbreitung des Bildnisses der Klägerinnen in der Mieterbroschüre der Beklagten ohne deren Einwilligung sei zwar nicht bereits nach § 23 Abs. 1 Nr. 1 KUG erlaubt, weil die Teilnahme der Klägerinnen an dem Mieterfest kein zeitgeschichtliches Ereignis gewesen sei. Jedoch sei die Veröffentlichung des Bildnisses der Klägerinnen jedenfalls nach § 23 Abs. 1 Nr. 3 KUG auch ohne deren Einwilligung zulässig gewesen. Der Anwendungsbereich dieser Regelung sei nicht von vorneherein auf Fotos von Personengruppen beschränkt, sondern erfasse auch sogenannte repräsentative Aufnahmen, bei denen einzelne Personen als charakteristisch und beispielhaft für die Ansammlung herausgegriffen worden seien. Die auch im Rahmen des § 23 Abs. 1 Nr. 3 KUG erforderliche Abwägung zwischen dem Interesse der Klägerinnen am Schutz ihrer Persönlichkeit und dem von dem Beklagten wahrgenommenen Informationsinteresse der Öffentlichkeit führe zu dem Ergebnis, dass die Veröffentlichung des Bildnisses der Klägerinnen auch ohne deren Einwilligung zulässig gewesen sei.

B) Das Berufungsurteil hält im Ergebnis revisionsrechtlicher Nachprüfung stand.

1. Entgegen der Auffassung des Berufungsgerichts hatten die Klägerinnen gegen die Beklagte allerdings bereits deshalb keinen Anspruch aus § 1004 Abs. 1 Satz 2, § 823 Abs. 1, Abs. 2 BGB i.V.m. §§ 22, 23 KUG, Art. 1 Abs. 1, Art. 2 Abs. 1 GG auf Unterlassung der Veröffentlichung des beanstandeten Bildnisses, weil dieses Bild dem Bereich der Zeitgeschichte zuzuordnen ist (§ 23 Abs. 1 Nr. 1 KUG) und berechtigte Interessen der Abgebildeten nicht verletzt wurden (§ 23 Abs. 2 KUG). Auf die Zulassungsfrage nach der Reichweite des § 23 Abs. 1 Nr. 3 KUG kommt es deshalb nicht an.

2. Das Berufungsgericht ist zutreffend davon ausgegangen, dass die Zulässigkeit von Bildveröffentlichungen nach der gefestigten Rechtsprechung des erkennenden Senats nach dem abgestuften Schutzkonzept der §§ 22, 23 KUG zu beurteilen ist (vgl. grundlegend Senatsurteile vom 6. März 2007 – VI ZR 51/06, BGHZ 171, 275 Rn. 9 ff.; vom 18. Oktober 2011 – VI ZR 5/10, VersR 2012, 116 Rn. 8 f.; vom 22. November 2011 – VI ZR 26/11, VersR 2012, 192 Rn. 23 f.; vom 18. September 2012 – VI ZR 291/10, VersR 2012, 1403 Rn. 25 f. und vom 28. Mai 2013 – VI ZR 125/12, VersR 2013, 1178 Rn. 10, jeweils mwN), das sowohl mit verfassungsrechtlichen Vorgaben (vgl. BVerfGE 120, 180, 201 ff.) als auch mit der Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte im Einklang steht (vgl. EGMR NJW 2004, 2647; 2006, 591 sowie NJW 2012, 1053 und 1058). Danach dürfen Bildnisse einer Person grundsätzlich nur mit deren Einwilligung verbreitet werden (§ 22 Satz 1 KUG). Hiervon besteht allerdings gemäß § 23 Abs. 1 Nr. 1 KUG eine Ausnahme, wenn es sich um Bildnisse aus dem Bereich der Zeitgeschichte handelt. Diese Ausnahme gilt aber nicht für die Verbreitung, durch die berechtigte Interessen des Abgebildeten verletzt werden (§ 23 Abs. 2 KUG).

3. Nach diesen Grundsätzen war die von den Klägerinnen angegriffene Veröffentlichung der beanstandeten Bildberichterstattung auch ohne ihre Einwilligung zulässig.

a) Bei dem beanstandeten Foto der Klägerinnen handelte es sich um ein Bildnis aus dem Bereich der Zeitgeschichte. Schon die Beurteilung, ob Abbildungen Bildnisse aus dem Bereich der Zeitgeschichte im Sinne von § 23 Abs. 1 Nr. 1 KUG sind, erfordert eine Abwägung zwischen den Rechten der Abgebildeten aus Art. 1 Abs. 1, Art. 2 Abs. 1 GG, Art. 8 Abs. 1 EMRK einerseits und den Rechten der Medien aus Art. 5 Abs. 1 GG, Art. 10 Abs. 1 EMRK andererseits (vgl. etwa Senatsurteil vom 28. Mai 2013 – VI ZR 125/12, aaO Rn. 12 mwN). Der für die Frage, ob es sich um ein Bildnis aus dem Bereich der Zeitgeschichte handelt, maßgebende Begriff des Zeitgeschehens umfasst alle Fragen von allgemeinem gesellschaftlichem Interesse. Dazu können auch Veranstaltungen von nur regionaler oder lokaler Bedeutung gehören (vgl. zu Sportveranstaltungen Senatsurteil vom 28. Mai 2013 – VI ZR 125/12, aaO). Ein Informationsinteresse besteht allerdings nicht schrankenlos, vielmehr ist der Grundsatz der Verhältnismäßigkeit zu berücksichtigen, und es bedarf gerade bei unterhaltenden Inhalten im besonderen Maß einer abwägenden Berücksichtigung der kollidierenden Rechtspositionen (vgl. Senatsurteile vom 1. Juli 2008 – VI ZR 67/08, VersR 2008, 1411 Rn. 20 und – VI ZR 243/06, VersR 2008, 1506 Rn. 20; vom 13. April 2010 – VI ZR 125/08, VersR 2010, 1090 Rn. 14 und vom 28. Mai 2013 – VI ZR 125/12, aaO Rn. 12 f.). Der Informationsgehalt einer Bildberichterstattung ist im Gesamtkontext, in den das Personenbildnis gestellt ist, zu ermitteln.

b) Die Bildberichterstattung in der Informationsbroschüre der Beklagten befasst sich mit dem – jährlich stattfindenden – Mieterfest der beklagten Wohnungsbaugenossenschaft im August 2010 und zeigt repräsentativ auf insgesamt zehn Bildern Teilnehmer,

sowohl in Gruppen, als auch einzeln. Die Bilder fangen Szenen des Mieterfestes ein, die ein harmonisches Zusammensein von Jung und Alt in fröhlicher und entspannter Atmosphäre zeigen. Die Bildberichterstattung vermittelt den Eindruck, dass Mitbewohner aller Altersgruppen das Fest genossen haben und zwischen ihnen gute nachbarschaftliche Beziehungen bestehen. In diesen Zusammenhang passt gerade das Bild der Klägerinnen, welches drei Generationen vereint. Zwar gibt es – außer dem Hinweis auf das Mieterfest und der Ankündigung der entsprechenden Veranstaltung im Folgejahr – keine begleitende Textberichterstattung, doch bereits durch die Auswahl der gezeigten Fotos wird dem Leser – so zutreffend das Berufungsgericht – ein Eindruck über dessen Verlauf vermittelt. Das Mieterfest ist ein Ereignis von lokaler gesellschaftlicher Bedeutung. Die Informationsbroschüre der Beklagten, in der über das Fest berichtet wurde, war an ihre Mieter gerichtet, also an den (beschränkten) Personenkreis, der üblicherweise an dem Fest teilnahm und entsprechend der Ankündigung eingeladen war, im Folgejahr teilzunehmen. Das Recht, über solche zeitgeschichtlichen Ereignisse aus dem gesellschaftlichen Bereich zu berichten, steht grundsätzlich auch der Beklagten zu, wenn sie eine Informationsbroschüre herausgibt; denn auch eine solche Broschüre gehört zu den Medien. Die Beklagte kann sich – wie das Berufungsgericht mit Recht angenommen hat – unter dem Gesichtspunkt der Meinungsfreiheit gemäß Art. 5 Abs. 1 Satz 1 GG auf ein schützenswertes Interesse berufen, ihre Genossenschaftsmieter im Bild über den Ablauf und die Atmosphäre der Veranstaltung zu informieren. Die Bildberichterstattung der Beklagten über das Mieterfest in ihrer Informationsbroschüre an ihre Mieter erfüllt eine wichtige Funktion, denn ein solches Fest pflegt und schafft gute nachbarschaftliche Beziehungen. Die Berichterstattung vermittelt den Eindruck, dass die Mitbewohner sich in der Wohnungsbaugenossenschaft wohlfühlen und es sich lohnt, dort Mitglied bzw. Mieter zu sein.

c) Die Beeinträchtigung der Rechte der Klägerinnen durch das – ohne Namensnennung – veröffentlichte Foto ist dagegen gering. Es handelte sich um ein für alle Mieter und Mitbewohner zugängliches Fest, über welches die Beklagte nach den Feststellungen des Berufungsgerichts schon in den Vorjahren in ihrer Mieterbroschüre in Bildern berichtet hatte. Insofern war zu erwarten, dass in entsprechender Weise auch über das Mieterfest 2010 berichtet werden würde. Es bestehen keine Anhaltspunkte, dass das Foto heimlich angefertigt wurde, auch wenn die Klägerinnen die Anfertigung der konkreten Aufnahmen möglicherweise nicht bemerkt haben. Die Informationsbroschüre der Beklagten wurde schließlich nur an ihre Mieter verteilt, mithin an einen begrenzten Adressatenkreis, aus dem die Teilnehmer des Mieterfestes stammten. Die Revision macht schließlich nicht geltend, dass die Veröffentlichung des Bildes die kindgerechte Entwicklung der Klägerin zu 3 beeinträchtigen könnte. Dafür ist auch nichts ersichtlich.

4. Der Verbreitung des beanstandeten Bildnisses stehen auch keine besonderen schützenswerten Interessen der Klägerinnen entgegen (§ 23 Abs. 2 KUG). Das Bild ist in keiner Weise unvorteilhaft oder ehrverletzend. Entsprechendes macht die Revision auch nicht geltend.

5. War mithin die von den Klägerinnen angegriffene Veröffentlichung der beanstandeten Bildberichterstattung auch ohne ihre Einwilligung zulässig, besteht weder ein Anspruch auf Erstattung vorgerichtlicher Abmahnkosten noch ein Anspruch auf Zahlung einer Geldentschädigung wegen Verletzung des allgemeinen Persönlichkeitsrechts.

Schadensersatz bei Verlust eines zur Schließanlage gehörenden Wohnungsschlüssels (Ls)

(**Bundesgerichtshof**, Urteil vom 5. März 2014 – VIII ZR 205/13 –)

Die Schadensersatzpflicht eines Mieters, der einen zu einer Schließanlage gehörenden Schlüssel verloren hat, kann auch die Kosten des Austausches der Schließanlage umfassen, wenn der Austausch wegen bestehender Missbrauchsgefahr aus Sicherheitsgründen erforderlich ist. Ein Vermögensschaden liegt aber insoweit erst vor, wenn die Schließanlage tatsächlich ausgetauscht ist.

(Nicht amtlicher Leitsatz)

Haftung eines Netzbetreibers für Überspannungsschäden (Ls)

(**Bundesgerichtshof**, Urteil vom 25. Februar 2014 – VI ZR 144/13 –)

a) Führt eine übermäßige Überspannung zu Schäden an üblichen Verbrauchsgeräten, liegt ein Fehler des Produkts Elektrizität vor.

b) Nimmt der Betreiber des Stromnetzes Transformationen auf eine andere Spannungsebene – hier in die sogenannte Niederspannung für die Netzanschlüsse von Letztverbrauchern – vor, ist er Hersteller des Produkts Elektrizität.

c) In diesem Falle ist das Produkt Elektrizität erst mit der Lieferung des Netzbetreibers über den Netzanschluss an den Anschlussnutzer in den Verkehr gebracht.

d) Der Netzbetreiber haftet aufgrund der verschuldungsunabhängigen (Gefährdungs-) Haftung nach §§ 1 Abs. 1, 11 ProdHaftG.

(Leitsatz d nicht amtlich)

Zulässigkeit von Torkontrollen

(**Bundesarbeitsgericht**, Beschluss vom 15. April 2014 – 1 ABR 2/13 (B) –)

1. Eine Regelung zur Tor- bzw. Taschenkontrolle muss einen angemessenen Ausgleich zwischen den Schutzinteressen des Arbeitgebers und dem Anspruch auf Persönlichkeitsschutz der Beschäftigten nach § 75 Abs. 2 BetrVG darstellen.

2. Sie trägt u.a. dem Grundsatz der Verhältnismäßigkeit Rechnung, wenn ein festgestellter Schaden durch Mitarbeiterdiebstahl durch nach dem Zufallsprinzip stich-

probenartig durchgeführte Kontrollen vermieden werden soll.

3. Genügt die Regelung dem § 75 Abs. 2 BetrVG ist die Kontrolle auch nach § 32 Abs. 1 BDSG zulässig.

(Nicht amtliche Leitsätze)

Sachverhalt:

Der Betriebsrat We schloss mit der Rechtsvorgängerin der Arbeitgeberinnen für den Standort W eine Betriebsvereinbarung über die Durchführung von Torkontrollen (BV-Torkontrolle). Diese datiert vom 8. Dezember 2009. In ihr ist bestimmt:

„… vor dem Hintergrund der aktuellen, im September 2009 in Kraft getretenen arbeitsrechtlich relevanten Änderungen des Bundesdatenschutzes, insbesondere des § 32 BDSG, ist eine Anpassung der derzeitigen betrieblichen Regelung über die Durchführung von Torkontrollen wie folgt erforderlich:

…

2. Geltungsbereich:

Diese Vereinbarung gilt für alle Beschäftigten am Standort DC W und alle dort eingesetzten Arbeitnehmer von Zeitarbeitsunternehmen.

…

4. Durchführung der Torkontrolle:

4.1 Zum Schutze des persönlichen und betrieblichen Eigentums werden aus den Ausgangsdrehkreuzen durch dazu bestimmten Personen Kontrollen durchgeführt. Alle Betriebsangehörigen haben auf Verlangen über Betriebsprodukte in ihrem Besitz einen Nachweis vorzuzeigen (Kassenbon Personalverkauf).

4.2 Durch die beim Verlassen des Werkes notwendige Öffnung der Drehkreuze mittels des Werksausweises wird eine Auswahl der zu kontrollierenden Personen über einen Zufallsgenerator getroffen. Der Kontrollzyklus wird dem Betriebsrat mitgeteilt. Bei Verlassen des Werksgeländes über die Pforte kann ebenfalls jederzeit eine Kontrolle durchgeführt werden.

4.3 Die Kontrolle findet im Pförtnerraum an einer nicht einsehbaren Stelle statt. Die Kontrolle bezieht sich auf die Durchsicht mitgeführter Behältnisse, Jacken- und Manteltaschen. In begründeten Verdachtsfällen wird der Mitarbeiter aufgefordert sämtliche Kleidertaschen (Hosen und Kleider) zu leeren. Weigert sich der Mitarbeiter dem nachzukommen, kann die Kontrolle, auf Veranlassung der Firma, durch die zuständige Polizei durchgeführt werden. Über jede durchgeführte Kontrolle wird ein Protokoll angefertigt. Dieses Protokoll ist von demjenigen zu unterzeichnen, der die Kontrolle durchgeführt hat, und von dem/der betroffenen Mitarbeiter/in gegenzuzeichnen. Es dient als Nachweis der Durchführung sowie hinsichtlich etwaig beschlagnahmter Gegenstände.

5. Zusätzliche Kontrollmaßnahmen:

Bei Verdacht des Diebstahls von Firmen- oder Privateigentum können außerhalb der Zufallskontrolle weitergehende Kontrollmaßnahmen an den Werkstoren und im Werk angeordnet werden. Der Betriebsrat ist hierüber zu informieren. …

6. Schlussbestimmung:

Diese Betriebsvereinbarung tritt mit Unterzeichnung in Kraft und ist erstmals mit einer Frist von 3 Monaten zum 01.08.2012 und sodann mit einer Frist von 3 Monaten jeweils zum Folgejahr kündbar. Im Falle der Kündigung wirkt die Betriebsvereinbarung bis zum Abschluss einer neuen Vereinbarung nach.

Mit Unterzeichnung dieser Betriebsvereinbarung tritt die Betriebsvereinbarung über die Durchführung von Torkontrollen vom 30.06.2006 außer Kraft."

Bei den Arbeitgeberinnen wurden in der Zeit vom Oktober 2009 bis September 2010 im DC W Parfum- und Kosmetikwaren im Wert von etwa 250.000,00 Euro entwendet. Auf der Grundlage der BV-Torkontrolle führen sie nunmehr jährlich an 30 Tagen Torkontrollen durch, bei denen 86 Personen kontrolliert werden. Hierbei wurden in einer Reihe von Fällen Waren der Arbeitgeberinnen gefunden und Strafanzeigen erstattet.

Der Betriebsrat vertritt u.a. die Auffassung, dass die Betriebsvereinbarung über die Durchführung von Torkontrollen keine Rechtswirkung entfaltet, soweit ohne konkreten Tatverdacht Arbeitnehmerinnen und Arbeitnehmer Kontrollmaßnahmen wie die Durchsicht mitgeführter Behältnisse, Jacken- und Manteltaschen zu dulden haben.

Aus den Gründen:

3. Die in der Nr. 4 BV-Torkontrolle vereinbarten Taschenkontrollen sind materiell-rechtlich nicht zu beanstanden. Sie dienen dem repressiven wie dem präventiven Schutz der Arbeitgeberinnen vor Diebstählen. Die mit den Kontrollen einhergehenden Beeinträchtigungen des Persönlichkeitsrechts der Arbeitnehmer erfolgen unter Wahrung des Verhältnismäßigkeitsgrundsatzes.

a) Die Betriebsparteien haben mit den in dieser Betriebsvereinbarung geregelten Kontrollen nicht die ihnen nach § 75 Abs. 2 Satz 1 BetrVG obliegende Pflicht verletzt, die freie Entfaltung der Persönlichkeit der im Betrieb beschäftigten Arbeitnehmer zu schützen und zu fördern.

aa) Nach dieser Bestimmung haben die Betriebsparteien beim Abschluss von Betriebsvereinbarungen das aus Art. 2 Abs. 1 iVm. Art. 1 Abs. 1 GG abgeleitete allgemeine Persönlichkeitsrecht zu beachten (BAG 26. August 2008 – 1 ABR 16/07 – Rn. 14, BAGE 127, 276). Dieses gewährleistet Elemente der Persönlichkeit, die nicht Gegenstand der besonderen Freiheitsgarantien des Grundgesetzes sind, diesen aber in ihrer konstituierenden Bedeutung für die Persönlichkeit nicht nachstehen. Die Zuordnung eines konkreten Rechtsschutzbegehrens zu den verschiedenen Aspekten des Persönlichkeitsrechts richtet sich vor allem nach der Art der Persönlichkeitsgefährdung (BVerfG 27. Februar 2008 – 1 BvR 370/07, 1 BvR 595/07 – Rn. 151, BVerfGE 120, 274). Außerhalb des absoluten Kernbereichs privater Lebensgestaltung wird das allgemeine Persönlichkeitsrecht in den Schranken der verfassungsmäßigen Ordnung garantiert. Es kann deshalb durch verfassungsgemäße Gesetze eingeschränkt werden. Derartige Regelungen können auch die von den Betriebsparteien im Rahmen ihrer Regelungskompetenz geschlossenen Betriebsvereinbarungen enthalten. Der Gesetzgeber genügt insoweit seiner Pflicht, die Arbeitnehmer als Grundrechtsträger vor einer unverhältnismäßigen Beschränkung ihrer Grundrechte durch privatautonome Regelungen zu bewahren, indem er die Betriebsparteien in § 75 Abs. 2 Satz 1 BetrVG verpflichtet, die freie Entfaltung der Persönlichkeit der im Betrieb beschäftigten Arbeitnehmer zu schützen (BAG 26. August 2008 – 1 ABR 16/07 – Rn. 16 f., aaO).

bb) Das zulässige Maß einer Beschränkung des allgemeinen Persönlichkeitsrechts zugunsten schützenswerter Belange eines anderen Grundrechtsträgers richtet sich nach dem Grundsatz der Verhältnismäßigkeit (BAG 26. August 2008 – 1 ABR 16/07 – Rn. 17, BAGE 127, 276). Dieser verlangt eine Regelung, die geeignet, erforderlich und unter Berücksichtigung der gewährleisteten Freiheitsrechte angemessen ist, um den erstrebten Zweck zu erreichen (BAG 29. Juni 2004 – 1 ABR 21/03 – zu B I 2 d der Gründe, BAGE 111, 173). Den Betriebsparteien dürfen zur Zielerreichung keine anderen, gleich wirksamen und das Persönlichkeitsrecht der Arbeitnehmer weniger einschränkende Mittel zur Verfügung stehen. Eine Regelung ist verhältnismäßig im engeren Sinn, wenn die Schwere des Eingriffs bei einer Gesamtabwägung nicht außer Verhältnis zu dem Gewicht der ihn rechtfertigenden Gründe steht (BVerfG 4. April 2006 – 1 BvR 518/02 – zu B I 2 b dd der Gründe, BVerfGE 115, 320).

cc) Nach diesen Grundsätzen beeinträchtigen die in der BV-Torkontrolle geregelten Kontrollen das allgemeine Persönlichkeitsrecht der Arbeitnehmer nicht in unverhältnismäßiger Weise.

(1) Die Taschenkontrollen greifen allerdings in die Privatsphäre der betroffenen Arbeitnehmer ein. Diese umfasst Angelegenheiten, die wegen ihres Informationsinhalts typischerweise als „privat" eingestuft werden, weil ihre öffentliche Erörterung oder Zurschaustellung als unschicklich gilt, das Bekanntwerden als peinlich empfunden wird oder nachteilige Reaktionen der Umwelt auslöst (BVerfG 15. Dezember 1999 – 1 BvR 653/96 – zu B I 1 b cc der Gründe, BVerfGE 101, 361). Der Inhalt mitgeführter Taschen oder auch von Mantel- und Jackentaschen ist in diesem Sinne privat. Ihr Inhaber möchte die darin mitgeführten Gegenstände typischerweise nicht ohne seine Einwilligung Dritten gegenüber zeigen. Darüber hinaus wird durch Taschenkontrollen auch das Ehrgefühl von Arbeitnehmern beeinträchtigt, denn hiermit bringt der Arbeitgeber zum Ausdruck, dass er ihnen nicht uneingeschränkt vertraut.

(2) Die Beeinträchtigungen des Persönlichkeitsrechts durch die in der BV-Torkontrolle vorgesehenen Taschenkontrollen genügen jedoch den Anforderungen des Verhältnismäßigkeitsgrundsatzes.

(a) Die in der BV-Torkontrolle vereinbarten Taschenkontrollen sind geeignet, das Eigentum der Arbeitgeberinnen zu schützen. Da hierdurch Diebstähle aufgedeckt werden können und durch die Auswahl der zu kontrollierenden Arbeitnehmer über einen Zufallsgenerator die Beschäftigten jederzeit damit rechnen müssen, kontrolliert zu werden, entfaltet dieses Überwachungssystem repressive wie präventive Wirkung. Dieser Annahme steht nicht entgegen, dass die Anzahl der bislang aufgedeckten Diebstähle gering ist. Dies kann ohne weiteres auch auf der abschreckenden Wirkung der Kontrollen beruhen.

(b) Die Taschenkontrollen sind erforderlich. Andere, gleich wirksame und das Persönlichkeitsrecht der Arbeitnehmer weniger einschränkende Mittel stehen den Betriebsparteien zum Schutz des Eigentums der Arbeitgeberinnen vor Diebstählen nicht zur Verfügung. Eine Kameraüberwachung bei Verlassen des Betriebsgeländes wäre nicht gleich wirksam, da mitgeführte Gegenstände in Taschen oder Behältnissen nicht erkannt werden könnten. Eine Videoüberwachung in den Arbeitsbereichen würde das allgemeine Persönlichkeitsrecht der Arbeitnehmer stärker beeinträchtigen, da diese einer dauerhaften Beobachtung ausgesetzt wären. Ein Verbot des Mitführens von Taschen auf das Betriebsgelände wäre nicht in gleicher Weise geeignet, Diebstähle zu verhindern, weil hierdurch die Mitnahme der eher kleinräumigen Parfum- und Kosmetikprodukte in Bekleidungstaschen nicht verhindert werden kann.

(c) Die in Nr. 4 der BV-Torkontrolle vorgesehenen Kontrollmaßnahmen tragen dem Gebot der Verhältnismäßigkeit im engeren Sinn Rechnung. Die Arbeitgeberinnen haben unbestritten vorgetragen, im Rahmen von Inventuren sei festgestellt worden, dass von Oktober 2009 bis September 2010 insgesamt 1890 „Stück Parfüm" zu einem Wert zwischen 20,00 Euro und 250,00 Euro entwendet worden seien. Bei einem gemittelten Wert von 135,00 Euro ergibt sich hieraus ein Schaden in einer Größenordnung von ca. 250.000,00 Euro. Im Hinblick darauf haben die Betriebsparteien in der BV-Torkontrolle zum Schutz des Eigentumsrechts der Arbeitgeberinnen aus Art. 14 Abs. 1 GG Regelungen getroffen, die nur geringfügige Beeinträchtigungen des durch Art. 2 Abs. 1 iVm. Art. 1 Abs. 1 GG geschützten allgemeinen Persönlichkeitsrechts bewirken. Die Auswahl der zu kontrollierenden Person erfolgt nach Nr. 4.2 der BV-Torkontrolle durch einen Zufallsgenerator. Dies vermeidet eine Stigmatisierung, da hierdurch für alle Arbeitnehmer klargestellt ist, dass die Kontrolle nicht durch ein Verhalten der jeweils kontrollierten Person veranlasst ist. Die Durchführung der Kontrollmaßnahmen in dem von außen nicht einsehbaren Pförtnerraum gewährleistet, dass andere Arbeitnehmer die Kontrolle nicht beobachten können. Des Weiteren ist die Kontrollintensität in Nr. 4.3 der BV-Torkontrolle gestaffelt und abhängig von konkreten Verdachtsumständen. Zunächst wird eine Sichtkontrolle der mitgeführten Behältnisse vorgenommen. Nur in begründeten Verdachtsfällen ist die Leerung sämtlicher Kleidertaschen vorgesehen, im Falle der Weigerung, die Durchführung dieser Kontrollmaßnahme durch die Polizei. Der Kontrollzyklus ist angemessen. Pro Jahr werden an 30 Tagen insgesamt 86 Arbeitnehmer kontrolliert. Dass die Kontrolle „durch dazu bestimmte Personen" – ggf. also auch externe Sicherheitsmitarbeiter – und ohne Hinzuziehung eines Betriebsratsmitglieds durchgeführt wird, ist nicht zu beanstanden. Es ist nicht ersichtlich, dass eine Kontrolle durch eigene Mitarbeiter und in Anwesenheit eines Betriebsratsmitglieds das Persönlichkeitsrecht der Arbeitnehmer weniger beeinträchtigen würde.

b) Aus der Rechtsprechung des Bundesgerichtshofs zu AGB-Klauseln im Einzelhandel, nach denen eine nicht anlassbezogene Sichtkontrolle mitgeführter Taschen der Kunden unzulässig ist, lässt sich entgegen der Auffassung des Betriebsrats nicht die Unwirksamkeit der in der BV-Torkontrolle vorgesehenen Taschenkontrollen herleiten (dazu BGH 3. Juli 1996 – VIII ZR 221/95 –BGHZ 133, 184). Dem steht schon entgegen, dass die Arbeitgeberinnen nicht einseitig die Taschenkontrollen angeordnet haben, sondern im Zusammenwirken mit dem Betriebsrat einen rechtlichen Rahmen geschaffen haben, der die Voraussetzungen und die Durchführung der Taschenkontrollen regelt. Diese Regelung ist keine Allgemeine Geschäftsbedingung iSd. § 305 Abs. 1 Satz 1 BGB und unterliegt auch nicht den Grundsätzen einer darauf bezogenen Inhaltskontrolle. Vielmehr ist eine Betriebsvereinbarung am Maßstab des § 75 BetrVG zu überprüfen.

c) Entgegen der Ansicht des Betriebsrats steht die Protokollierungsregelung in Nr. 4.3 der BV-Torkontrolle in Einklang mit dem Bundesdatenschutzgesetz. Die mit der Protokollierung einer durchgeführten Taschenkontrolle verbundene nicht automatisierte Erhebung, Nutzung und ggf. auch Verarbeitung personenbezogener Daten von Beschäftigten der Arbeitgeberinnen sowie der bei ihnen eingesetzten Leiharbeitnehmer ist mit dem Bundesdatenschutzgesetz vereinbar. Dabei bedarf es keiner Entscheidung, ob eine solche Protokollierung über die Verweisung in § 32 Abs. 2 BDSG überhaupt dem Anwendungsbereich des § 32 Abs. 1 Satz 1 BDSG unterfällt (ablehnend Joussen NZA 2011 Beil. 1 S. 35, 40 f.) oder unter den Voraussetzungen des § 32 Abs. 1 Satz 2 BDSG als repressive sowie unter Beachtung von § 32 Abs. 1 Satz 1 BDSG als präventive Maßnahme erlaubt ist (so ErfK/Franzen 14. Aufl. § 32 BDSG Rn. 30; Taeger/Gabel-Zöll § 32 BDSG Rn. 23 f.; Wedde in Däubler/Klebe/Wedde/Weichert BDSG 4. Aufl. § 32 Rn. 130; Thüsing NZA 2009, 865, 868; Wybitul BB 2010, 1085). Ebenso wenig ist zu entscheiden, ob Leiharbeitnehmer im Entleiherbetrieb dem Anwendungsbereich des § 32 BDSG unterliegen oder für sie mangels eines Beschäftigtenverhältnisses zum Entleiher die Vorschriften des Bundesdatenschutzgesetzes nur bei einer automatisierten Erhebung, Nutzung oder Verarbeitungen ihrer personenbezogenen Daten gemäß § 28 BDSG greifen (vgl. ErfK/Franzen § 32 BDSG Rn. 5). Denn in allen Fällen ist die BV-Torkontrolle eine Rechtsvorschrift iSd. § 4 Abs. 1 BDSG, die sowohl die automatisierte als auch die nicht automatisierte Erhebung, Nutzung oder Verarbeitung personenbezogener Daten von Arbeitnehmern der Arbeitgeberinnen sowie der in ihrem Gemeinschaftsbetrieb eingesetzten Leiharbeitnehmer erlaubt (vgl. BAG 20. Dezember 1995 – 7 ABR 8/95 – zu B III 2 der Gründe, BAGE 82, 36; 30. August 1995 – 1 ABR 4/95 – zu B II 3 der Gründe, BAGE 80, 366; Gola/Schomerus BDSG

11. Aufl. § 4 Rn. 7; ErfK/Franzen § 4 BDSG Rn. 3). Da die in der BV-Torkontrolle geregelten Kontrollmaßnahmen einer Rechtskontrolle am Maßstab des § 75 Abs. 2 BetrVG standhalten, werden hierdurch datenschutzrechtliche Belange der betroffenen Arbeitnehmer nicht beeinträchtigt.

Außerordentliche Kündigung mit Auslauffrist aus betrieblichen Gründen – Sonderkündigungsschutz als Datenschutzbeauftragter

(**Bundesarbeitsgericht**, Urteil vom 23. Januar 2014, 2 AZR 372/13 –)

1. **Eine auf betriebliche Gründe gestützte außerordentliche Kündigung kommt – unter Einhaltung einer der für die ordentliche Kündigung bestehenden Auslauffrist – ggf. in Betracht, wenn ein nur außerordentlich kündbarer Arbeitnehmer trotz Wegfall der Beschäftigungsmöglichkeit noch für Jahre vergütet werden müsste.**

2. **Da es an obigen Voraussetzung im konkreten Fall fehlt, kann es dahinstehen, ob der Sonderkündigungsschutz eines betrieblichen Datenschutzbeauftragten nach § 4 f Abs. 3 S. 4 und 5 BDSG eine außerordentliche Kündigung aus betrieblichen Anlass zulässt.**

(Nicht amtliche Leitsätze)

Sachverhalt:

Die Parteien streiten über die Wirksamkeit einer außerordentlichen Kündigung.

Die Beklagte erbringt Dienstleistungen für die Stahlindustrie und deren Zulieferer. Der im März 1956 geborene Kläger war bei ihr und ihren Rechtsvorgängern seit April 1989 als kaufmännischer Angestellter beschäftigt. Er ist mit einem Grad von 50 schwerbehindert.

1997 wurde der Kläger Bereichsleiter Administration. Arbeitsvertraglich war vereinbart, dass ihn die Gesellschaft, sollte es sich als notwendig erweisen, nach vorheriger Abstimmung innerhalb des Unternehmenskreises auch mit anderen seinen Fähigkeiten, Kenntnissen und Erfahrungen entsprechenden Aufgaben betrauen könne. Die arbeitsvertraglich vereinbarte ordentliche Kündigungsfrist betrug nach Vollendung des 50. Lebensjahres des Klägers und mindestens zehn Dienstjahren zwölf Monate zum Quartalsende.

Ende 2004 bestellte die Beklagte den Kläger zum Datenschutzbeauftragten. Im Jahr 2010 löste sie den Bereich „Betriebswirtschaft" aus seinem bisherigen Verantwortungsbereich heraus. Der Kläger sollte als Bereichsleiter der Allgemeinen Verwaltung weiter tätig sein. Außerdem plante die Beklagte, ihren Verwaltungsbereich und den der H S I GmbH (HSI) in einer Servicegesellschaft zusammenzuführen. Dies geschah im August 2011 mit der neu geschaffenen HSR GmbH (HSR), von deren Anteilen die Beklagte und die HSI jeweils 50 vH hielten.

Im Hinblick auf den mit der Umstrukturierung einhergehenden Betriebsteilübergang schloss die Beklagte mit dem Betriebsrat einen Interessenausgleich und Sozialplan. Der Kläger war in der Liste der auf die HSR übergehenden Arbeitnehmer nicht genannt. Mit Schreiben vom 28. Juli 2011 teilte ihm die Beklagte mit, auch sein Arbeitsverhältnis gehe auf die HSR über. Dem widersprach der Kläger am 25. August 2011.

Mit Schreiben vom 6. September 2011 hörte die Beklagte den Betriebsrat und die Schwerbehindertenvertretung zu einer beabsichtigten außerordentlichen und hilfsweise ordentlichen betriebsbedingten Kündigung des Arbeitsverhältnisses der Parteien an. Der Betriebsrat teilte mit Schreiben vom 7. September 2011 mit, er nehme – da der Kläger leitender Angestellter sei – keine Stellung.

Am 15. September 2011 berief die Beklagte den Kläger als Datenschutzbeauftragten ab und widerrief vorsorglich seine Bestellung. Seine hiergegen gerichtete Klage wies das Arbeitsgericht zurück. Die Abberufung als Datenschutzbeauftragter sei zu Recht erfolgt. Die Entscheidung ist rechtskräftig.

Das Integrationsamt erteilte mit Bescheid vom 23. September 2011 die beantragte Zustimmung zur außerordentlichen Kündigung mit Auslauffrist. Mit Schreiben vom 26. September 2011 kündigte die Beklagte das Arbeitsverhältnis außerordentlich betriebsbedingt mit sozialer Auslauffrist zum 30. September 2012.

Mit seiner rechtzeitig erhobenen Klage hat der Kläger geltend gemacht, die Kündigung sei schon aus formalen Gründen unwirksam. Das Verfahren beim Integrationsamt sei nicht wirksam eingeleitet worden. Außerdem fehle es an einem wichtigen Grund zur Kündigung. Der Übergang seines Arbeitsverhältnisses auf die HSR habe nicht den Planungen entsprochen. Er habe als Mitarbeiter der Beklagten im Wege der Personalüberlassung für die HSR arbeiten sollen. Schon am 25. Juli 2011 habe er seine Arbeit bei der HSR aufgenommen. Trotz seines Widerspruchs gegen den Übergang seines Arbeitsverhältnisses sei ihm erst am 13. Januar 2012 mitgeteilt worden, dass er in die Räumlichkeiten der Beklagten zurückkehren solle. Statt seiner sei nun ein Mitarbeiter der HSI zum IT-Leiter bestellt worden. Er könne ohne weiteres im Bereich Organisation, Controlling und Prozessentwicklung bei der Beklagten weiterbeschäftigt werden. Es bestünden auch Weiterbeschäftigungsmöglichkeiten im Konzern. Im Übrigen seien weder die Sozialauswahl ordnungsgemäß durchgeführt noch der Betriebsrat ordnungsgemäß angehört worden.

Die Vorinstanzen haben der Klage stattgegeben. Mit der Revision verfolgt die Beklagte ihr Begehren weiter, die Klage abzuweisen.

Aus den Gründen:

Die Revision ist unbegründet. Das Landesarbeitsgericht hat der Klage zu Recht stattgegeben. Die außerordentliche Kündigung der Beklagten vom 26. September 2011 ist unwirksam. Die Umdeutung in eine ordentliche Kündigung ist nicht möglich.

I. Das Arbeitsverhältnis der Parteien ist durch die außerordentliche Kündigung vom 26. September 2011 nicht aufgelöst worden.

1. Gemäß § 626 Abs. 1 BGB kann ein Arbeitsverhältnis aus wichtigem Grund außerordentlich gekündigt werden, wenn Tatsachen vorliegen, aufgrund derer dem Kündigenden unter Berücksichtigung aller Umstände des Einzelfalls und unter Abwägung der Interessen beider Vertragsteile die Fortsetzung des Arbeitsverhältnisses selbst bis zum Ablauf der Kündigungsfrist oder der vereinbarten Beendigung des Arbeitsverhältnisses nicht zugemutet werden kann.

a) Eine außerordentliche Kündigung aus betrieblichen Gründen ist gegenüber einem ordentlich kündbaren Arbeitnehmer grundsätzlich unzulässig. Sie setzt voraus, dass dem Arbeitgeber die Weiterbeschäftigung bis zum Ablauf der Kündigungsfrist unzumutbar ist. Das ist bei einer betriebsbedingten Kündigung regelmäßig nicht der Fall. Dem Arbeitgeber ist es, wenn eine Weiterbeschäftigungsmöglichkeit für den Arbeitnehmer aus betrieblichen Gründen entfällt, selbst im Insolvenzfall zuzumuten, die Kündigungsfrist einzuhalten (BAG 20. Juni 2013 – 2 AZR 379/12 – Rn. 14; 24. Januar 2013 – 2 AZR 453/11 – Rn. 22).

b) Eine auf betriebliche Gründe gestützte außerordentliche Kündigung kommt – unter Einhaltung einer der ordentlichen Kün-

digungsfrist entsprechenden Auslauffrist – allenfalls in Betracht, wenn die Möglichkeit einer ordentlichen Kündigung ausgeschlossen ist und dies dazu führt, dass der Arbeitgeber den Arbeitnehmer andernfalls trotz Wegfalls der Beschäftigungsmöglichkeit noch für Jahre vergüten müsste, ohne dass dem eine entsprechende Arbeitsleistung gegenüberstünde (BAG 20. Juni 2013 – 2 AZR 379/12 – Rn. 15; 24. Januar 2013 – 2 AZR 453/11 – Rn. 22). Es kann dem Arbeitgeber unzumutbar sein, ein sinnentleertes Arbeitsverhältnis über solche Zeiträume hinweg allein durch Gehaltszahlungen ohne adäquate Gegenleistung aufrechtzuerhalten (BAG 18. März 2010 – 2 AZR 337/08 – Rn. 17). Allerdings ist der Arbeitgeber wegen des Ausschlusses der ordentlichen Kündigung in einem besonderen Maß verpflichtet zu versuchen, die Kündigung durch geeignete andere Maßnahmen zu vermeiden. Besteht irgendeine Möglichkeit, das Arbeitsverhältnis sinnvoll fortzusetzen, wird er den Arbeitnehmer in der Regel entsprechend einzusetzen haben. Erst wenn alle denkbaren Alternativen ausscheiden, kann ein wichtiger Grund zur außerordentlichen Kündigung vorliegen (BAG 20. Juni 2013 – 2 AZR 379/12 – aaO; 22. November 2012 – 2 AZR 673/11 – Rn. 14).

2. Im Streitfall fehlt es an einem wichtigen Grund in diesem Sinne. Es muss deshalb nicht entschieden werden, ob es in Betracht kommt, auch das Arbeitsverhältnis eines Mitarbeiters, das nach § 15 KSchG oder § 4f Abs. 3 Satz 5 bzw. Satz 6 BDSG nur aus wichtigem Grund gekündigt werden kann, aus betrieblichem Anlass wirksam außerordentlich zu kündigen. Ob bei der Prüfung des wichtigen Grundes iSv. § 626 Abs. 1 BGB auch in diesen Fällen nicht auf die fiktive Kündigungsfrist, sondern auf das Ende des Bestandsschutzes abzustellen ist, kann damit gleichermaßen offenbleiben (vgl. zur betrieblich veranlassten außerordentlichen Änderungskündigung des Arbeitsverhältnisses eines Betriebsratsmitglieds BAG 21. Juni 1995 – 2 ABR 28/94 – zu B II 2 b der Gründe, BAGE 80, 185).

a) Zugunsten der Beklagten kann unterstellt werden, dass das Arbeitsverhältnis der Parteien nach § 4f Abs. 3 Satz 6 BDSG ordentlich nicht kündbar und der Arbeitsplatz des Klägers bei ihr infolge des Betriebsübergangs entfallen war.

b) Auch unter diesen Annahmen war die Beklagte wegen des Sonderkündigungsschutzes des Klägers nicht für Jahre ohne eine entsprechende Gegenleistung zur Vergütungszahlung verpflichtet. Sie hatte den Kläger im Zeitpunkt der Kündigung als Datenschutzbeauftragten bereits abberufen. Der Ausschluss der ordentlichen Kündigung galt danach gemäß § 4f Abs. 3 Satz 6 BDSG allenfalls noch für ein Jahr. Einen solchen Zeitraum ggf. auch ohne adäquate Gegenleistung des Arbeitnehmers überbrücken zu müssen, ist einem Arbeitgeber grundsätzlich nicht unzumutbar. Die Grenze zum wichtigen Grund ist allenfalls dann überschritten, wenn ein sinnentleertes Arbeitsverhältnis über deutlich längere Zeiträume fortgeführt werden müsste. Dafür ist im Streitfall nichts ersichtlich. Nach Auslaufen des Sonderkündigungsschutzes kann die Beklagte – bei Vorliegen eines Kündigungsgrundes – wieder ordentlich kündigen. Auf die dann einzuhaltende Kündigungsfrist ist nicht zusätzlich abzustellen. Dass eine ordentliche Kündigung nur unter Wahrung der maßgeblichen Frist erfolgen kann, ist keine Folge des Sonderkündigungsschutzes. Der Arbeitgeber hätte die Frist auch dann zu wahren, wenn die Möglichkeit der ordentlichen Kündigung nicht ausgeschlossen wäre.

c) Hinzu kommt, dass die Beklagte nicht dargelegt hat, alle Anstrengungen unternommen zu haben, um einen weiteren Einsatz des Klägers bei der HSR zu ermöglichen.

aa) Im Falle einer außerordentlichen Kündigung aus betrieblichen Gründen hat der Arbeitgeber nicht nur darzutun, dass eine Weiterbeschäftigung des Arbeitnehmers am bisherigen Arbeitsplatz infolge seiner Organisationsentscheidung nicht mehr möglich ist. Er hat vielmehr außerdem und von sich aus darzulegen, dass überhaupt keine Möglichkeit besteht, das Arbeitsverhältnis – und sei es zu geänderten Bedingungen und nach entsprechender Umschulung – sinnvoll fortzusetzen (BAG 20. Juni 2013 – 2 AZR 379/12 – Rn. 36; 22. November 2012 – 2 AZR 673/11 – Rn. 41). Anders als bei der ordentlichen Kündigung reicht es nicht aus, dass der Arbeitgeber zunächst vorträgt, eine Weiterbeschäftigung des Arbeitnehmers sei infolge des Wegfalls des Arbeitsplatzes nicht möglich, und sodann eine dem widersprechende Darlegung des Arbeitnehmers abwartet. Das Fehlen jeglicher Beschäftigungsmöglichkeit zählt bei der außerordentlichen betriebsbedingten Kündigung zum „wichtigen Grund". Es ist deshalb vom Arbeitgeber darzulegen (BAG 20. Juni 2013 – 2 AZR 379/12 – aaO; 22. November 2012 – 2 AZR 673/11 – aaO). Dessen Vorbringen muss deutlich machen, dass er alles Zumutbare unternommen hat, um die durch sein (neues) unternehmerisches Konzept notwendig werdenden Anpassungen der Vertragsbedingungen auf das unbedingt erforderliche Maß zu beschränken (BAG 20. Juni 2013 – 2 AZR 379/12 – Rn. 26).

bb) Die Beklagte hat nicht vorgetragen, in welcher Weise sie sich nach dem Widerspruch des Klägers gegen einen Übergang seines Arbeitsverhältnisses auf die HSR um ein Einverständnis von deren anderer Gesellschafterin – der HSI – mit einem weiteren Einsatz des Klägers bei der HSR – zumindest für die Dauer seines Sonderkündigungsschutzes – bemüht habe. Der Kläger hatte seine seit Ende Juli 2011 für die HSR ausgeübte Tätigkeit auch nach seinem Widerspruch zunächst noch für diese fortgeführt. Die Beklagte hat zwar geltend gemacht, sie habe keinen bestimmenden Einfluss auf die HSR und könne eine Beschäftigung des Klägers dort nicht durchsetzen. Daraus wird jedoch nicht deutlich, dass sie alles Zumutbare unternommen hätte, um die Weiterbeschäftigung des Klägers auch ohne einseitige Entscheidungsbefugnis zu ermöglichen. Einzige weitere Gesellschafterin der HSR neben ihr war – zu gleichen Anteilen – die HSI. Dass sie sich um deren Einverständnis mit einem weiteren Einsatz des Klägers bei der HSR überhaupt bemüht hätte, wird aus ihrem Vorbringen nicht ersichtlich. Sie hat allein darauf verwiesen, zu einem entsprechenden Gesellschafterbeschluss bestehe vor dem Hintergrund einer drohenden „Zweiklassengesellschaft" keine Bereitschaft. Dies lässt weder erkennen, dass nicht nur ihr selbst, sondern gerade der HSI die entsprechende Bereitschaft fehlte, noch wird deutlich, dass sie jedenfalls versucht hat, sich mit der HSI über einen weiteren tatsächlichen Einsatz des Klägers bei der HSR zu einigen.

3. Die außerordentliche Kündigung ist nicht nach § 15 Abs. 4 oder Abs. 5 KSchG wirksam, selbst wenn diese Bestimmungen – analoge – Anwendung fänden. § 15 Abs. 4 und Abs. 5 KSchG senken nicht etwa die Anforderungen an eine außerordentliche Kündigung ab. Sie erklären vielmehr unter bestimmten Voraussetzungen eine ordentliche Kündigung für zulässig (vgl. BAG 21. Juni 2001 – 2 AZR 137/00 – zu II 1 der Gründe; 14. Oktober 1982 – 2 AZR 568/80 – zu B I 2 a der Gründe, BAGE 41, 72; ErfK/Kiel 14. Aufl. § 15 KSchG Rn. 40; KR/Etzel 10. Aufl. § 15 KSchG Rn. 73; vHH/L/v. Hoyningen-Huene 15. Aufl. § 15 Rn. 164; SPV/Vossen 10. Aufl. Rn. 1700, 1706).

4. Eine Umdeutung der außerordentlichen Kündigung in eine ordentliche Kündigung nach § 140 BGB ist nicht möglich. Auch in diesem Zusammenhang kann unentschieden bleiben, ob im Streitfall die ordentliche Kündigung nach § 4f Abs. 3 Satz 5 bzw. Satz 6 BDSG ausgeschlossen war. Ebenso wenig kommt es darauf an, ob auf Arbeitnehmer, die nach § 4f Abs. 3 Satz 5 bzw. Satz 6 BDSG geschützt sind, die Regelungen des § 15 Abs. 4 und Abs. 5 KSchG entsprechend anzuwenden sind und die Voraussetzungen für eine ordentliche Kündigung vorgelegen haben. Es fehlt in jedem Fall an der nach § 85 SGB IX erforderlichen Zustimmung des Integrationsamts.

a) Der Sonderkündigungsschutz nach § 85 SGB IX gilt ggf. neben § 15 Abs. 4 und Abs. 5 KSchG (KR/Etzel 10. Aufl. § 15 KSchG Rn. 151, 152; APS/Linck 4. Aufl. § 15 KSchG Rn. 197; ebenso LAG München 3. August 2006 – 3 Sa 459/06 –).

b) Das Integrationsamt hatte im Streitfall lediglich die Zustimmung zu einer außerordentlichen Kündigung erteilt. Darin war weder – zugleich – eine Zustimmung zu einer auch ordentlichen Kündigung enthalten, noch kann die Zustimmung zur außerordentlichen Kündigung nach § 43 Abs. 1 SGB X in eine Zustimmung zur ordentlichen Kündigung umgedeutet werden (vgl. auch BAG 7. Juli 2011 – 2 AZR 355/10 – Rn. 36, BAGE 138, 312).

aa) Der Bescheid des Integrationsamts über die Zustimmung zur außerordentlichen Kündigung ist nicht dahin auszulegen, dass mit ihm (auch) die Zustimmung zu einer ordentlichen Kündigung erteilt worden wäre. Das Integrationsamt wollte erkennbar keine Zustimmung zur ordentlichen Kündigung erteilen. Es hat ausdrücklich allein einer außerordentlichen Kündigung – mit sozialer Auslauffrist – zugestimmt. Nur darauf war auch der Antrag der Beklagten gerichtet.

bb) Eine Umdeutung des Bescheids ist nicht möglich.

(1) Nach § 43 Abs. 1 SGB X kann nur ein fehlerhafter Verwaltungsakt umgedeutet werden. Anhaltspunkte dafür, dass die Zustimmung des Integrationsamts im Streitfall fehlerhaft erfolgt wäre, gibt es nicht.

(2) Eine Umdeutung setzt gemäß § 43 Abs. 1 SGB X außerdem voraus, dass der neue Bescheid von der erlassenden Behörde in der tatsächlich gewählten Verfahrensweise und Form ebenfalls rechtmäßig hätte erlassen werden können. Das ist hier nicht der Fall. Wie sich aus § 91 Abs. 1 SGB IX ergibt, unterscheiden sich die Verfahren auf Zustimmung zu einer ordentlichen und zu einer außerordentlichen Kündigung nicht unerheblich (vgl. APS/Vossen 4. Aufl. § 91 SGB IX Rn. 23; KR/Etzel/Gallner 10. Aufl. § 91 SGB IX Rn. 35). Die Entscheidungsgrundlage für das Integrationsamt ist nicht dieselbe (Schaub/Koch ArbR-HdB 15. Aufl. § 179 Rn. 37). Das gilt auch mit Blick auf die außerordentliche Kündigung mit Auslauffrist. Auch auf diese findet nicht § 85 SGB IX, sondern findet § 91 SGB IX Anwendung (BAG 12. Mai 2005 – 2 AZR 159/04 – zu B I 1 der Gründe). Soweit im Schrifttum – hiervon abweichend – angenommen wird, die außerordentliche Kündigung mit Auslauffrist erfordere eine Zustimmung allein nach § 85 SGB IX (vgl. HaKo/Fiebig/Osnabrücke 4. Aufl. §§ 85 – 92 SGB IX Rn. 69; HaKo/Gieseler 4. Aufl. § 626 BGB Rn. 46; aA AnwK-ArbR/Euler 2. Aufl. Bd. 2 § 91 SGB IX Rn. 2; Neumann in Neumann/Pahlen/Majerski-Pahlen SGB IX 12. Aufl. § 91 Rn. 2, 4; KR/Etzel/Gallner § 91 SGB IX Rn. 2, 35), folgt im Übrigen auch daraus nicht, dass die Zustimmung zu einer außerordentlichen Kündigung mit Auslauffrist in eine Zustimmung zur ordentlichen Kündigung umgedeutet werden könnte (vgl. ErfK/Rolfs 14. Aufl. § 91 SGB IX Rn. 8; Neumann in Neumann/Pahlen/Majerski-Pahlen SGB IX § 91 Rn. 7).

II. Als unterlegene Partei hat gemäß § 97 Abs. 1 ZPO die Beklagte die Kosten der Revision zu tragen.

Einsichtsrecht des Betriebsrats in Bruttoentgeltlisten

(**Bundesarbeitsgericht**, vom 14. Januar 2014 – 1 ABR 54/12 –)

1. In einer Klinik ist einem vom Betriebsrat benannten Mitglied Einsicht in die Bruttolohn- und Gehaltslisten der Arbeitnehmer mit Ausnahme der leitenden Angestellten hinsichtlich sämtlicher Entgeltbestandteile, d.h. einschließlich der privatärztlichen Liquidationserlöse, zu gewähren.

2. Die mit der Einsichtnahme erfolgte Datennutzung ist nach § 32 Abs. 1 BDSG zulässig aufgrund der Informationspflicht nach § 80 Abs. 2 S.2, 2 Halbs.BetrVG.

3. Ein Widerspruchsrecht steht den Mitarbeitern gegenüber dem Informationsanspruch nicht zu. Der Arbeitgeber ist nicht befugt, sich gegenüber dem Anspruch des Betriebsrats aus & 80 Abs. 2 Satz 2 Halbs. 2 BetrVG auf das informationelle Selbstbestimmungsrecht von Arbeitnehmern zu berufen.

(Nicht amtliche Leitsätze)

Sachverhalt:

A. Die Beteiligten streiten über das Einsichtsrecht des Betriebsrats in die Bruttoentgeltlisten der Arbeitnehmer.

Die Arbeitgeberin betreibt in H eine neurochirurgische Klinik mit ca. 120 Arbeitnehmern. Antragsteller ist der dort gebildete Betriebsrat.

Die Arbeitgeberin hat mit der „DHV – Die Berufsgewerkschaft e. V." und mit der Arbeitnehmervereinigung „medsonet" als „Haustarifverträge" bezeichnete Kollektivvereinbarungen abgeschlossen. Hiernach haben deren Mitglieder Anspruch auf eine gegenüber anderen Arbeitnehmern erhöhte jährliche Sonderzahlung. Darüber hinaus bestehen arbeitsvertragliche Entgeltvereinbarungen, die eine Beteiligung der betreffenden Arbeitnehmer an privatärztlichen Liquidationserlösen vorsehen.

Ende des Jahres 2009 lehnte es die Arbeitgeberin ab, dem Betriebsrat Einsicht in die Bruttoentgeltlisten der bei ihr beschäftigten Arbeitnehmer zu geben, weil dem etwa die Hälfte der Arbeitnehmer widersprochen habe.

Der Betriebsrat hat die Auffassung vertreten, er könne umfassend in die Listen der Bruttolöhne und -gehälter Einsicht nehmen. Dieses Recht erfasse sämtliche Vergütungsbestandteile, einschließlich tariflicher Sonderzahlungen und privatärztlicher Liquidationserlöse.

Die Arbeitgeberin hat zur Begründung ihres Abweisungsantrags ausgeführt, der Einsichtnahme stünden datenschutzrechtliche und grundrechtliche Belange der Arbeitnehmer entgegen.

Aus den Gründen:

IV. Der Antrag ist begründet. Die Arbeitgeberin ist nach § 80 Abs. 2 Satz 2 Halbs. 2 BetrVG verpflichtet, einem vom Betriebsrat zu benennenden Betriebsratsmitglied Einsicht in die Bruttoentgeltlisten zu gewähren. Datenschutzrechtliche oder grundrechtliche Belange stehen dem Anspruch nicht entgegen.

1. Nach § 80 Abs. 2 Satz 2 BetrVG sind dem Betriebsrat auf Verlangen jederzeit die zur Durchführung seiner Aufgaben erforderlichen Unterlagen zur Verfügung zu stellen; in diesem Rahmen ist der Betriebsausschuss oder ein nach § 28 BetrVG gebildeter Ausschuss berechtigt, in die Listen über die Bruttolöhne und -gehälter Einblick zu nehmen. Das Einsichtsrecht nach § 80 Abs. 2 Satz 2 Halbs. 2 BetrVG unterliegt dabei den Grenzen der allgemeinen Regelung in § 80 Abs. 2 Satz 2 Halbs. 1 BetrVG (BAG 30. September 2008 – 1 ABR 54/07 – Rn. 25, BAGE 128, 92).

a) In Betrieben, in denen kein Betriebsausschuss gebildet ist, kann das Einsichtsrecht durch den Betriebsratsvorsitzenden, dessen Stellvertreter oder ein anderes beauftragtes Betriebsratsmitglied, dem die Führung der laufenden Geschäfte nicht übertragen sein muss, wahrgenommen werden (vgl. BAG 16. August 1995 – 7 ABR 63/94 – zu B I 1 der Gründe mwN, BAGE 80, 329). Da der

Betriebsrat hier nur sieben Mitglieder hat, war nach § 27 Abs. 1 BetrVG kein Betriebsausschuss zu bilden. Nach den Feststellungen des Landesarbeitsgerichts bestand auch kein Ausschuss nach § 28 BetrVG. Das Einsichtsrecht steht daher einem vom Betriebsrat zu benennenden Mitglied zu.

b) Der Betriebsrat kann nur Einsicht in Unterlagen verlangen, die der Arbeitgeber zumindest in Form einer elektronischen Datei tatsächlich besitzt. Der Arbeitgeber ist nicht verpflichtet, nicht vorhandene Unterlagen erst zu erstellen (BAG 30. September 2008 – 1 ABR 54/07 – Rn. 26, BAGE 128, 92). Dieses Verständnis liegt auch der Antragstellung des Betriebsrats zugrunde.

c) Das Einsichtsrecht umfasst alle Lohn- und Gehaltsbestandteile tariflicher wie außertariflicher Art, unabhängig davon, ob es sich um einmalige oder wiederkehrende Leistungen des Arbeitgebers handelt, und unabhängig davon, ob sie kollektivrechtlich oder einzelvertraglich vereinbart sind. § 80 Abs. 2 Satz 2 Halbs. 2 BetrVG lässt sich nicht entnehmen, dass bestimmte Lohnbestandteile generell vom Einsichtsrecht des Betriebsrats ausgenommen sind (BAG 10. Februar 1987 – 1 ABR 43/84 – zu B II 2 a der Gründe; Fitting 27. Aufl. § 80 Rn. 73 mwN).

d) Das Einsichtsrecht des Betriebsrats besteht, soweit dies zur Durchführung seiner Aufgaben erforderlich ist.

aa) Der Betriebsrat muss ein besonderes Überwachungsbedürfnis nicht darlegen. Der nötige Aufgabenbezug ist regelmäßig schon deshalb gegeben, weil der Betriebsrat nach § 80 Abs. 1 Nr. 1 BetrVG darüber zu wachen hat, dass die zugunsten der Arbeitnehmer geltenden Gesetze und Tarifverträge durchgeführt werden. Hierzu gehört auch die sich aus § 75 Abs. 1 BetrVG ergebende Verpflichtung des Arbeitgebers zur Beachtung des allgemeinen Gleichbehandlungsgrundsatzes. Der Darlegung eines besonderen Anlasses für die Ausübung des Einsichtsrechts bedarf es dabei auch im Hinblick auf individuell vereinbarte übertarifliche Vergütungen nicht. Der Betriebsrat benötigt die Kenntnis der effektiv gezahlten Vergütungen, um sich ein Urteil darüber bilden zu können, ob insoweit ein Zustand innerbetrieblicher Lohngerechtigkeit existiert oder nur durch eine andere betriebliche Lohngestaltung erreicht werden kann. Ein Einsichtsrecht besteht deshalb auch dann, wenn der Betriebsrat gerade feststellen will, welche Arbeitnehmer Sonderzahlungen erhalten und wie hoch diese sind. Die Grenzen des Einsichtsrechts liegen dort, wo ein Beteiligungsrecht oder eine sonstige Aufgabe offensichtlich nicht in Betracht kommt (BAG 13. Februar 2007 – 1 ABR 14/06 – Rn. 23 ff., BAGE 121, 139).

bb) Nach diesen Grundsätzen ist der Einblick in die Bruttoentgeltlisten zur Durchführung der Aufgaben des Betriebsrats erforderlich.

(1) Hierdurch will der Betriebsrat zum einen feststellen, ob die Beteiligung an den privatärztlichen Liquidationserlösen auf einem abstrakten System beruht und damit ein kollektiver Tatbestand vorliegt. Da dies jedenfalls nicht offensichtlich ausgeschlossen ist, besteht eine ausreichende Wahrscheinlichkeit für das Bestehen eines Mitbestimmungsrechts nach § 87 Abs. 1 Nr. 10 BetrVG (dazu BAG 16. Juni 1998 – 1 ABR 67/97 – BAGE 89, 128). Dem steht nicht entgegen, dass die Beteiligung der einzelnen Mitarbeiter an diesen Erlösen nach dem Vortrag der Arbeitgeberin individuell ausgehandelt ist. Es geht dem Betriebsrat gerade darum, dies zu überprüfen.

(2) Der Einblick in die Bruttoentgeltlisten ermöglicht dem Betriebsrat zum anderen, die Einhaltung des Gleichbehandlungsgrundsatzes bei der Erbringung von Sonderzahlungen zu überwachen. Es ist nicht ausgeschlossen, dass die Arbeitgeberin nicht nur Mitgliedern der DHV oder von medsonet derartige Zahlungen leistet, sondern auch anderen Arbeitnehmern. Hinzu kommt, dass medsonet zu keinem Zeitpunkt tariffähig war (BAG 11. Juni 2013 – 1 ABR 33/12 –) und der DHV jedenfalls bis zum 9. Januar 2013 nur für Arbeitnehmer in kaufmännischen oder verwaltenden Berufen tarifzuständig war (vgl. BAG 11. Juni 2013 – 1 ABR 32/12 –). Damit steht fest, dass die seitens der Arbeitgeberin mit medsonet geschlossenen Kollektivvereinbarungen keine Tarifverträge darstellen und die mit der DHV geschlossenen Vereinbarungen jedenfalls insoweit unwirksam sind, als sie darauf gerichtet sind, die Arbeitsbedingungen des medizinischen Personals zu gestalten. Diese Kollektivvereinbarungen sind damit als solche nicht geeignet, eine Ungleichbehandlung der Arbeitnehmer bei der Leistung von Jahressonderzahlungen zu rechtfertigen.

2. Dem Anspruch des Betriebsrats auf Einblick in die Bruttoentgeltlisten stehen datenschutzrechtliche Belange nicht entgegen.

Bruttoentgeltlisten enthalten personenbezogene Daten iSv. § 3 Abs. 1 BDSG, die von Arbeitgebern zur Durchführung des Arbeitsverhältnisses nach § 32 Abs. 1 Satz 1 BDSG zulässigerweise erhoben, verarbeitet und genutzt werden (vgl. hierzu BT-Drucks. 16/13657 S. 21). Gewährt die Arbeitgeberin einem Betriebsratsmitglied nach § 80 Abs. 2 Satz 2 Halbs. 2 BetrVG Einsicht in die Bruttoentgeltlisten, handelt es sich um eine nach § 32 Abs. 1 BDSG zulässige Form der Datennutzung. Dies folgt schon daraus, dass die Beteiligungsrechte der Interessenvertretungen der Beschäftigten nach § 32 Abs. 3 BDSG durch die nach Absatz 1 dieser Bestimmung erlaubte Datennutzung nicht berührt werden. Zu den Interessenvertretungen der Beschäftigten in diesem Sinne zählt auch der Betriebsrat (vgl. BT-Drucks. 16/13657 S. 21). Hinzu kommt, dass dieser selbst Teil der verantwortlichen Stelle iSd. § 3 Abs. 7 BDSG ist (BAG 7. Februar 2012 – 1 ABR 46/10 – Rn. 43 mwN, BAGE 140, 350). Die Einsichtsgewährung stellt daher keine Weitergabe von Daten an Dritte dar (Fitting § 80 Rn. 58; Gola/Schomerus BDSG 11. Aufl. § 3 Rn. 49).

3. Es bedarf keiner Entscheidung, ob das durch Art. 2 Abs. 1 iVm. Art. 1 Abs. 1 GG gewährleistete Recht auf informationelle Selbstbestimmung der Arbeitnehmer dem Einsichtsrecht des Betriebsrats entgegensteht (verneinend zu der entsprechenden Vorschrift in § 78 Abs. 2 Satz 1 und Satz 2 HmbPersVG BVerwG 16. Mai 2012 – 6 PB 2/12 – Rn. 3). Der Arbeitgeber ist nicht befugt, sich gegenüber dem Anspruch des Betriebsrats aus § 80 Abs. 2 Satz 2 Halbs. 2 BetrVG auf Grundrechte von Arbeitnehmern zu berufen (vgl. zum Überwachungsrecht des Betriebsrats aus § 84 Abs. 2 Satz 7 SGB IX BAG 7. Februar 2012 – 1 ABR 46/10 – BAGE 140, 350).

4. Die Arbeitgeberin kann zur Begründung der Ablehnung des Einsichtsrechts des Betriebsrats auch nicht eine Verletzung des durch Art. 8 Abs. 1 GRC gewährleisteten Schutzes personenbezogener Daten der bei ihr beschäftigten Arbeitnehmer geltend machen. Hierbei handelt es sich nicht um ein eigenes Recht der Arbeitgeberin, sondern um Individualinteressen der Arbeitnehmer. Art. 8 Abs. 1 GRC vermittelt der Arbeitgeberin weder unmittelbar noch mittelbar eine geschützte Rechtsposition, die sie dem Einsichtsrecht des Betriebsrats entgegenhalten könnte (für Rechte aus der UN-Behindertenrechtskonvention vgl. BAG 14. Mai 2013 – 1 ABR 10/12 – Rn. 27).

5. Dem Einsichtsrecht steht die durch Art. 5 Abs. 3 Satz 1 GG geschützte Wissenschaftsfreiheit nicht entgegen.

a) Dieses Freiheitsrecht – das auch juristischen Personen zustehen kann (vgl. Starck in v. Mangoldt/Klein/Starck GG 6. Aufl. Art. 5 Rn. 408 mwN) – gewährt jedem, der in Wissenschaft, Forschung und Lehre tätig ist, ein Grundrecht auf freie wissenschaftliche Betätigung. Wissenschaft ist ein grundsätzlich von Fremdbestimmung freier Bereich autonomer Verantwortung. Den Kernbereich wissenschaftlicher Betätigung stellen die auf wissenschaftlicher Eigengesetzlichkeit beruhenden Prozesse, Verhaltensweisen und Entscheidungen bei der Suche nach Erkenntnissen, ihrer Deutung und Weitergabe dar. Als Abwehrrecht schützt das Grundrecht die wissenschaftliche Betätigung gegen staatliche Ein-

griffe und gewährt dem einzelnen Wissenschaftler einen vorbehaltlos geschützten Freiraum (BVerfG 28. Oktober 2008 – 1 BvR 462/06 – Rn. 40, BVerfGE 122, 89).

b) Der Schutzbereich dieses Freiheitsrechts ist vorliegend nicht berührt. Die Arbeitgeberin trägt nicht einmal vor, wissenschaftlich tätig zu sein. Sie bezieht sich lediglich auf wissenschaftliche Publikationen einiger bei ihr angestellter Ärzte. Damit beruft sie sich auf ein Grundrecht der Arbeitnehmer, das ihr selbst keine eigene geschützte Rechtsposition vermittelt. Hinzu kommt, dass die durch Art. 5 Abs. 3 GG geschützte Wissenschaftsfreiheit der einzelnen Arbeitnehmer nicht die hierbei erzielten Verdienste schützt. Gegenteiliges folgt auch nicht aus der von der Rechtsbeschwerde angezogenen Entscheidung des VGH Baden-Württemberg (vgl. VGH Baden-Württemberg 25. November 2008 – PL 15 S 2634/07 –) zum Einsichtsrecht eines Personalrats in Vergütungslisten der an einem Theater tätigen Personen. Diese hat das Bundesverwaltungsgericht aufgehoben, weil das personalvertretungsrechtliche Einsichtsrecht die durch Art. 5 Abs. 3 Satz 1 GG geschützte Kunstfreiheit der Theaterleitung, soweit sie sich in der Vereinbarung bestimmter Entgelte für die am Theater beschäftigten Künstler ausdrückt, nicht beschränkt (BVerwG 16. Februar 2010 – 6 P 5/09 – Rn. 26).

6. Das Einsichtsrecht aus § 80 Abs. 2 Satz 2 Halbs. 2 BetrVG ist entgegen der Ansicht der Arbeitgeberin auch nicht gleichheitswidrig (Art. 3 Abs. 1 GG).

Es ist verfassungsrechtlich nicht zu beanstanden, dass leitende Angestellte nach § 5 Abs. 3 BetrVG von den Vorschriften des Betriebsverfassungsgesetzes ausgenommen sind und deren Bruttoentgeltunterlagen deshalb nicht dem Einblicksrecht des Betriebsrats unterliegen. Die Herausnahme leitender Angestellter aus dem Betriebsverfassungsrecht beruht darauf, dass leitende Angestellte kraft ihrer Funktion Unternehmerinteressen wahrzunehmen haben und daher nicht gleichzeitig in der Betriebsverfassung Arbeitnehmerinteressen vertreten sollen. Dieser Grund rechtfertigt die Herausnahme der leitenden Angestellten aus dem Geltungsbereich der Vorschriften des Betriebsverfassungsgesetzes (vgl. BAG 16. Juli 1985 – 1 AZR 206/81 – zu III 3 c der Gründe, BAGE 49, 199). Soweit die Arbeitgeberin auf praktische Schwierigkeiten bei der Abgrenzung von leitenden Angestellten iSv. § 5 Abs. 3 BetrVG und Arbeitnehmern iSv. § 5 Abs. 1 BetrVG hinweist, führt dies zu keinem anderen Ergebnis. Die in § 5 Abs. 3 BetrVG enthaltene Umschreibung des Personenkreises der leitenden Angestellten genügt nach der Rechtsprechung des Bundesverfassungsgerichts dem rechtsstaatlichen Bestimmtheitsgebot (BVerfG 24. November 1981 – 2 BvL 4/80 – BVerfGE 59, 104; vgl. auch BAG 29. Januar 1980 – 1 ABR 45/79 – BAGE 32, 381).

Haftung des Personalberaters wegen Verletzung der Verschwiegenheitspflicht

(**Oberlandesgericht Frankfurt a.M.**, Urteil vom 8. Mai 2014 – 16 U 175/13 –)

Informiert ein Personalberater eine Bewerberin, dass sein Auftraggeber es ablehne, eine Frau einzustellen, und motiviert er die Bewerberin zur Geltendmachung von AGG-Entschädigungsansprüchen, so verletzt er seine gegenüber seinem Auftraggeber bestehende Verschwiegenheitspflicht.

(Nicht amtlicher Leitsatz)

Sachverhalt:

Die Klägerin begehrt von dem Beklagten Schadensersatz wegen Verletzung einer Verschwiegenheitsverpflichtung.

Die Klägerin beauftragte am …. Juni 2012 den Beklagten, einen Personalberater, der in seinen Unterlagen … mit strikter Diskretion und einer Vertrauensgarantie wirbt, mit der Suche einer geeigneten Persönlichkeit für die Position eines …. Anfang September 2012 übersandte der Beklagte der Klägerin die Bewerbungsunterlagen von Frau A. Mit E-Mail vom …. September 2012 teilte der Personalleiter der Klägerin dem Beklagten mit, dass der Geschäftsführer der Klägerin keine Frau wünsche. Nachdem der Vertrag zwischen den Parteien aufgrund von Differenzen beendet worden war und der Beklagte sein Honorar erhalten hatte, unterrichtete er die Bewerberin A mit E-Mail vom …. Oktober 2012 darüber, dass der Geschäftsführer der Klägerin keine Frau einstellen wolle; zugleich bezeichnete er das Verhalten als skandalös und als eine Diskriminierung im Sinne des Gleichbehandlungsgesetzes und riet der Bewerberin, sich an einen Rechtsanwalt unter Berücksichtigung der erforderlichen Fristen zu wenden, wenn sie wegen Schadensersatz dagegen vorgehen wolle. Zudem leitete er am …. Oktober 2012 die E-Mail des Personalleiters vom …. September 2012 an die Bewerberin weiter. Diese führte daraufhin ein arbeitsgerichtliches Verfahren gegen die Klägerin wegen Verstoßes gegen das AGG. In diesem Verfahren schloss die Klägerin mit der Bewerberin einen Vergleich über eine Entschädigung in Höhe von 8.500,-- €. Die Klägerin begehrt von dem Beklagten Ersatz dieses Betrags sowie der ihr entstandenen Anwaltskosten.

Das Landgericht hat die Klage abgewiesen. Eine Verschwiegenheitsverpflichtung sei vertraglich nicht ausdrücklich vereinbart worden. Die Werbeaussagen des Beklagten seien nicht Vertragsbestandteil geworden. Allerdings sei es dem Beklagten aufgrund einer sich aus dem Beratervertrag ergebenden Nebenpflicht auf Verschwiegenheit grundsätzlich verwehrt, vertrauliche Informationen weiterzugeben. Diese Treuepflicht gegenüber dem Vertragspartner finde aber ihre Grenze in den Geboten von Treu und Glauben. So sei eine Strafanzeige eines Arbeitnehmers gegen seinen Arbeitgeber grundsätzlich als berechtigt einzuordnen und stelle nur dann einen Verstoß gegen die aus dem Arbeitsverhältnis folgende Treuepflicht dar, wenn der Arbeitnehmer bei Erstattung der Anzeige wisse oder jedenfalls erkennen könne, dass der erhobene Vorwurf nicht zutreffe, oder wenn er unverhältnismäßigen Gebrauch von seinem Recht mache. Diese Grundsätze seien hier übertragbar. Ein Vertragspartner dürfe nicht darauf vertrauen, dass Verstöße gegen das AGG vertraulich behandelt würden. Dies gelte jedenfalls dann, wenn die Vorwürfe berechtigt seien. Im Fall eines Verstoßes gegen das AGG gebe es ein anerkennenswertes Interesse der Allgemeinheit. Dem Ziel des Gesetzes entsprechende effektive Schutzgewährung könne nur dann erfolgen, wenn ein sog. „whistleblowing" hinsichtlich der häufig geheim gehaltenen Diskriminierung nicht sanktionslos bleibe. Andernfalls würde das gesetzgeberisch unerwünschte Ziel die Folge sein, dass tatsächlich nicht der Diskriminierende die Entschädigungsleistung zu zahlen habe, sondern der Anzeigende.

Hinzu käme, dass der Klägerin an dem ihr entstandenen Schaden ein überwiegendes Mitverschulden vorzuwerfen sei, da sie mit ihrer E-Mail gegen das AGG verstoßen und damit die maßgebliche Ursache für ihre Vermögenseinbuße gesetzt habe.

Gegen dieses ihr am 29. August 2013 zugestellt Urteil hat die Klägerin Berufung eingelegt.

Sie vertritt die Auffassung, der Beklagte bewerbe mit seinen Werbeaussagen seine strikte Vertraulichkeit und erwecke damit den Eindruck, er verhalte sich im Hinblick auf die Vertraulichkeit wie jemand aus der in § 203 StGB genannten Personengruppe. Die Werbeaussagen des Beklagten, mit denen er strikte Diskretion zusage und eine „Vertrauensgarantie" gebe, seien im Sinne einer Verschwiegenheitsverpflichtung Vertragsbestandteil geworden. Darüber hinaus treffe den Beklagten zum Schutz des Vermögens des Vertragspartners eine umfassende Treuepflicht.

…

Aus den Gründen:

Die zulässige Berufung ist teilweise begründet.

Die Klägerin hat gegen den Beklagten einen Schadensersatzanspruch in Höhe von 3.684,97 € wegen Verletzung einer vertraglichen Verschwiegenheits- und Treuepflicht.

1. Das Landgericht geht zunächst zu Recht davon aus, dass die Parteien in ihrem Vertrag eine Verschwiegenheitspflicht des Beklagten nicht ausdrücklich vereinbart haben, sich aber eine Verschwiegenheitsverpflichtung grundsätzlich aus den Geboten von Treu und Glauben ergibt.

Ein Schuldverhältnis erschöpft sich grundsätzlich nicht in der Herbeiführung des geschuldeten Erfolgs; es ist vielmehr eine von Treu und Glauben beherrschte Sonderverbindung (Palandt/Grünberg, 73 A., § 241 BGB Rn. 6) und kann gemäß § 241 Abs. 1 BGB nach seinem Inhalt jeden Teil zur Rücksicht auf die Rechte, Rechtsgüter und Interessen des anderen Teils verpflichten. Vorliegend brachte es der zwischen den Parteien geschlossene Beratervertrag zwangsläufig mit sich, dass der Beklagte mit einer Vielzahl von Interna aus dem Geschäftsbetrieb der Klägerin in Berührung kommen würde, die nicht für Außenstehende bestimmt waren. Von daher liegt es auf der Hand, dass den Beklagten bereits aus der Natur des Vertrags heraus die Pflicht traf, über die ihm im Rahmen seiner Tätigkeit bekannt werdenden Verhältnisse, Vorgänge und Informationen Stillschweigen zu wahren. Zudem hat der Beklagte im Vorfeld des Vertragsschlusses mit seiner Diskretion geworben. So ist ausweislich seines Flyers (…) – fett gedruckt – strikte Diskretion selbstverständlich, wobei diese Aussage zwar in der Rubrik „Unternehmensverkäufe“ und nicht in der daneben abgedruckten Rubrik „Personalsuche“ aufgenommen ist, ein unbefangener Leser angesichts der Gestaltung des Flyers allerdings davon ausgehen kann und darf, dass diese Diskretionszusage allgemeine Geltung haben soll; zudem heißt es … unter einem ebenfalls fett gedruckten, hervorgehobenen Punkt „Vertrauensgarantie“: „Wir sagen (…) strikte Vertraulichkeit zu. (…) Informationen geben wir nur mit Ihrer Genehmigung weiter“. Unabhängig davon, ob diese Werbeaussagen unmittelbar Vertragsbestandteil geworden sind, hat der Beklagte mit ihnen zu erkennen gegeben, welchen Pflichten er sich unterworfen sieht, so dass sie zumindest zur Bestimmung der nach Treu und Glauben den Beklagten treffenden Nebenpflichten heranzuziehen sind. Von daher ist eine grundsätzlich umfassende Verschwiegenheitsverpflichtung anzunehmen. Diese wird ergänzt durch eine Treuepflicht dahingehend, die Rechtsgüter einschließlich des Vermögens des anderen Teils nicht zu verletzen.

2. Diese zwischen den Parteien als vertragliche Nebenpflicht bestehende Verschwiegenheits- und Treuepflicht hat der Beklagte verletzt, indem er der Bewerberin die Gründe für die Absage mitgeteilt und auf einen Verstoß gegen das AGG hingewiesen hat.

a) Dabei kann sich der Beklagte entgegen der Auffassung des Landgerichts nicht darauf berufen, zu der Weitergabe dieser Gründe berechtigt gewesen zu sein oder dabei in Wahrnehmung berechtigter Interessen gehandelt zu haben. Soweit das Landgericht eine Parallele zu den Fällen gezogen hat, in denen im Arbeitsrecht das Erstatten einer Strafanzeige eines Arbeitnehmers gegen seinen Arbeitgeber als zulässig erachtet wird, vermag der Senat dem nicht zu folgen. Dabei ist unerheblich, ob ein Arbeitsverhältnis mit seinen besonderen Rücksichtnahmepflichten mit einem Dienst- bzw. Maklervertrag der hier vorliegenden Art vergleichbar ist. Entscheidend ist, dass ein Arbeitnehmer – wie jede Person – mit der Erstattung einer Strafanzeige eine von Verfassungs wegen geforderte und von der Rechtsordnung erlaubte und gebilligte Möglichkeit der Rechtsverfolgung wahrnimmt (BVerfG, Beschluss vom 25.2.1987, 1 BvR 1086/85 = BVerfGE 74, 247; BAG, Urteil vom 3.7.2003, 2 AZR 235/02 = NJW 2004, 1547). Eine (nicht wissentlich unwahre oder leichtfertige) Strafanzeige liegt im allgemeinen Interesse an der Erhaltung des Rechtsfriedens und an der Aufklärung von Straftaten; darauf kann der Rechtsstaat bei der Strafverfolgung nicht verzichten (BVerfG, a.a.O.; BAG, a.a.O.). Dementsprechend kann sich ein Arbeitnehmer – oder auch ein sonstiger Vertragspartner – bei der Erstattung einer Strafanzeige auf ein ihm von der Rechtsordnung eingeräumtes Grundrecht nach Art. 2 Abs. 1 GG i.V.m. dem Rechtsstaatsprinzip nach Art. 20 Abs. 3 GG berufen (BAG, a.a.O.).

Hier hat der Beklagte allerdings keine Strafanzeige wegen einer möglichen Straftat der Klägerin erstattet, sondern der Betroffenen einen Verstoß der Klägerin gegen das AGG mitgeteilt. Diese Sachverhalte sind nicht vergleichbar. Ein Verstoß gegen das AGG stellt keine Straftat dar; er ist nicht einmal als gesetzliches Verbot im Sinne des § 134 BGB ausgestaltet, sondern führt lediglich zu einem zivilrechtlichen Entschädigungsanspruch des Betroffenen. Zwar ist es Ziel des AGG, Benachteiligungen u.a. aus Gründen des Geschlechts zu verhindern oder zu beseitigen; es greift damit für den Bereich der Privatautonomie den Gleichheitssatz des Art. 3 Abs. 3 GG auf, der in allen Staaten, die sich zu Demokratie und zu Menschenrechten bekennen, zu den grundlegenden verfassungsrechtlichen Wertentscheidungen gehören (Palandt/Ellenberger, a.a.O., Einl v AGG Rn. 7). Dennoch war es eine bewusste Entscheidung des Gesetzgebers, an einen Verstoß gegen das AGG keine straf- oder ordnungsrechtlichen Sanktionen zu knüpfen, für deren Verfolgung der Staat verantwortlich zeichnet, sondern allein einen zivilrechtlichen Entschädigungsanspruch. Geht es allein um einen solchen zivilrechtlichen Sachverhalt, kann sich der Beklagte nicht darauf berufen, im Interesse der Allgemeinheit gehandelt zu haben.

Etwas anderes folgt nach Auffassung des Senats auch nicht aus der von beiden Parteien in Bezug genommenen sog. „Heinisch“-Entscheidung des EGMR (Urteil vom 21.7. 2011, 28274/08, zitiert nach juris). Der EGMR hat für die Anwendung des Art. 10 der Konvention (= Recht auf freie Meinungsäußerung) auf das Arbeitsleben festgestellt, dass Hinweise auf strafbares oder rechtswidriges Verhalten am Arbeitsplatz durch Beschäftigte unter gewissen Umständen Schutz genießen sollen und insoweit eine Abwägung zwischen dem Recht des Arbeitnehmers auf freie Meinungsäußerung in Form von Hinweisen auf strafbares oder rechtswidriges Verhalten seitens des Arbeitgebers und dem Recht des Arbeitgebers auf Schutz seines guten Rufs und seiner wirtschaftlichen Interessen vorzunehmen ist. Der Beklagte hat aber nicht ein Recht auf freie Meinungsäußerung in Anspruch genommen, um einen Missstand in die Öffentlichkeit zu bringen, sondern entgegen seiner vertraglichen Verschwiegenheitspflicht einer von einem Verstoß gegen das AGG Betroffenen dazu verholfen, eine zivilrechtliche Entschädigung geltend machen zu können.

Ohne Erfolg beruft sich der Beklagte ergänzend auf Schutzpflichten gegenüber der Bewerberin, die einen Anspruch darauf gehabt habe zu erfahren, warum sie nicht ausgewählt worden sei. Zum einen war der Beklagte vertraglich mit der Klägerin und nicht mit der Bewerberin verbunden, so dass er in erster Linie die Interessen der Klägerin zu wahren hatte, für die er tätig wurde. Zum anderen besteht nach der Rechtsprechung des BAG grundsätzlich kein Anspruch eines Bewerbers auf Auskunft über die Gründe einer Absage bzw. über eine von einem Unternehmen getroffene Personalentscheidung (BAG, Urteil vom 25.4.2012, 8 AZR 287/08, zitiert nach juris). Dies muss dann aber auch für einen Personalvermittler oder -berater gelten, der bei der Personalsuche für die Klägerin tätig

wird. Er darf dann nicht ohne Rücksprache und Einverständnis des Unternehmens von sich aus die Gründe für die Absage mitteilen.

b) Unabhängig von den vorstehenden Erwägungen verdient das Verhalten des Beklagten aber auch deshalb keinen Schutz, weil es rechtsmissbräuchlich war.

…

Nach alledem hat der Beklagte seiner Verschwiegenheits- und Treuepflicht verletzt, wobei sein Verschulden vermutet wird, § 280 Abs. 1 S. 2 BGB.

3. Durch die Pflichtverletzung des Beklagten ist der Klägerin ein Schaden in Höhe von 11.054,90 € entstanden, den der Beklagte in Anrechnung des Mitverschuldens (§ 254 Abs. 1 BGB) der Klägerin zu 1/3 zu ersetzen hat. …

Insoweit ist zu berücksichtigen, dass der Schaden zwar dadurch eingetreten ist, weil der Beklagte gegen seine Verschwiegenheits- und Treuepflicht verstoßen und damit die Inanspruchnahme der Klägerin veranlasst hat; die Klägerin hat aber die wesentliche Ursache für den ihr entstandenen Schaden gesetzt, indem sie es war, die den Verstoß gegen das AGG begangen hat. Nach den Grundsätzen von Treu und Glauben, die dem § 254 BGB zugrunde liegen (Palandt/Grüneberg, a.a.O., § 254 BGB Rn. 1), kann die Klägerin deshalb nicht vollen Ersatz des erlittenen Schadens verlangen; vielmehr ist es gerechtfertigt, die Klägerin überwiegend haften zu lassen. Auf der anderen Seite war der Beitrag des Beklagten für den Eintritt des Schadens bei der Klägerin nicht so gering, dass er vollständig zurücktreten würde. Der Senat erachtet deshalb eine Haftungsquote von 1/3 zu 2/3 zu Lasten der Klägerin als angemessen.

Verstoß gegen § 28 Abs. 3 BDSG wegen Datenverwendung zur Mandantenakquise

(**Oberlandesgericht Köln**, Urteil vom 17. Januar 2014 – 6 U 167/13 –)

1. **§ 28 Abs. 3 BDSG stellt eine Marktverhaltensregelung im Sinne von § 4 Nr. 11 UWG dar. Wenn sich ein Marktteilnehmer auf einen BDSG-Erlaubnistatbestand beruft, um Werbung für sich zu machen, bezwecken die Grenzen, die das BDSG einem solchen Marktverhalten setzt, den Schutz des Betroffenen in seiner Stellung als Marktteilnehmer.**
2. **Kontaktdaten von Anlegern, die ein Rechtsanwalt im Namen eines Mandanten infolge eines Auskunftsersuchens von einer Fondgesellschaft erhält, dürfen aufgrund der Zweckgebundenheit nicht verwendet werden, um sich mit einem Werbeschreiben an Anleger des Fonds zu werden.**
3. **Der Begriff der Werbung in § 28 Abs. 3 BDSG ist weit und umfassend zu verstehen; auch eine indirekte und unbewusste Ansprache ist darunter zu fassen.**
4. **Ein Werbeverbot nach § 43b BRAO kommt nicht in Betracht, wenn ein potentieller Mandant in Kenntnis von dessen konkreten Beratungsbedarf angesprochen wird, d.h. ein Schreiben an Anleger eines Fonds sich allein mit der sachlichen Information über den Zustand des Fonds befasst.**

(Nicht amtliche Leitsätze)

Sachverhalt:

Die Parteien sind Rechtsanwälte. Die Antragsgegner versandten im Mai 2013 namens eines Anlegers in einem geschlossenen Immobilienfonds ein Rundschreiben an die Anleger dieses Fonds, in dem sie auf die kritische Lage des Fonds hinwiesen und für den Beitritt zu einer „Schutzgemeinschaft" der Anleger warben. In dem Anschreiben wurde auf den Internetauftritt der Schutzgemeinschaft verwiesen, für den die Antragsgegner verantwortlich zeichnen und auf dem umfangreich die Tätigkeit der Antragsgegner unter Hinweis auf ihre Spezialisierung für Bank- und Kapitalmarktrecht dargestellt wird. Die Kontaktdaten der Anleger hatten die Antragsgegner erlangt, indem sie namens eines Anlegers die Fondsgesellschaft auf Auskunft in Anspruch genommen hatten.

Der Antragsteller beanstandet die Verwendung der Kontaktdaten der Anleger, da diese datenschutzrechtlich unzulässig sei, sowie das Anschreiben an sich als eine nach § 43b BRAO unzulässige Werbemaßnahme. Das Landgericht hat mit einstweiliger Verfügung vom 10. Juni 2013 den Antragsgegnern untersagt,

a) im geschäftlichen Verkehr zum Zwecke des Wettbewerbs personenbezogene Daten von Gesellschaftern und Treugebern der J. Fonds GmbH & Co. KG für eigene Werbezwecke mit dem Ziel der Mandatsgewinnung zu nutzen, wenn diese Daten im Rahmen eines Mandatsverhältnisses zu einem Gesellschafter dieser Kommanditgesellschaft ausschließlich zur Kontaktaufnahme zum Zwecke des Informationsaustausches zwischen den Gesellschaftern übermittelt wurden;

b) im geschäftlichen Verkehr zum Zwecke des Wettbewerbs Personen, die eine Beteiligung an der J. Fonds GmbH & Co. KG halten und die nicht in einem Mandatsverhältnis zu den Antragsgegnern stehen, unaufgefordert Anschreiben zu übersenden, in welchem um die Erteilung eines Mandats im Zusammenhang mit dieser Gesellschaft geworden wird, wenn diese Werbung erfolgt wie nachstehend wiedergegeben: [es folgt die Wiedergabe des Anschreibens wie Seite 3-6 LGU sowie des Internetauftritts der Schutzgemeinschaft wie Seite 8-17 LGU].

Auf den Widerspruch der Antragsgegner hat das Landgericht mit dem angefochtenen Urteil die einstweilige Verfügung bestätigt.

Aus den Gründen:

Die zulässige Berufung hat teilweise Erfolg.

…

b) Dem Antragsteller steht gegen die Antragsgegner ein auf §§ 3, 4 Nr. 11, 8 Abs. 1 und Abs. 3 Nr. 1 UWG i.V.m. §§ 4 Abs. 1, 28 Abs. 3 BDSG gestützter Unterlassungsanspruch wegen der Verwendung der von den Antragsgegnern erlangten Kontaktdaten der Anleger zu.

aa) § 28 Abs. 3 BDSG stellt eine Marktverhaltensregelung im Sinn des § 4 Nr. 11 UWG dar. Die Regelungen des BDSG bezwecken zwar in erster Linie den Schutz des Persönlichkeitsrechts, nämlich des Rechts auf informationelle Selbstbestimmung des Einzelnen vor Zugriffen Dritter und stellen nicht schon aus diesem Grund Marktverhaltensregelungen zum Schutze der Verbraucher dar. Soweit sich jedoch ein Marktteilnehmer auf einen Erlaubnistatbestand beruft, um diese Erlaubnis dazu zu nutzen, Werbung für sich zu machen, bezwecken die Grenzen, die das BDSG einem solchen Marktverhalten setzt, den Schutz des Betroffenen in seiner Stellung als Marktteilnehmer. Dieser Schutz ist zwar Ausfluss des allgemeinen Schutzes eines Rechts des Verbrauchers, nämlich seines Rechts auf informationelle Selbstbestimmung. Auch eine dem Schutz von Rechten oder Rechtsgütern dienende Vorschrift ist aber dann eine Marktverhaltensvorschrift, wenn das geschützte Interesse gerade durch die Marktteilnahme berührt wird. § 28 Abs. 3 BDSG ist daher als Marktverhaltensregelung zu qualifizieren (Senat, GRUR-RR 2010, 34 – Rückgewinnungsschreiben; OLG Karlsruhe, GRUR-RR 2012, 396, 398f. – Neuer Versorger; Köhler, in: Köhler/Bornkamm, UWG, 32. Aufl. 2014, § 4 Rn. 11.42; offen Plath/Plath, BDSG, 2013, § 1 Rn. 16).

Der gegenteiligen Auffassung des OLG München (GRUR-RR 2012, 395, 396 – Personenbezogene Daten), die eine generelle Betrachtung des Schutzzwecks des BDSG in den Vordergrund stellt, folgt der Senat nicht. Sie wird auch nicht durch die dort zitierte Entscheidung „Kraftfahrzeuganhänger mit Werbeschildern" (BGH, GRUR 2006, 872 Tz. 16ff.) gestützt: Die vom Bundesgerichtshof zu beurteilende Vorschrift diente allein der Sicherheit und Leichtigkeit des Straßenverkehrs, nicht aber dem Schutz der Mitbewerber oder der Verbraucher. §§ 4 Abs. 1, 28 Abs. 3 BDSG regeln dagegen die Nutzung personenbezogener Daten für Werbezwecke und dienen damit jedenfalls auch dem Schutz von Rechtsgütern der Kunden im Zusammenhang mit ihrer Marktteilnahme (OLG Karlsruhe a.a.O.S. 399). Die Regelungen der §§ 4 Abs. 1, 28 Abs. 3 BDSG haben auch eine unionsrechtliche Grundlage in Gestalt der Datenschutzrichtlinie 95/46/EG, die von der UGP-Richtlinie nicht berührt wird, so dass diese einem auf §§ 4 Abs. 1, 28 Abs. 3 BDSG gestützten Verbot nicht entgegensteht (OLG Karlsruhe a. a. O.).

bb) Die Verwendung der Kontaktdaten der Anleger, um sich mit dem Schreiben vom Mai 2013 an sie zu wenden, war datenschutzrechtlich unzulässig. Nach § 28 Abs. 3 S. 1 BDSG ist die Verwendung von personenbezogenen Daten für Werbung grundsätzlich nur bei Einwilligung des Betroffenen zulässig; die weiteren Ausnahmen des § 28 Abs. 3 S. 2 BDSG liegen nicht vor. Insbesondere greift § 28 Abs. 3 S. 2 Nr. 1 BDSG nicht ein. Nach dieser Bestimmung kann zwar die Verwendung von Daten zulässig sein, soweit sie der Verwender im Rahmen eines Schuldverhältnisses zulässigerweise nach § 28 Abs. 1 S. 1 Nr. 1 BDSG erhoben hat. Damit ist aber ein Schuldverhältnis mit dem Betroffenen gemeint, so dass der vorliegende Fall – bei denen die Antragsgegner die Daten unbeteiligter Dritter im Rahmen der Mandatsausübung erlangt haben – nicht erfasst ist. Auch Daten, die zur Begründung eines Schuldverhältnisses erforderlich sind, müssen bei dem Betroffenen, mit dem das Schuldverhältnis begründet werden soll, erhoben werden. Andernfalls liefe § 28 Abs. 3 BDSG mit seinen strengeren Anforderungen an die Nutzung der Daten für Werbezwecke (die regelmäßig auf die Begründung eines Schuldverhältnisses abzielen) weitgehend leer.

§ 28 Abs. 3 BDSG ist eine abschließende Spezialregelung für die Nutzung personenbezogener Daten für die Werbung, so dass ein Rückgriff auf andere Erlaubnistatbestände nicht möglich ist (Gola/Schomerus, BDSG, 11. Aufl. 2012, § 28 Rn. 42; Plath/Plath, BDSG, 2013, § 28 Rn. 100; Wolff/Brink, Datenschutzrecht, 2013, § 28 BDSG Rn. 112). Der Begriff der Werbung in § 28 Abs. 3 BDSG ist weit und umfassend zu verstehen; auch die indirekte und unbewusste Ansprache ist darunter zu fassen (Bergmann/Möhrle/Herb, Datenschutzrecht, Stand: Januar 2012, § 28 Rn. 322). Das Schreiben vom Mai 2013 dient zwar auch der Information der Anleger und enthält Vorschläge für das Stimmverhalten in der bevorstehenden Gesellschafterversammlung. Ob ein Schreiben allein diesen Inhalts als „Werbung" zu im Sinn des Bundesdatenschutzgesetzes zu qualifizieren wäre, kann offen bleiben. Jedenfalls der letzte Teil des Schreibens (Seite 3, ab: „Die Einschätzung von auf Kapitalanlagen spezialisierten Rechtsanwälten ist folgende") dient ersichtlich der Mandatsgewinnung der Antragsgegner. Auch der vorbereitete Antwortschein mit den Rubriken „Möchten Sie von der Schutzgemeinschaft beraten/vertreten werden?" weist in diese Richtung. Besonders deutlich wird dies schließlich auch durch den Verweis auf die Internetseite der Schutzgemeinschaft, von der die Antragsgegner selber einräumen, dass es sich bei ihr um eine („anwaltsübliche") Werbemaßnahme der Antragsgegner handelt. Im Übrigen haben die Antragsgegner das Schreiben selber als „Werbeschreiben" bezeichnet. Damit war die Verwendung der Daten der Anleger für das Schreiben jedenfalls in der Form, in der es versandt worden ist, und wie es nunmehr allein Gegenstand des Unterlassungsantrags ist, unzulässig. Soweit die Antragsgegner mit dem Schreiben Werbung in eigener Sache betreiben, ist es unerheblich, dass das Schreiben nicht im eigenen Namen, sondern in Vertretung eines Dritten verfasst worden ist.

Eine Interessenabwägung, ob die Form der Kontaktaufnahme im überwiegenden Interesse der Anleger war, sieht § 28 Abs. 3 BDSG nicht vor; eine solche Abwägung ist nur im Rahmen der – wegen des Vorrangs des Abs. 3 nicht einschlägigen – Absätze 1 und 6 vorgesehen. Im Rahmen des Abs. 3 sieht S. 6 hingegen eine Interessenabwägung nur als zusätzliche Voraussetzung vor. Die Zulässigkeit der Verwendung der Daten folgt auch nicht aus § 28 Abs. 6 Nr. 3 BDSG, unabhängig vom Vorrang des § 28 Abs. 3 BDSG. Die Verwendung der Daten zur Werbung – Mandantenakquise – ist nicht zur Durchführung des Mandatsverhältnisses mit dem bisherigen Auftraggeber „erforderlich".

cc) Die Antragsgegner haben zwar bestritten, dass sie die Daten ausschließlich zur Kontaktaufnahme der Anleger untereinander erhalten haben. Auf diese Frage kommt es an sich für die Anwendung des § 28 Abs. 3 BDSG nicht an, da der Tatbestand allein durch die Verwendung der Daten erfüllt worden ist. Selbst wenn die Antragsgegner die Daten seitens der Fondsgesellschaft ausdrücklich zum Zweck der Mandantenakquise erhalten haben sollten, wäre ihre Verwendung ohne die Zustimmung der Betroffenen immer noch unzulässig. Die Frage, zu welchem Zweck die Antragsgegner die Daten erhalten haben, ist allerdings relevant im Hinblick auf die Fassung des Antrags, mit dem der Antragsteller die Nutzung der Daten ausdrücklich unter der Voraussetzung, „wenn diese Daten im Rahmen eines Mandatsverhältnisses zu einem Gesellschafter dieser Kommanditgesellschaft ausschließlich zur Kontaktaufnahme zum Zwecke des Informationsaustausches zwischen den Gesellschaftern übermittelt wurden", untersagt wissen möchte.

Diese vom Antragsteller gewählte Fassung ist nicht zu weitgehend, da in dem Fall, dass die Antragsgegner die Kontaktdaten erst zum Zweck der Kontaktaufnahme der Anleger untereinander erhalten haben, eine Einwilligung der betroffenen Anleger noch nicht vorliegen kann. Auch die Voraussetzungen der Ausnahmen des § 28 Abs. 3 S. 2 BDSG liegen dann nicht vor, da die Daten dann nicht aus einer öffentlich zugänglichen Quelle (oder einem früheren Mandatsverhältnis der Antragsgegner mit den Betroffenen) stammen können.

Demgegenüber durften sich die Antragsgegner nicht darauf beschränken, zu bestreiten, dass sie die Daten ausschließlich zur Kontaktaufnahme der Anleger untereinander erhalten haben. Sie haben selber vorgetragen, dass sie die Herausgabe der Daten in einem gerichtlichen Verfahren zu Gunsten eines Anlegers erstritten haben. Nach dem Inhalt des Auskunftsanspruchs, den die Antragsgegner hier für einen der betroffenen Anleger geltend gemacht haben, dürfen die so erlangten Daten allein für bestimmte Zwecke benutzt werden. Der Bundesgerichtshof hat dazu ausgeführt:

„Der Senat verkennt hierbei nicht, dass anwaltliche Vertreter von Anlegern die aus Auskunftsverfahren der vorliegenden Art gewonnenen Erkenntnisse zur Kontaktaufnahme mit bislang unbekannten Anlegern nutzen können. Allein dadurch wird jedoch nicht die konkrete Gefahr eines Datenmissbrauchs begründet. Erfolgt die Kontaktaufnahme etwa im Auftrag des obsiegenden Auskunftsklägers, scheidet ein Missbrauch bereits dann aus, wenn ein Kläger den Kontakt deshalb sucht, um sich mit den anderen Anlegern über aus seiner Sicht hinsichtlich der Gesellschaft bestehende Probleme auszutauschen. Ebenso wenig ist es bedenklich, wenn ein Klägeranwalt im Auftrag seines Mandanten durch die Kontaktaufnahme mit anderen Anlegern z.B. versucht, eine Interessengemeinschaft unter den Anlegern zu organisieren. Nutzt der Anwalt eines (erfolgreich) auf Auskunft klagenden Anlegers dagegen die Daten eigenmächtig, d.h. ohne eine dahingehende Beauftragung durch den Anleger im

Rahmen der Verfolgung von dessen Interessen, zur Werbung um konkrete Mandate, liegt darin zwar ein Missbrauch der Daten. ... In diesem Fall [sind] berufsrechtliche (durch Einschaltung der Aufsicht der Rechtsanwaltskammern), wettbewerbsrechtliche (vgl. hierzu OLG München, GRUR-RR 2012, 163; OLG Köln, BeckRS 2013, 01363; allgemein Köhler/Bornkamm, UWG, 31. Aufl., § 4 Rn. 11.96; siehe auch AG Weilheim, NJW 2013, 243) und datenschutzrechtliche (siehe hierzu Paul, GWR 2011, 225, 230) Rechtsbehelfe gegeben, um gegen ein derartiges missbräuchliches Verhalten eines Anwalts vorzugehen" (BGH, WM 2013, 603, zit. nach juris Tz. 40).

Dies ist aus Sicht des Senats dahingehend zu verstehen, dass die Verwendung der so erlangten Daten „zur Werbung um konkrete Mandate" Dritter per se unzulässig ist. Sprachlich wäre zwar auch das Verständnis möglich, dass die Nutzung zu Werbezwecken für weitere Mandate auch dann möglich sein soll, wenn es „im Auftrag" des klagenden Anlegers erfolgt. Ein solches Verständnis erscheint jedoch inhaltlich wenig sinnvoll: Für die Interessen des Auftraggebers ist es unerheblich, ob seine Anwälte noch weitere Mandate erhalten. Dass ein Mandant seine Anwälte ausdrücklich beauftragt, noch weitere Mandanten zu akquirieren, ist fernliegend.

Allein aufgrund des Umstandes, dass die Antragsgegner die Daten aufgrund eines gerichtlich durchgesetzten Auskunftsanspruchs gegen die Fondsgesellschaft erlangt haben, steht daher fest, dass sie diese Daten allein zur Kontaktaufnahme mit anderen Anlegern (beispielsweise, um eine Interessengemeinschaft zu organisieren) nutzen durften, nicht aber, um daneben auch für eigene Mandate zu werben. Die Abgrenzung zwischen legitimer Kontaktaufnahme mit anderen Anlegern, bei der sich gewisse Werbeeffekte zugunsten der betreffenden Rechtsanwälte kaum vermeiden lassen werden, und darüber hinausgehender unzulässiger Werbung mag im Einzelfall schwierig sein. Erforderlich ist es, dass in einem solchen Fall die Werbeeffekte auf das Minimum reduziert werden. Hinweise, wie im vorliegenden Fall, auf die Erfolgsaussichten von Schadensersatzklagen wegen etwaiger Prospektfehler, die allein im Interesse des individuellen Anlegers liegen, stellen jedenfalls eine – im Rahmen der Prüfung der §§ 4 Abs. 1, 28 Abs. 3 BDSG – unzulässige Werbemaßnahme dar.

dd) Soweit die Antragsgegner beanstanden, der Verbotstenor sei zu weit gefasst, da er ihnen auch die (weitere) Nutzung der Daten derjenigen Anleger untersage, die ihnen inzwischen Mandate erteilt hätten, wird diesem Bedenken durch die Formulierung „mit dem Ziel der Mandatsgewinnung" Rechnung getragen. Ist das Mandatsverhältnis einmal begründet, dürfen die Daten auch weiter genutzt werden.

2. Hinsichtlich des Antrags zu 1 b) hat die Berufung der Antragsgegner dagegen Erfolg. Ein Anspruch des Antragstellers aus §§ 3, 4 Nr. 11, 8 Abs. 1 und 3 UWG i.V.m. § 43b BRAO besteht nicht.

Der Senat hat zu den Voraussetzungen des § 43b BRAO in einem Urteil vom 15.6.2012 (6 U 129/11, BRAK-Mitt. 2012, 281 = BeckRS 2013, 01363) ausgeführt:

„Die Regelung des § 43b BRAO, wonach Rechtsanwälte nur sachlich über ihre berufliche Tätigkeit unterrichten und nicht um einzelne Mandate werben dürfen, begegnet für sich genommen keinen verfassungsrechtlichen Bedenken (vgl. BVerfG, GRUR 2008, 618 = WRP 2008, 492 [Rn. 11] – Anwaltsdienste bei ebay), ist im Licht der durch Art. 12 GG garantierten Werbefreiheit allerdings dahin auszulegen, dass jede Einschränkung durch ausreichende Gründe des Gemeinwohls gerechtfertigt und verhältnismäßig sein muss (vgl. BVerfG, GRUR 2003, 965 f. = WRP 2003, 1213; BGHZ 147, 71 = GRUR 2002, 84 = WRP 2001, 923 – Anwaltswerbung II; BGH, GRUR 2005, 520 [521] = WRP 2005, 738 – Optimale Interessenvertretung; KG, GRUR-RR 2010, 437 [438 f.]; OLG München, GRUR-RR 2012, 163 [164]). Auch nach Art. 24 Abs. 2 der Richtlinie 2006/123/EG über Dienstleistungen im Binnenmarkt müssen berufsrechtliche Regeln über die kommerzielle Kommunikation, die Unabhängigkeit, Würde und Integrität des Berufsstandes sowie die Wahrung des Berufsgeheimnisses gewährleisten sollen, durch einen zwingenden Grund des Allgemeininteresses gerechtfertigt und verhältnismäßig sein (vgl. Köhler/Bornkamm, a. a. O., § 4 Rn. 11.85). Bleibt es mithin regelmäßig dem Anwalt überlassen, wie er sich vor der interessierten Öffentlichkeit darstellt, so darf sein Werbeverhalten doch nicht durch aufdringlich wirkendes Ausnutzen eines konkreten Beratungsbedarfs das Vertrauen der Rechtssuchenden in die vor allem sein Interesse wahrende anwaltliche Tätigkeit untergraben und die Wahlfreiheit der Umworbenen gefährden, die sich in der aktuellen Situation möglicherweise nicht mehr unvoreingenommen für einen anwaltlichen Berater oder Vertreter entscheiden können und durch die Art der Werbung bedrängt, genötigt oder überrumpelt zu werden drohen (vgl. BVerfG, GRUR 2008, 618 = WRP 2008, 492 [Rn. 22] – Anwaltsdienste bei ebay; BGHZ 147, 71 = GRUR 2002, 84 [86] = WRP 2001, 923 – Anwaltswerbung II; OLG Hamburg, NJW 2005, 2783 [2785]; OLG Jena, GRUR 2006, 606 [607]; OLG Naumburg, WRP 2007, 1502 f.; KG, GRUR-RR 2010, 437 [439]; OLG München, GRUR-RR 2012, 163 [164]). Bei unaufgeforderten, nicht vom Rechtssuchenden selbst erbetenen Schreiben an geschädigte Kapitalanleger hängt es von einer umfassenden Würdigung der Umstände des Einzelfalles ab, ob eine lauterkeitsrechtlich unbedenkliche Publikumswerbung oder eine unzulässige gezielte Einflussnahme vorliegt" (a. a. O., zit. nach juris Tz. 11).

An dieser Rechtsprechung hält der Senat fest. Sie steht auch grundsätzlich in Einklang mit der neuesten Rechtsprechung des Bundesgerichtshofs. Danach ist § 43b BRAO im Licht des Art. 24 der Richtlinie 2006/123/EG über Dienstleistungen im Binnenmarkt dahingehend auszulegen, dass ein Werbeverbot nur in Betracht kommt, wenn sich ein Verbotsgrund im Einzelfall aus der Form, aus dem Inhalt oder aus dem verwendeten Mittel der Werbung ergibt. Allein der Umstand, dass ein potenzieller Mandant in Kenntnis von dessen konkretem Beratungsbedarf angesprochen wird, genügt nicht, um die Unzulässigkeit der Werbung zu begründen. Zwar gilt weiterhin, dass ein Werbeverbot zum Schutz des potenziellen Mandanten vor einer Beeinträchtigung seiner Entscheidungsfreiheit durch Belästigung, Nötigung und Überrumpelung gerechtfertigt sein kann. Aus der gesetzlichen Anordnung einer Verhältnismäßigkeitsprüfung folgt ferner, dass eine Interessenabwägung im Einzelfall vorzunehmen ist, bei der neben der Beeinträchtigung der Unabhängigkeit, der Würde oder der Integrität der Rechtsanwaltschaft auch Art und Grad der Beeinträchtigung der Entscheidungsfreiheit des Verbrauchers durch Form, Inhalt oder das verwendete Mittel der Werbung zu berücksichtigen sind. Außerdem ist zu berücksichtigen, ob der Verbraucher sich in einer Situation befindet, in der er auf Rechtsrat angewiesen ist und ihm eine an seinem Bedarf ausgerichtete sachliche Werbung Nutzen bringen kann (BGH, GRUR 2014, 86 Tz. 18, 21 – Kommanditistenbrief).

Im vorliegenden Fall kommen als Begründung für die Unzulässigkeit des Anschreibens als Werbemaßnahme in erster Linie zwei Umstände in Betracht:

– Auch nach der zitierten Rechtsprechung des Bundesgerichtshofs kann eine werbliche Ansprache in einer Situation, in der die Gefahr des Verlustes erheblicher Vermögenswerte derart unmittelbar droht, dass eine überlegte und informationsgeleitete Entscheidung für oder gegen das Angebot des Rechtsanwalts erheblich erschwert wird, unzulässig sein (BGH a.a.O.Tz. 23).

– In der zitierten Entscheidung des Senats stand im Vordergrund, dass dort der Anschein erweckt worden war, das Anschreiben erfolge im Namen einer als Idealverein organisierten Verbrau-

cherschutzorganisation und verfolge in erster Linie den Zweck, einer massenhaften Petition an den Deutschen Bundestag zum Erfolg zu verhelfen. Für die Adressaten des Schreibens war dabei nicht erkennbar, dass tatsächlich hinter dem Schreiben Rechtsanwälte standen, die das Ziel verfolgten, weitere namentlich bekannte Anleger zur Erteilung eines konkreten Mandats zu veranlassen (Senat, a. a. O., zitiert nach juris Tz. 12).

Auch im vorliegenden Fall wird zwar durchaus der Eindruck konkreten Handlungsbedarfs geweckt, auf den das Landgericht in erster Linie abgestellt hat. Soweit das Landgericht dabei aber als entscheidend herausgestellt hat, dass durch die Formulierungen in dem Schreiben auf konkreten Beratungsbedarf der Anleger hingewiesen werde, so ist allerdings nach der zitierten – erst nach dem Urteil des Landgerichts veröffentlichten – Entscheidung des Bundesgerichtshofs allein der Umstand, dass ein potenzieller Mandant in Kenntnis von dessen konkretem Beratungsbedarf angesprochen wird, nicht geeignet, einen Verstoß gegen § 43b BRAO zu begründen (a.a.O. Tz. 18). Daher ist auch das Urteil des OLG Hamburg (NJW 2005, 2783), auf das sich der Antragsteller unter anderem berufen hat, insoweit überholt, als dort das Bestehen eines konkreten Beratungsbedarfs bei den angesprochenen Verbrauchern als zentrales Kriterium für die Unzulässigkeit der Werbung herausgestellt wird (a.a.O. S. 2785).

Besondere Eilbedürftigkeit wird im vorliegenden Fall in erster Linie durch die Formulierung in dem Antragsformular „Bitte schnellstmöglich zurück an [die Antragsgegner]“ suggeriert. Im laufenden Text des Anschreibens wird zwar auch auf gerichtliche Eilverfahren Bezug genommen, es werden jedoch zugleich Entscheidungen in Hauptsacheverfahren aus dem Jahr 2012 (das Schreiben wurde im Mai 2013 versandt) genannt. Der überwiegende Teil des Schreibens befasst sich mit einer bevorstehenden Gesellschafterversammlung der Fondsgesellschaft und den dort zu treffenden Maßnahmen. Eine besondere Drucksituation könnte allenfalls dann angenommen werden, wenn diese Gesellschafterversammlung unmittelbar bevorgestanden hätte. Dies lässt sich jedoch dem Schreiben nicht entnehmen und wird von den Parteien auch nicht vorgetragen.

Der Bundesgerichtshof hat in der zitierten Entscheidung ein Urteil des OLG München (GRUR-RR 2012, 163) aufgehoben, auf das sich sowohl der Antragsteller wie auch das Landgericht bezogen haben. Das OLG München hatte es für unzulässig gehalten, dass sich ein Rechtsanwalt an Kommanditisten eines Fonds wandte, die sich mit Ansprüchen des Insolvenzverwalters über das Vermögen der Fondsgesellschaft konfrontiert sahen. Teilweise waren dort Kommanditisten bereits gerichtlich in Anspruch genommen worden. Dennoch hat der Bundesgerichtshof darin keine Situation gesehen, in der die Gefahr des Verlustes erheblicher Vermögenswerte derart unmittelbar drohte, dass eine überlegte und informationsgeleitete Entscheidung für oder gegen das Angebot des Rechtsanwalts erheblich erschwert worden wäre (BGH a.a.O. Tz. 23). Aus Sicht des Anlegers stellt sich eine Situation, in der andere Anleger bereits gerichtlich in Anspruch genommen werden und er daher selber mit einer entsprechenden Inanspruchnahme rechnen muss, als zumindest ebenso gravierend dar wie die in dem Schreiben der Antragsgegner im vorliegenden Fall dargestellte kritische Situation des Fonds.

Eine Irreführung über den tatsächlichen Hintergrund des Schreibens ist nicht anzunehmen. Das Schreiben ist zwar im Namen eines Mitglieds der Schutzgemeinschaft verfasst. Anders als in dem Sachverhalt, der der zitierten Entscheidung des Senats zu Grunde lag, ist für den Adressaten des Schreibens jedoch offensichtlich, dass die Antragsgegner maßgeblichen Einfluss auf die Schutzgemeinschaft haben. Das Schreiben ist auf dem Briefkopf der Antragsgegner verfasst worden, unter ihrer Anschrift versandt worden und auch von einem der Antragsgegner unterschrieben worden. Die Rückantwort wird ausdrücklich an die Antragsgegner erbeten. Auch der Internetauftritt der Schutzgemeinschaft lässt keinen Zweifel daran, dass die Antragsgegner maßgeblichen Einfluss in ihr ausüben. Eine Verschleierung der tatsächlichen Verhältnisse erfolgt in diesem Schreiben daher nicht.

Demgegenüber kann nicht unberücksichtigt bleiben, dass mit dem Schreiben zwar auch dafür geworben wird, die Antragsgegner zur Durchsetzung von Ansprüchen des angesprochenen Anlegers zu mandatieren. Der überwiegende Teil des Schreibens befasst sich jedoch mit einer Information über die Lage des Fonds sowie den auf der anstehenden Gesellschafterversammlung zu treffenden Beschlüssen. Insoweit stellt das Schreiben daher nicht nur Werbung der Antragsgegner, sondern auch eine sachgerechte Maßnahme der Kommunikation der Anleger untereinander dar, um die Durchsetzung bestimmter Maßnahmen auf der Gesellschafterversammlung zu ermöglichen. Die Werbemaßnahme ist daher durchaus auch von Nutzen für die angesprochenen Anleger. Ein damit verbundener Werbeeffekt zugunsten der Antragsgegner ist – im Rahmen des § 43b BRAO, anders als bei der Prüfung der §§ 4 Abs. 1, 28 Abs. 3 BDSG – hinzunehmen.

Insgesamt führt die Abwägung der vorstehenden Umstände daher zu dem Ergebnis, dass das beanstandete Schreiben nicht als eine nach § 43b BRAO unzulässige Werbemaßnahme angesehen werden kann.

Kündigung wegen Veröffentlichung von Patientenfoto in sozialen Netzwerken (Ls)

(**Landesarbeitsgericht Berlin-Brandenburg**, Urteil vom 11. April 2014 – 17 Sa 2200/13 –)

Eine private Veröffentlichung eines Säuglingspatienten eines Krankenhauses durch eine Pflegerin in einem sozialen Netzwerk stellt in der Regel einen wichtigen Grund für eine fristlose Kündigung dar. Aufgrund besonderer Umstände kann ein solches Verhalten aber auch nur eine ordentliche Kündigung oder eine Abmahnung rechtfertigen.

(Nicht amtlicher Leitsatz)

Abmahnung bei krankheitsbedingter Kündigung (Ls)

(**Landesarbeitsgericht Hessen**, Urteil vom 18. März 2014 – 13 Sa 1207/13 –)

Vor dem Ausspruch einer krankheitsbedingten Kündigung kann eine Abmahnung geboten sein, wenn die Erkrankung durch ein steuerbares Verhalten beseitigt werden kann; hier: Wideraufnahme der unterbrochenen Medikation mit Psychopharmaka.

(Nicht amtlicher Leitsatz)

Berichte, Informationen, Sonstiges

Modelle zur Vergabe von Prüfzertifikaten, die im Wege der Selbstregulierung entwickelt und durchgeführt werden

Beschluss der Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich (Düsseldorfer Kreis am 25./26. Februar 2014)

I. Ausgangslage

Freiwillige Audits leisten einen bedeutenden Beitrag für den Datenschutz, weil sie als aus eigenem Antrieb veranlasste Maßnahme die Chance in sich bergen, zu mehr Datenschutz in der Fläche zu gelangen.

Datenschutz sollte ein Wettbewerbsvorteil sein. Unternehmen, die sich um einen hohen Datenschutzstandard bemühen, möchten dies auch anerkannt sehen. Ein Datenschutzzertifikat ist ein wichtiges Signal an diese Unternehmen.

Zugleich trägt ein Zertifikat dazu bei, das Vertrauen von Bürgerinnen und Bürgern, Verbraucherinnen und Verbraucher in den achtsamen Umgang mit ihren Daten zu fördern.

Eigenverantwortung ist eine wichtige Säule für einen funktionierenden Datenschutz.

Der Ruf nach einem Audit hat im Zuge der Diskussion um den Europäischen Rechtsrahmen weiteren Auftrieb erhalten. Initiativen auf Landesebene und nunmehr auch auf Bundesebene haben dieses Anliegen aufgegriffen.

II. Erprobung von Modellen, Anforderungen

Die Gesetzgeber haben bisher lediglich einzelne Teilregelungen zu Zertifizierungen getroffen.

Der Düsseldorfer Kreis unterstützt weitergehende Bemühungen, Erfahrungen mit Zertifizierungen zu sammeln, die in eigener Verantwortung im Wege der Selbstregulierung auf der Grundlage von Standards erfolgen, die die Aufsichtsbehörden befürworten.

Verlässliche Aussagen für Bürgerinnen und Bürger, für Verbraucherinnen und Verbraucher erfordern, dass Zertifizierungsdienste anbietende Stellen (Zertifizierungsdienste) geeignete inhaltliche und organisatorische Vorkehrungen für derartige Verfahren mit dem Ziel treffen, eine sachgerechte und unabhängige Bewertung zu gewährleisten.

Dazu gehören im Kern folgende, von Zertifizierungsdiensten zu bearbeitende Strukturelemente:

- Prüffähige Standards, die von den Aufsichtsbehörden befürwortet werden, zu entwickeln, zu veröffentlichen und zur Nutzung für Dritte freizugeben,
- beim Zertifizierungsprozess zwischen verschiedenen Ebenen zu unterscheiden (Prüfung, Zertifizierung, Akkreditierung),
- für verschiedene auf Ebenen und/oder in Verfahrensabschnitten anfallende Aufgaben voneinander abzugrenzende Rollen der jeweils Mitwirkenden vorzusehen,
- Regelungen zur Vermeidung von Interessenkollisionen der an einem Zertifizierungsprozess Beteiligten zu treffen,
- Anforderungen an die Eignung als Prüferin und Prüfer festzulegen und diesen Personenkreis für Zertifizierungen zu qualifizieren,
- den geprüften Sachbereich so zu umschreiben, dass Bürgerinnen und Bürger, Kundinnen und Kunden die Reichweite der Prüfaussage ohne weiteres dem Zertifikat entnehmen können,
- Bedingungen für Erteilung, Geltungsdauer und Entzug von Zertifikaten zu bestimmen,
- Zertifikate zusammen mit den wesentlichen Ergebnissen der Prüfberichte zu veröffentlichen.

III. Abstimmung im Düsseldorfer Kreis

Der Düsseldorfer Kreis verfolgt die Entwicklung von sowohl auf Landesebene mit dieser Zielrichtung begleiteten Initiativen als auch auf Bundesebene begonnenen weiteren Initiativen. Er beteiligt sich an einer ergebnisoffenen Diskussion, um zu optimalen Verfahrensgestaltungen zu gelangen.

Die im Düsseldorfer Kreis zusammenwirkenden Aufsichtsbehörden sehen daher als gemeinsame Aufgabe, sich auf inhaltliche und verfahrensmäßige Anforderungen für Zertifizierungsverfahren zu verständigen und zu Beratungsersuchen im Interesse einer bundesweit einheitlichen Aufsichtspraxis auf im Düsseldorfer Kreis abgestimmter Grundlage Stellung zu nehmen.

Smartes Fernsehen nur mit smartem Datenschutz

– Gemeinsame Position der Aufsichtbehörden für den Datenschutz im nicht-öffentlichen Bereich (Düsseldorfer Kreis) und der Datenschutzbeauftragten der öffentlich-rechtlichen Rundfunkanstalten vom Mai 2014

Moderne Fernsehgeräte (Smart-TV) bieten neben dem Empfang des Fernsehsignals u.a. die Möglichkeit, Internet-Dienste aufzurufen. Den Zuschauern ist es somit möglich, simultan zum laufenden TV-Programm zusätzliche Web-Inhalte durch die Sender auf dem Bildschirm anzeigen zu lassen (etwa durch den HbbTV-Standard). Auch Endgerätehersteller bieten über eigene Web-Plattformen für Smart-TV-Geräte verschiedenste Internet-Dienste an. Für die Zuschauer ist aufgrund der Verzahnung der Online- mit der TV-Welt oft nicht mehr erkennbar, ob sie gerade das TV-Programm oder einen Internet-Dienst nutzen. Überdies können sie vielfach nicht erkennen, um welchen Dienst es

sich handelt. Durch die Online-Verbindung entsteht – anders als beim bisherigen Fernsehen – ein Rückkanal vom Zuschauer zum Fernsehsender, zum Endgerätehersteller oder zu sonstigen Dritten. Das individuelle Nutzungsverhalten kann über diesen Rückkanal erfasst und ausgewertet werden.

Fernsehen ist ein maßgebliches Medium der Informationsvermittlung und notwendige Bedingung für eine freie Meinungsbildung. Das Recht auf freien Informationszugang ist verfassungsrechtlich geschützt und Grundbedingung der freiheitlich demokratischen Grundordnung. Die Wahrnehmung dieses Rechts würde durch die umfassende Erfassung, Auswertung und Nutzung des Nutzungsverhaltens empfindlich beeinträchtigt.

Aus datenschutzrechtlicher Sicht sind die folgenden Anforderungen zu beachten:

1. Die anonyme Nutzung von Fernsehangeboten muss auch bei Smart-TV-Nutzung gewährleistet sein. Eine Profilbildung über das individuelle Fernsehverhalten ist ohne informierte und ausdrückliche Einwilligung der Zuschauer unzulässig.

2. Soweit Web- oder HbbTV-Dienste über Smart-TV-Geräte genutzt werden, unterliegen diese als Telemedien den datenschutzrechtlichen Anforderungen des Telemediengesetzes. Endgerätehersteller, Sender sowie alle sonstigen Anbieter von Telemedien müssen entweder eine entsprechende Einwilligung der Betroffenen einholen oder zumindest die folgenden rechtlichen Vorgaben beachten:

   - Auch personenbeziehbare Daten der Nutzer dürfen nur verwendet werden, sofern dies zur Erbringung der Dienste oder zu Abrechnungszwecken erforderlich ist.

   - Spätestens bei Beginn der Nutzung müssen die Nutzer erkennbar und umfassend über die Datenerhebung und -verwendung informiert werden.

   - Anbieter von Telemedien dürfen nur dann Nutzungsprofile erstellen und analysieren, sofern hierzu Pseudonyme verwendet werden und die betroffene Nutzerin oder der betroffene Nutzer dem nicht widersprochen hat. Derartige Widersprüche sind wirksam umzusetzen, insbesondere im Gerät hinterlegte Merkmale (z.B. Cookies) sind dann zu löschen. Auf das Widerspruchsrecht sind die Nutzer hinzuweisen. IP-Adressen und Gerätekennungen sind keine Pseudonyme im Sinne des Telemediengesetzes.

   - Verantwortliche Stellen haben sicherzustellen, dass Nutzungsprofildaten nicht mit Daten über den Träger des Pseudonyms zusammengeführt werden.

3. Beachtung des Prinzips „privacy by default“: Die Grundeinstellungen der Smart-TV-Geräte und Web-Dienste sind durch die Hersteller und Anbieter derart zu gestalten, dass dem Prinzip der anonymen Nutzung des Fernsehens hinreichend Rechnung getragen wird. Der Aufruf der Web-Dienste und die damit einhergehende wechselseitige Kommu-

nikation mit Endgerätehersteller, Sender oder sonstigen Anbietern per Internet dürfen erst nach umfassender Information durch die Nutzer selbst initiiert werden, z.B. die Red-Button-Aktivierung bei HbbTV. Die auf den Geräten gespeicherten Daten müssen der Kontrolle durch die Nutzer unterliegen. Insbesondere muss die Möglichkeit bestehen, Cookies zu verwalten.

4. Smart-TV-Geräte, die HbbTV-Angebote der Sender sowie sonstige Web-Dienste müssen über sicherheitstechnische Mechanismen verfügen, die die Geräte und den Datenverkehr vor dem Zugriff unbefugter Dritter schützen. Diese Position wird von der Konferenz der Direktoren der Landesanstalten für Medien unterstützt.

Jeder Zweite würde per Fingerabdruck zahlen

Jeder zweite kann sich vorstellen, bargeldlose Zahlungen zum Beispiel per Fingerabdruck oder per Iris-Scan freizugeben. Das geht aus einer repräsentativen Umfrage des Branchenverbands Bitkom hervor. Unter denjenigen, die offen sind für biometrische Verfahren, bevorzugen rund zwei Drittel (64 Prozent) den Fingerabdruck. 54 Prozent würden den Iris-Scan, zwölf Prozent das eigene Stimmprofil nutzen. Für elf Prozent kommt die Herzschlagrate in Betracht.

(Bitkom Pressemitteilung vom 5.8.2014)

Mutter stellt Internet ab – Sohn dreht durch

(Meldung Welt am Sonntag vom 3.8.2014)

Nachdem ihr 15jähriger Sohn 7 Stunden lang ununterbrochen online Playstation gespielt hatte, stellte die Mutter schließlich die Internetverbindung ab. Vor dem anschließenden Tobsuchtanfall des Sohnes floh die Mutter mit einem jüngeren Sohn in ein anderes Zimmer und schloss sich dort ein. Der von dort alarmierten Polizei warf sie durch ein Fenster den Wohnungsschlüssel zu. Zu viert gelang es den Beamten die Wohnungstür zu öffnen, gegen die sich der 15jährige noch stemmte. Er wurde in eine Klinik gebracht.

Literaturhinweise

Buchbesprechungen

Hans-Jürgen Schaffland/Noeme Wiltfang, **Bundesdatenschutzgesetz – BDSG**, 2014, Loseblatt-Kommentar. 2.168 S. in 1 Ordner, Jahresabonnement 112,00 €. Datenbank, im Jahresabonnement 157,08 €.

Die Grundlage für den optimalen Datenschutz ist eine verlässliche, aktuelle Informationsquelle. Genau das bietet der „Schaffland/Wiltfang". Er macht den Zugriff auf andere Gesetzesveröffentlichungen überflüssig, denn er enthält

- die vollständige Kommentierung zum BDSG,
- alle Landesdatenschutzgesetze und Auszüge aus den wichtigsten vom BDSG tangierten Gesetzen.

Ob umfassende Regelungen zu Werbung, Scoring, Arbeitnehmerdaten sowie Meldeplicht bei Datenschutzpannen – bei der täglichen Umsetzung unterstützen

- praktische Beispiele und Hinweise,
- konkrete Formulierungsvorschläge,
- Checklisten zur Prüfung der Zulässigkeit der Datenverarbeitung, der Datennutzung und zu Benachrichtigungspflichten,
- Lösungsvorschläge für die Bewältigung der Datensicherungsmaßnahmen nach § 9 und der Anlage zu § 9,
- der Leitfaden zum PC-Einsatz.

Die 4. Lieferung des Jahres 2014 ergänzt den Kommentarteil um zwischenzeitlich veröffentliche Urteile und Fachbeiträge. Insbesondere wurde die seit kurzem erschienene Fachzeitschrift PinG ausgewertet.

(Redaktion)

Sassenberg, Thomas/Mantz, Reto, **WLAN und Recht. Aufbau und Betrieb von Internet-Hotspots**, Erich Schmidt Verlag, 2014, 270 S., 38,00 €

Die Autoren haben mit dem Werk eine verdienstvolle Zusammenstellung der wesentlichen Rechtsfragen aus den betroffenen Rechtsgebieten vorgelegt, die der Einsatz von WLAN-Funktechnik mit sich bringt. Ausgehend von typischen Betreibermodellen wird der umfangreiche Stoff geordnet und – über ein ausführliches Stichwortverzeichnis – gut auffindbar dargestellt, wobei die ausführliche Unterlegung mit Fußnoten sowie die den einzelnen Kapiteln vorangestellte aktuelle Literatur zum Thema jederzeit vertiefende Recherchen erleichtert.

Das Grundlagenkapitel beginnt mit einer einführenden kleinen Geschichte dieser Technologie, erklärt die verwen-

dete Terminologie und berichtet über die Verbreitung in der Praxis. Dabei werden die gebräuchlichen Formen in ihren konfigurationellen Eigenarten dargestellt. Es folgt eine Beschreibung des durch das Telekommunikationsgesetz festgelegten Rechtsrahmens – insbesondere des Anbieter-Nutzer-Verhältnisses – und seiner Relevanz, abhängig vom typischen Betriebsmodell. Es folgt eine Aufzählung der im Einzelnen zugunsten des Kunden bestehenden gesetzlichen Informationspflichten sowie ein längerer Abschnitt zu Fernmeldegeheimnis und TK-Datenschutz. Die technischen Vorschriften zur öffentlichen Sicherheit runden dieses Kapitel ab.

Ein weiteres Kapitel beschäftigt sich zunächst kurz mit der Verantwortlichkeit der Nutzer und daran anschließend sehr ausführlich mit der Verantwortlichkeit der Betreiber des WLAN. Dabei wird insbesondere auf die Haftungsprivilegierung des § 8 TMG und dessen Anwendung in der Praxis hingewiesen. Gleichzeitig geben die Autoren den WLAN-Betreibern eine Übersicht von empfehlenswerten Maßnahmen an die Hand, um den vom BGH entwickelten Prüfungs- und Überwachungspflichten eines WLAN-Betreibers gerecht zu werden. Dazu gehören z.B. eine Belehrung und eine Überwachung der WLAN-Nutzer, die teilweise ebenfalls notwendig sein kann. Darüber hinaus wird die prozessuale Seite der Verantwortlichkeit dargestellt, die hauptsächlich für die WLAN-Betreiber hinsichtlich einer möglichen Reaktion auf Hinweise, Abmahnungen und Auskunftsverlangen relevant ist.

Daran anschließend wird das Verhältnis zwischen den WLAN-Anbietern und WLAN-Nutzern gebracht. In diesem Zusammenhang werden die verschiedenen Typen eines WLAN-Vertrages beleuchtet, die aufgrund der tatsächlichen Konstellationen zwischen WLAN-Anbieter und WLAN-Nutzer möglich sind. Nach der Einordnung des Vertragsverhältnisses folgt ein Abschnitt zur Vertragsgestaltung zwischen dem Anbieter und dem Nutzer im Hinblick auf die anwendbaren Vorschriften des Verbraucherschutzes sowie der Vorschriften des Telemediendatenschutzes, insbesondere der §§ 11 bis 15 TMG.

Danach befassen sich die Autoren des Werkes mit der Realisierung des WLAN-Betriebs und mit den damit einhergehenden Fragestellungen in den Bereichen der Aggregation von Endkundenanschlüssen, des Einkaufs von (Vor-)Leistungen, der notwendigen Vereinbarungen mit dem Grundstückseigentümer und dem WLAN-Angebot für die öffentliche Hand. Hier hätte man sich gewünscht, wenn auf die häufige Konstellation, dass Kommunen WLAN nicht selbst betreiben, sondern durch Dienstleister betreiben lassen, eingegangen worden wäre. Die Darstellung von Spezialfällen – wie z.B. die Realisierung von WLAN im Flugzeug oder im Gesundheitswesen – bildet den Abschluss dieses Kapitels.

Das Buch endet mit einer Checkliste und weiteren Übersichten, die dem Leser einen schnellen Einstieg in die relevanten Themenkomplexe ermöglichen, und die sich dazu eignen, einen Überblick über die im Werk behandelten Rechtsfragen zu erhalten.

Insgesamt handelt es sich bei dem Werk um eine sinnvolle Zusammenstellung, mit der der Leser Antworten auf die mit dem Aufbau und Betrieb von WLAN-Hotspots einhergehenden Rechtsfragen erhält. Gerade die Checkliste am Ende des Werkes sowie die tabellarischen Zusammenfassungen innerhalb der einzelnen Kapitel bilden dabei eine übersichtliche und damit auch nützliche Hilfe für die Praxis. So kann dieses Werk als wertvolle und interessante Informationsquelle bezeichnet werden, die Betreibern, Nutzern und allen Personengruppen im Zusammenhang mit einem WLAN-Betrieb die einschlägigen Rechtsfragen beantwortet.

Dr. Martin Zilkens, Düsseldorf

Neuerscheinungen

Aufsätze

Die RDV weist regelmäßig auch auf in anderen Zeitschriften erschienene Beiträge zum Recht der Datenverarbeitung hin, um Recherchen zu relevanten Themen zu erleichtern. Einreichungen von Beiträgen zur Aufnahme eines Hinweises werden gerne entgegengenommen.

Gerrit Hornung/Kai Hofmann, **Die Zulässigkeit der Markt- und Meinungsforschung nach Datenschutz- und Wettbewerbsrecht, WRP 2014, S. 776 (Teil I) und WRP 2014, S. 910 ff. (Teil II)**
Der Beitrag gibt zunächst Erläuterungen zu § 30a BDSG. Dabei spielt die notwendigerweise europarechtliche Definition der Werbung nach § 7 UWG eine wesentliche Rolle. Wann Umfragen einen werblichen Charakter haben, wird in Fallgruppen und an Hand der Rechtsprechung eingegrenzt. Für eine für die Rechtspraxis befriedigende Antwort hoffen die Autoren auf eine Entscheidung des BGH, der über § 30a BDSG selbst befinden könnte, zu § 7 Abs. 2 Nr. 2 bis 4 und Abs. 3 UWG im Hinblick auf die Interpretation des Art. 13 EG-DSRL eine Vorabentscheidung des EuGH jedoch einzuholen hätte.

Niko Härting, **Profiling: Vorschläge für eine intelligente Regulierung, CR 2014, S. 528 ff.**
Das Datenschutzrecht muss unter Akzeptanz der neuen Big Data-Technologie die persönlichkeitsrechtlichen Risiken des Profilings minimieren. Betrachtet wird die zweistufige Vorgehensweise, d.h. die Erstellung der Datenbasis und deren nachfolgende Auswertung. Hinsichtlich des bejahten Regulierungsbedarfs werden die diesbezüglichen Vorschläge zur EU-DS-GVO erörtert, wobei der Verfasser eigene Vorschläge macht.

Thomas Hoeren, **Das Konzerntelefonverzeichnis – ein datenschutzrechtlicher Sündenpfuhl?, ZD 2014, S. 441 ff.**
Unter Erörterung diverser – durchweg negativer – Stellungnahmen von Aufsichtsbehörden sieht der Autor eine Berechtigung für derartige Verzeichnisse für den Einzelfall, wenn es gemäß der Konzernstruktur zur Arbeitserledigung funktionsbezogen erforderlich ist (§ 28 Abs. 1 S. 1 Nr. 2 BDS). Ggf. kann unter dieser Voraussetzung auch eine Einwilligung oder eine Betriebsvereinbarung die Erlaubnisgrundlage bilden.

Christoph Bausewein, **Arbeitgeber-Persönlichkeitstests – datenschutzrechtlich zulässig?, ZD 2014, S. 443 ff.**
Der Beitrag widmet sich dem Einsatz von psychischen Eignungstests bei der Bewerberauswahl und Personalentwicklung. Er vermittelt Grundlagenwissen und gibt eine Orientierungshilfe zu den Zulässigkeitsrahmen. Voraussetzung ist die Erforderlichkeit des auf eine konkrete Maßnahme abgestellten Tests (§ 32 Abs. 1 S. 1 BDSG) oder ggf. auch einer Einwilligung.

Martina Vomhof, **Verhaltensregelungen nach § 38a BDSG – Der Code of Conduct der Versicherungswirtschaft, PinG 2014, S. 209 ff.**
Der Beitrag erläutert Hintergründe und Regelungsinhalt des ersten nach § 38a BDSG abgeschlossenen Verhaltenscodex, d.h. einer Selbstverpflichtung auf eine branchenspezifische Konkretisierung der Zulässigkeit der Verarbeitung von Versichertendaten.

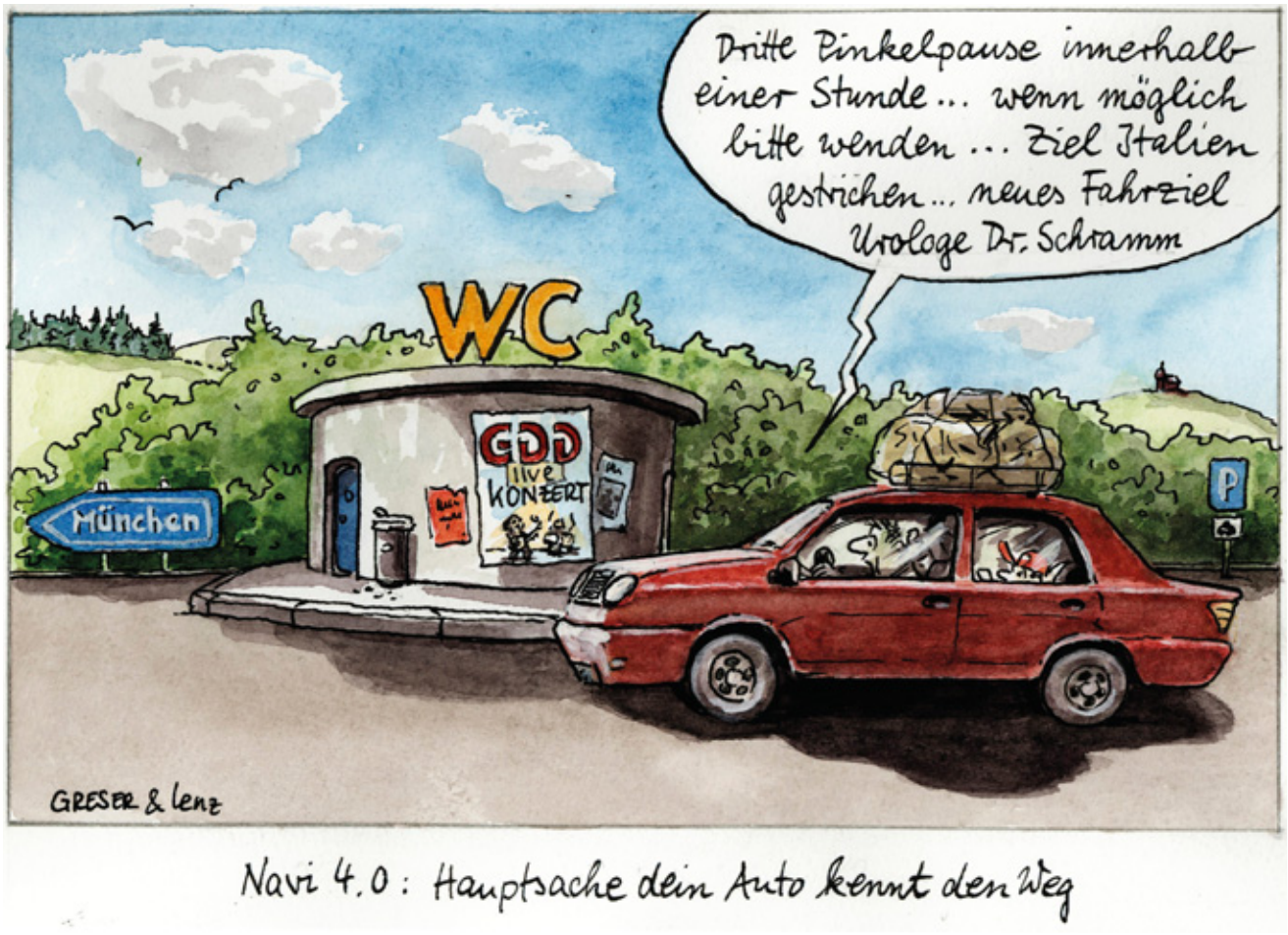
Stefan Wehmeyer, **Kapitalisierungsmöglichkeiten von Bestandskundendaten insbesondere im gewerblichen Bereich, PinG 2014, S. 183 ff.**
Der Autor kommentiert § 28 Abs. 3 BDSG und erörtert inwieweit nach dem UWG unzulässige werbliche Datennutzungen sich – was er verneint – auf das BDSG auswirken.

Christoph Werkmeister/Daniel Görlich, **Die neue EU-Verordnung zu Benachrichtigungspflichten bei Datenpannen, K&R 2014, S. 632 ff.**
Der einheitlichen Umsetzung der in der EG-DSRL vorgesehenen Benachrichtigungspflicht bei sog. Datenpannen dient die Verordnung Nr. 611/2013 vom 24.6.2013 (Meldeverordnung). Sie konkretisiert – unabhängig von der Umsetzung der DSRL Umstände, Form sowie Verfahren zu Benachrichtigungspflichten. Für § 42a BDSG bzw. § 15a TMG bringt die Verordnung keinen Änderungsbedarf. pflichten Allein für§ 109a TKG ergeben sich Anwendungshinweise.

Juergen Taeger, **Rechtlicher Regelungsrahmen des Scorings in Deutschland, K&R, Beiheft zu Heft 10/2014, S. 4 ff.**
Der Beitrag erläutert zunächst die Übermittlungen von negativen Forderungsdaten und von Positivdaten an Auskunfteien (§ 28b Abs. 1 und 2 BDSG). Sodann werden die Voraussetzungen für das Kreditscoring in § 28b BDSG, §§ 10 Abs. 2, 18 Abs. 2 KWG und §§ 491a, 509 BGB und die diesbezüglichen Betroffenenrechte dargestellt. Letztlich wird ein Blick auf die Regelungen in dem Entwurf der EU-DS-GVO geworfen.

Edgar Rose, **Der rechtliche Rahmen des Scorings in ausgewählten Vergleichsländern – Bestandsaufnahme und Schlussfolgerungen, K&R Beiheft zu Heft 10/2014, S. 17 ff.**
Dargestellt und verglichen werden die Rechtslage in zwei EU-Ländern (Frankreich und Großbritannien), in den USA und auch Australien sowie eine Parallele zu Deutschland gezogen.

Klaus Heß, **Die „CallCentrifizierung", CuA 9/2014, S. 13 ff.**
Der Autor sieht die Leistungskontrolle, d.h. die ständige Überwachung, Bewertung und Steuerung nach dem „Call Center-Prinzip", auf dem Vormarsch in andere Dienstleistungsbereiche mit Kunden bzw. Servicefunktion.



Navi 4.0: Hauptsache dein Auto kennt den Weg

Digitale Verkehrserziehung

Frauen fahren besser Auto als Männer. Das ist kein Vorurteil, sondern durch Zahlen aus der Versicherungsbranche gestützt. Da sich das schon bei Fahranfängerinnen und Fahranfängern feststellen lässt, ist es doch eine gute Idee, wenn Jungs wie Mädchen fahren. Wie erzieht man zur Verbesserung der Unfallstatistik Rowdys zu Girlys? Eine englische Versicherung setzt mit ihrem Tarif „Drive like a girl“ http://www.drivelikeagirl.com/ auf ein Anreizsystem. Die Versicherung ist für junge Frauen von 17 bis 25 entwickelt worden. Aber wer sich der Frauenbewegung als Mann anschließen will, um von den günstigen Provisionen zu profitieren, kann das natürlich auch.

Voraussetzung für die Buchung des Tarifs ist aber, dass man sein Fahrverhalten zur Bewertung offenlegt. Das funktioniert nicht, indem man im Antragsformular der Versicherung etwa unter Fahrstil statt bei rowdylike sein Kreuzchen bei girlylike setzt. Die Versicherung will das genau wissen und verlangt den Einbau einer Telematikbox. Diese speichert mit dem Einverständnis des Versicherten jeden gefahrenen Kilometer und meldet Daten über Position, Uhrzeit, Geschwindigkeit, Brems- und Beschleunigungsverhalten, Fahrtrichtung und eine Kennung des KFZ an die Versicherung. Die Versicherung bewertet dann, ob das Fahrverhalten im Sinne der Versicherung dem einer vorbildlichen Fahranfängerin angemessen ist. Wenn das so ist, gibt es einen Bonus, wenn nicht, zahlt man mehr.

Es gibt viele solcher Angebote, die unser Verhalten steuern sollen. Sie regen uns z.B. durch Apps zu richtiger Ernährung und ausreichender Bewegung an und sie liefern uns Erfolgskontrollen in Echtzeit. Der positive Effekt solcher Geschäftsmodelle ist klar. Sie können zu besonnenem Verhalten, Gesundheit und Sicherheit beitragen, und sie können uns erziehen. Dafür wird unser Verhalten gespeichert und durchsichtig gemacht, kontrolliert und verwertet. Wenn wir solche Dienste benutzen, sollten wir uns immer fragen, welche Daten dabei übertragen werden und zu welchem Zweck das geschieht. Dass Volksgesundheit und Verkehrssicherheit der Hauptzweck bleiben, können wir als Nutzer jedenfalls nicht kontrollieren.