ISSN 0178-8930

G 20 141

Zeitschrift für Datenschutz-, Informations- und Kommunikationsrecht

RDV

4/2015

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

31. Jahrgang
August 2015
Seiten 165–218

GDD
Gesellschaft für Datenschutz und Datensicherheit e.V.

DATAKONTEXT
www.rdv-online.de

Zeitschrift für
Datenschutz-, Informations-
und Kommunikationsrecht

31. Jahrgang 2015
Heft 4
Seiten 165–218

RDV

Recht der Datenverarbeitung

Inhaltsverzeichnis

Beilagenhinweis GDD-Mitteilungen 4/2015; DATAKONTEXT GmbH, Frechen

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 GmbH, 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 GmbH, 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 GmbH, Frechen
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
31. Jahrgang 2015 Heft 4
Seiten 165–218

RDV
Recht der Datenverarbeitung

31. Jahrgang · August 2015 · Seiten 165–218

Editorial

Die EU-DS-GVO und die Fortgeltung deutschen Datenschutzrechts – kein Kahlschlag im Datenschutzrecht

Mit Inkrafttreten der EU-DS-GVO, mit der nach den nunmehr offenbar zügig angegangenen Trilog-Gesprächen u.U. im Jahre 2018 zu rechnen ist (Art. 91), wird der Datenschutz in der der EU weitgehend auf unmittelbar geltendem einheitlichen europäischen Recht basieren. Gemäß Art. 288 Abs. 2 des Vertrags über die Arbeitsweise der Europäischen Union sind Verordnungen allgemein und unmittelbar geltende und in allen ihren Teilen verbindliche Rechtsakte. Auf Grund ihrer „Durchgriffswirkung" müssen sie von den EU-Mitgliedstaaten nicht in nationales Recht umgesetzt werden. Vielmehr besteht ein „Umsetzungsverbot", das auch Modifikationen der vorgegebenen Regelungen durch die einzelnen Mitgliedstaaten grundsätzlich untersagt. Zur Frage steht jedoch, ob dieses Umsetzungsverbot tatsächlich für die EU-DS-GVO gelten und zum vollständigen Ende des aktuellen deutschen Datenschutzrechts führen wird, d.h. dass dieses durch die Verordnung „kompromisslos" abgelöst werden wird (so z.B. Eckhardt/Kramer/Mester, DuD 2013, 623).

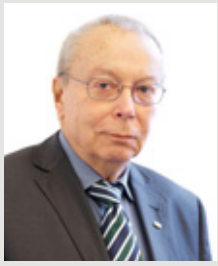
Dies gilt zunächst nicht für die Bereiche, für die die Verordnung ausdrücklich Öffnungsklauseln enthält, wie es u.a. hinsichtlich der öffentlichen Verbreitung von Informationen, Meinungen und Ideen zu insbesondere journalistischen, künstlerischen Zwecken (Art. 80) und zum Beschäftigtendatenschutz (Art. 82) der Fall ist. Indirekte Öffnungsklauseln enthalten Art. 6 Abs. 1 Buchst. c und e EU-DS-GVO (gem. Vorschlag Kom./Parl./Rat), wenn sie die zur Erfüllung einer dem Verantwortlichen auferlegten rechtlichen Verpflichtung, für die Wahrnehmung einer im öffentlichen Interesse liegenden Aufgabe oder in Ausübung hoheitlicher Gewalt erforderlichen Verarbeitungen für zulässig erklärt.

Diese Erlaubnisvorschrift setzt die nationale Kompetenz nicht nur zur Regelung der rechtlichen Verpflichtung bzw. der öffentlichen Aufgabe, sondern auch zur Festlegung der dafür erforderlichen Datenverarbeitungen voraus, wobei es nach der Vorgabe des Bundesverfassungsgerichts, des EuGH und des EMRGH normenklarer, auf konkrete Zweckbestimmungen bezogener Eingriffsregelungen bedarf. Art. 6 Abs. 3 S. 2 und Erwägungsgrund 37 (Vorschlag Rat) konkretisiert dies, indem festzulegen ist, „welche Art von Daten verarbeitet werden, welche Personen betroffen sind, an welche Einrichtungen die Daten weitergegeben werden, für welche Zwecke und wie lange sie gespeichert werden dürfen" und welche anderen Maßnahmen ergriffen werden, um zu gewährleisten, dass die Verarbeitung nach Recht und Gesetz erfolgt.

Die Regelung soll „lesbar und in sich verständlich" sein. Dazu sollen Mitgliedstaaten auch Bestandteile der Verordnung in der nationalen Regelung wiederholen dürfen (Erwägungsgrund 6a (Rat)). Zudem soll das Mitgliedsland zur Beibehaltung von bereits zur Umsetzung der Richtlinie 95/46/EG erlassener notwendiger sektorspezifischer Rechtsvorschriften berechtigt sein. (Erwägungsgrund 8 S. 4 und 5a (Rat))

Datenschutzbezogene Regelungen im Meldegesetz, der Abgabenordnung, in den Sozialgesetzbüchern, den Krankenhaus- oder Schulgesetzen werden genausowenig zur Makulatur werden wie möglichweise auch einige „sektorspezifische" Bestimmungen im derzeitigen BDSG.

Prof. Peter Gola



Prof. Peter Gola
Mitherausgeber und federführender Schriftleiter der Fachzeitschrift RDV sowie Ehrenvorsitzender der Gesellschaft für Datenschutz und Datensicherheit (GDD) e.V., Bonn

Termin	Thema	Ort	Kontakt
14.-16.09.2015	Das SAP-System für Datenschutzbeauftragte	Köln	GDD e.V. und DATAKONTEXT
14.-18.09.2015	Einführung in den Datenschutz für die Privatwirtschaft – Teil 1	Köln	GDD e.V. und DATAKONTEXT
22.-23.09.2015	Datenschutz Kompakt	Köln	GDD e.V. und DATAKONTEXT
24.09.2015	Grundlagen der Auftragsdatenverarbeitung	Köln	GDD e.V. und DATAKONTEXT
29.09.2015	ISO 27001 und Datenschutz	Köln	GDD e.V. und DATAKONTEXT
30.09.2015	Kundendatenschutz	Köln	GDD e.V. und DATAKONTEXT
01.10.2015	Big Data-Analysen und der Datenschutz	Köln	GDD e.V. und DATAKONTEXT
06.10.2015	Verfahrensverzeichnis, Verarbeitungsübersicht, Vorabkontrolle	Köln	GDD e.V. und DATAKONTEXT
06.-08.10.2015	Einführung in den technisch-organisatorischen Datenschutz – Teil 2	Berlin	GDD e.V. und DATAKONTEXT
08.10.2015	Datenschutz und Videoüberwachung – Was geht und was geht nicht?	Stuttgart	GDD e.V. und DATAKONTEXT
12.10.2015	Einsatz mobiler Endgeräte: Datenschutz und IR-Sicherheit	Frankfurt/M.	GDD e.V. und DATAKONTEXT
14.10.2015	IT-Sicherheit für Datenschutzbeauftragte	Frankfurt/M.	GDD e.V. und DATAKONTEXT
19.10.2015	Der Datenschutzbeauftragte mit wenig Zeitbudget	Köln	GDD e.V. und DATAKONTEXT
19.-23.10.2015	Der Auditor zur Auftragsdatenverarbeitung	Köln	GDD e.V. und DATAKONTEXT
26.10.2015	Die häufigsten Datenschutz-Schwachstellen und wie man sie vermeiden kann	Köln	GDD e.V. und DATAKONTEXT
27.10.2015	Aktuelle Prüfpraxis der Datenschutzaufsichtsbehörden	Stuttgart	GDD e.V. und DATAKONTEXT
29.10.2015	SAP-Funktionen für den Datenschutz	Köln	GDD e.V. und DATAKONTEXT
29.10.2015	Das neue Melderecht	Berlin	GDD e.V. und DATAKONTEXT
02.11.2015	Moderne Unternehmenskommunikation	Köln	GDD e.V. und DATAKONTEXT
02.-03.11.2015	Datenschutz Management – Teil 3	Berlin	GDD e.V. und DATAKONTEXT
04.11.2015	Prüfung von SAP-Systemen durch Datenschutzbeauftragte	Frankfurt/M.	GDD e.V. und DATAKONTEXT
05.11.2015	Kontrolle von Auftragnehmern im Rahmen der Auftragsdaten-verarbeitung	Köln	GDD e.V. und DATAKONTEXT
09.11.2015	Umsetzung des neuen Datenschutzstandards bei Dienstleistern	Köln	GDD e.V. und DATAKONTEXT
10.11.2015	Datenschutz Aktuell	Stuttgart	GDD e.V. und DATAKONTEXT
12.11.2015	Die neue Herausforderung im Datenschutz: Connected Car bei der Dienstwagennutzung	Stuttgart	GDD e.V. und DATAKONTEXT

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

Aufsätze

Prof. Dr. Rainer W. Gerling

Das IT-Sicherheitsgesetz: purer Aktionismus oder doch mehr IT-Sicherheit?

Während in Deutschland seit über 40 Jahren Datenschutz detailliert geregelt ist, fehlen explizite gesetzliche Vorgaben zur IT-Sicherheit weitgehend. Lediglich in vier Gesetzen (BDSG[1], TKG[2], TMG[3] und EnWG[4]) gibt es konkrete, allerdings Sektorspezifische Regelungen. Auch ein IT-Sicherheitsbeauftragter in Analogie zum Datenschutzbeauftragten ist nur für „Erbringer von Telekommunikationsdiensten für die Öffentlichkeit" vorgeschrieben.

Trotzdem haben viele Unternehmen organisatorische Strukturen zur IT-Sicherheit geschaffen, weil es für die Unternehmen sinnvoll ist. Während große Unternehmen hier gut aufgestellt sind, sieht es bei den kleineren Unternehmen eher nicht so optimal aus.

Der Bundestag verabschiedete am 12.6.2015 in dritter Lesung das Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) in der Fassung des Regierungsentwurfs[5] mit den Änderungsvorschlägen[6] des Innenausschusses.

Das IT-Sicherheitsgesetz ändert das BSI-Gesetz (Artikel 1 und 8), das Atomgesetz (Artikel 2), das Energiewirtschaftsgesetz (Artikel 3), das Telemediengesetz (Artikel 4), das Telekommunikationsgesetz (Artikel 5), das Bundesbesoldungsgesetz (Artikel 6) und das Bundeskriminalamtgesetz (Artikel 7). Die Änderungen treten (bis auf Artikel 8) am Tag nach der Verkündung des Gesetzes in Kraft. Eine Synopse der Änderungen ist auf der Homepages des Autors zu finden[7].

In § 10 Abs. 1 BSIG neu wird die Bundesregierung ermächtigt, ohne Zustimmung des Bundesrates eine Rechtsverordnung zu erlassen, welche „wegen ihrer Bedeutung als kritisch anzusehenden Dienstleistungen und deren als bedeutend anzusehenden Versorgungsgrads, welche Einrichtungen, Anlagen oder Teile davon als Kritische Infrastrukturen im Sinne dieses [IT-Sicherheits-]Gesetzes gelten". Zwei Jahre nach In-Kraft-Treten dieser Verordnung müssen die betroffenen Unternehmen die erforderlichen technischen und organisatorischen Maßnahmen getroffen haben. Da viele (kleinere) Unternehmen abwarten werden, ob sie unter die zukünftige Definition der kritischen Infrastruktur fallen, wird es dann zeitlich u.U. eng. Das In-Kraft-Treten dieser Verordnung startet die diversen Übergangsfristen.

Neue Rechte und Pflichten des BSI

Im Rahmen der Tätigkeit des BSI als „IT-Sicherheitsdienstleister" werden die entsprechenden Bundesbehörden jetzt dazu verpflichtet, entsprechende Protokolldateien (§ 5 Abs. 1 Nr. 1 BSIG) und Schnittstellendaten (§ 5 Abs. 1 Nr. 2 BSIG), die beim Betrieb von Kommunikationstechnik des Bundes anfallen, zur Verfügung zu stellen (§ 5 Abs. 1 Satz 4 BSG neu). Gerade vor den aktuellen Sicherheitsvorfällen im Deutschen Bundestag[8] stellt sich die pragmatische Frage, ob die bundeseigenen IT-Sicherheitsexperten nicht auch hier tätig werden sollten, da nach unveränderter Rechtslage das BSI für die *„Kommunikationstechnik der Bundesgerichte, soweit sie nicht öffentlich-rechtliche Verwaltungsaufgaben wahrnehmen, des Bundestages, des Bundesrates, des Bundespräsidenten und des Bundesrechnungshofes"* nicht zuständig ist (§ 2 Abs. 3 Satz 2 BSIG).

Das BSI erhält als neue Aufgabe die Funktion der zentralen Meldestelle für IT-Sicherheitsvorfälle bei Unternehmen, die dem Bereich Kritische Infrastruktur zuzuordnen sind (§ 8b BSIG neu).

Das BSI muss die eingegangenen Meldungen auswerten und daraus Lagebilder für den Bereich Kritische Infrastruktur erstellen und diese Lagebilder über die Kontaktstellen an die Unternehmen kommunizieren (§ 8b Abs. 2 Nr. 4 BSIG neu).

Kritische Infrastrukturen

Für die Unternehmen[9] ist es wichtig, beurteilen zu können, inwieweit sie unter die Regelungen des IT-Sicherheitsgesetzes fallen. Der § 2 Abs. 10 BSIG neu definiert grob den Begriff „Kritische Infrastruktur" als die Bereiche *„Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen"* und weiter als alle *„von hoher Bedeutung für das*

1 § 9 BDSG mit Anlage für verantwortliche Stellen bei der Verarbeitung personenbezogener Daten.

2 § 109 Abs. 1 TKG für „jeden Dienstleister" und § 109 Abs. 2 und 3 für „Erbringer von Telekommunikationsdiensten für die Öffentlichkeit".

3 § 13 Abs. 4 TMG für Diensteanbieter.

4 § 11 Abs. 1a EnWG für Betreiber von Energieversorgungsnetzen.

5 BT-Drs. 18/4096, http://dip.bundestag.de/btd/18/040/1804096.pdf; abgerufen am 13.6.2015.

6 BT-Drs. 18/5121, http://dip.bundestag.de/btd/18/051/1805121.pdf; abgerufen am 13.6.2015.

7 Http://www.rainer-gerling.de/gesetze

8 Http://www.golem.de/news/iuk-kommission-das-protokoll-des-bundestags-hacks-1506-114635.html

9 Kleinstunternehmen (weniger als 10 Beschäftigte und weniger als 2 Mio. Euro Jahresumsatz bzw. Jahresbilanzsumme (Empfehlung der Kommission 2003/361/EG, ABl. L 124 vom 20.5.2003, S. 36) sind ausgenommen.

Funktionieren des Gemeinwesens […], weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten" könnten. Die Rechtsverordnung nach § 10 Abs. 1 BSIG neu soll dies weiter konkretisieren.

Das Bundesministerium des Innern stellt eine Seite mit einer etwas detaillierten Definition von Kritischer Infrastruktur zur Verfügung[10]. Danach sind *„Kritische Infrastrukturen […] Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden."* Darüber hinaus liefert diese Seite eine „Sektoren- und Brancheneinteilung Kritischer Infrastrukturen".

Durch das Terrorismusbekämpfungsgesetz[11] wurde 2002 das Sicherheitsüberprüfungsgesetz[12] um Regelungen zum vorbeugenden personellen Sabotageschutz ergänzt und die Bundesregierung ermächtigt, durch Rechtsverordnung festzustellen, welche Behörden und nichtöffentlichen Stellen lebens- oder verteidigungswichtige Einrichtungen i.S. des Sicherheitsüberprüfungsgesetzes sind. Die Sicherheitsüberprüfungsfeststellungsverordnung[13] regelt dies und dürfte eine Grundlage für die entsprechende neue Verordnung sein. Insbesondere der zweite Teil, die §§ 9a bis 11, sind für Unternehmen relevant.

Meldepflicht

Unternehmen aus dem Bereich Kritische Infrastruktur müssen *„erhebliche Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse"* dem BSI melden (§ 8b Abs. 4 BSIG neu). Zur Durchführung der Kommunikation mit dem BSI wird beim Unternehmen eine Kontaktstelle eingerichtet (§ 8b Abs. 3 BSIG neu). Die Unternehmen müssen sicherstellen, dass sie über die Kontaktstelle *„jederzeit erreichbar sind"*. Dies kann wohl nur als eine 24/7-Erreichbarkeit verstanden werden. Die Betreiber kritischer Infrastruktur aus dem gleichen Sektor können eine gemeinsame Kontaktstelle benennen (§ 8b Abs. 5 BSIG neu), mit der dann das BSI in der Regel kommuniziert. Diese übergeordnete Kontaktstelle verteilt dann die Information unter den Unternehmen eines Sektors. Insbesondere vor dem Hintergrund der jederzeitigen Erreichbarkeit scheint das die zu bevorzugende Kommunikationsstruktur zu sein. Die übergeordnete Kontaktstelle entbindet ein Unternehmen aber nicht von der Pflicht eine eigene Kontaktstelle einzurichten.

Leider wird auch nicht definiert, was eine *„erhebliche Störung"* ist. Es sind alle Störungen, die zu *„einem Ausfall oder einer Beeinträchtigung der Funktionsfähigkeit"* der Kritischen Infrastrukturen führen können oder geführt haben (§ 8b Abs. 4 Satz 1 BSIG neu). Diese Formulierung muss wohl so verstanden werden, dass das operative Geschäft des Betreibers, also z.B. die Energieversorgung, von dem Ausfall betroffen oder bedroht sein muss.

Werden im Rahmen der Meldungen personenbezogene Daten übermittelt, unterliegen diese einer strikten Zweckbindung (§ 8b Abs. 7 BSIG neu). Die Regelungen aus § 5 Abs. 7 BSIG bezüglich Erkenntnissen aus dem Kernbereich privater Lebensgestaltung und über Personen mit einem Zeugnisverweigerungsrecht sind anzuwenden.

Das BSI wird ermächtigt, Hard- und Software zu untersuchen um Sicherheitslücken zu finden (§ 7a BSIG neu). Die dabei erlangten Erkenntnisse darf das BSI erforderlichen Falls veröffentlichen, wenn den Herstellern Gelegenheit zur Stellungnahme gegeben wird (Responsible Disclosure).

Mindeststandards zur IT-Sicherheit

Das BSI entwickelt Mindeststandards für die IT-Sicherheit der Informationstechnik des Bundes (§ 8 BSIG neu). Diese Mindeststandards können vom Bundesministerium des Innern mit Zustimmung des IT-Rats als Verwaltungsvorschriften erlassen werden. Für die Bundesgerichte, soweit sie nicht öffentlich-rechtliche Verwaltungsaufgaben wahrnehmen, den Bundestag, den Bundesrat, den Bundespräsidenten und den Bundesrechnungshof sind die Verwaltungsvorschriften lediglich Empfehlungen.

Die Branchenverbände der Betreiber Kritischer Infrastruktur können branchenspezifische Sicherheitsstandards zur Gewährleistung der IT-Sicherheit in der Branche entwickeln (§ 8a Abs. 2 BSIG neu). Das BSI stellt im Benehmen mit dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe und eventuell zuständigen Aufsichtsbehörden fest, ob die Standards ausreichend sind.

Auditieren, Evaluieren und das Bußgeld

Alle zwei Jahre müssen die betroffenen Unternehmen nachweisen, dass sie angemessene Sicherheitsmaßnahmen implementiert haben (§ 8a Abs. 3 BSIG neu). Der Nachweis kann durch Sicherheitsaudits, Prüfungen oder Zertifizierungen erfolgen.

Das BSI kann die Details der Auditierung, der Prüfungen und IT-Sicherheitsaudits sowie die fachlichen und organisatorischen Anforderungen an die prüfenden Stellen festlegen (§ 8a Abs. 4 BSIG neu).

Werden die Nachweise nicht erbracht oder die IT-Sicherheit nicht angemessen implementiert, kann ein Bußgeld verhängt werden (§ 14 BSIG neu). Falls auf Verlangen des BSI festgestellte Sicherheitsmängel nicht beseitigt werden, kann es bis 100.000 € betragen; ansonsten beträgt es bis 50.000 €. Eine

10 Https://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/Sicherheit/BevoelkerungKrisen/Sektoreneinteilung.pdf?__blob=publicationFile; abgerufen am 7.6.2015.

11 Gesetz vom 9. Januar 2002 (BGBl. I S. 361).

12 Sicherheitsüberprüfungsgesetz vom 20. April 1994 (BGBl. I S. 867) zuletzt geändert durch Artikel 4 des Gesetzes vom 7. Dezember 2011 (BGBl. I S. 2576).

13 Sicherheitsüberprüfungsfeststellungsverordnung in der Fassung der Bekanntmachung vom 12. September 2007 (BGBl. I S. 2294) zuletzt geändert durch Artikel 8 des Gesetzes vom 7. Dezember 2011 (BGBl. I S. 2576). Die §§ 2 bis 12 der Verordnung treten am 10. Januar 2016 außer Kraft, falls die Gültigkeit nicht verlängert wird. Hierzu findet derzeit eine Evaluierung und Bewertung statt.

Ordnungswidrigkeit begeht auch, wer keine Kontaktstelle benennt oder erforderliche Meldungen unterlässt.

Kleine Vorratsdatenspeicherung

Nach dem bisherigen § 100 Abs. 1 TKG darf ein Dienstanbieter zum *„Erkennen, Eingrenzen oder Beseitigen von Störungen oder Fehlern an Telekommunikationsanlagen die Bestandsdaten und Verkehrsdaten der Teilnehmer und Nutzer erheben und verwenden."* In der neuen Fassung wird die Befugnis auf *„Störungen, die zu einer Einschränkung der Verfügbarkeit von Informations- und Kommunikationsdiensten oder zu einem unerlaubten Zugriff auf Telekommunikations- und Datenverarbeitungssysteme der Nutzer"* erweitert (§ 100 Abs. 1 TKG neu).

Der Bundesrat hatte in seiner Stellungnahme[14] vom 6.2.1015 unter Nr. 9 geäußert: *„Gemäß § 100 Abs. 1 TKG-E sollen Telekommunikationsanbieter die erweiterten Befugnisse erhalten, Nutzungsdaten „zum Erkennen, Eingrenzen und Beseitigen von Störungen sowie von Missbrauch seiner für Zwecke seines Telemedienangebots[15] genutzten technischen Einrichtungen" zu erheben und zu verwenden. Bei der damit eingeführten Speicherbefugnis handelt es sich im Kern um eine weitreichende Vorratsdatenspeicherung, für die unter anderem das Bundesverfassungsgericht und der Europäische Gerichtshof enge Grenzen gesetzt haben."*

Tatsache ist jedoch, dass vorhandene Verkehrs- und Bestandsdaten gegebenenfalls auf Anforderung Strafverfolgungsbehörden zur Verfügung gestellt werden müssen. An dieser Stelle ist nicht geregelt, wie lange diese Daten gespeichert werden dürfen; es wird lediglich auf die Erforderlichkeit abgestellt. Es ist jedenfalls leicht vorstellbar, dass die heute etablierten sieben Tage für die hinzugekommenen Erlaubnistatbestände zu kurz sind.

Völlig neu ist der Erlaubnistatbestand des *„unerlaubten Zugriffs auf Telekommunikations- und Datenverarbeitungssysteme der Nutzer"*. Dies ist auch im Kontext des neuen § 109a Abs. 4 TKG neu zu sehen, nachdem Telekommunikationsanbieter für die Öffentlichkeit ihnen bekannt gewordene Störungen, die von Systemen des Nutzers ausgehen, dem Nutzer unverzüglich mitteilen müssen.

Da der Nutzer auch auf technische Maßnahmen zum Beseitigen der Störung hingewiesen werden muss, kann hier leicht ein neues Kommunikationsformat mit dem eigenen Provider entstehen, das Kriminellen die Arbeit „erleichtert". Die Standard-Mail eines Providers an seine DSL-Kunden mit dem Hinweis auf die Störung und dem Link auf den Patch ist schnell bekannt und wird dann nachgebaut. Ob im Massengeschäft mit Nutzern elektronische Signaturen zur Vertrauensbildung beitragen, darf bezweifelt werden.

BKA ermittelt Cybercrime

Das Bundeskriminalamt wird als zentrale Stelle für alle Ermittlungen bei Straftaten nach den §§ 202a, 202b, 202c, 263a, 303a und 303b StGB zuständig, soweit die innere oder äußere Sicherheit der Bundesrepublik Deutschland oder Bundesbehörden oder Kritische Infrastruktureinrichtungen betroffen sind (§ 4 Abs. 1 Nr. 5 BKAG neu).

EG-Richtlinie

Die Europäische Kommission hat im Februar 2013 einen Entwurf einer *„Richtlinie des Europäischen Parlaments und des Rates über Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit in der Union"*[16] vorgelegt. Dieser Entwurf setzt früher an und verlangt von den Mitgliedsstaaten das Erstellen einer nationalen IT-Sicherheitsstrategie und die Errichtung einer zuständigen Behörde. Regeln für die Zusammenarbeit zwischen den Mitgliedstaaten und der Kommission im Bereich der IT-Sicherheit, für den Austausch von Frühwarnungen vor Sicherheitsrisiken und -vorfällen über eine sichere Infrastruktur, für die Koordinierung und für die Durchführung regelmäßiger gegenseitiger Überprüfungen sollen geschaffen werden. Die Betreiber kritischer Infrastrukturen in bestimmten Bereichen (Finanzdienste, Verkehr, Energie und Gesundheitswesen), Betreiber zentraler Dienste der Informationsgesellschaft (vor allem App-Stores, eCommerce-Plattformen, Internet-Zahlungen, Cloud-Computing, Suchmaschinen, soziale Netze) und öffentliche Verwaltungen müssen Risikomanagementmethoden einführen und schwerwiegende Sicherheitsvorfälle in ihren Kerndiensten einer zuständigen nationalen Behörde melden.

Im März 2014 stimmte das Europäische Parlament dem Entwurf mit Änderungen zu[17]. Der nächste Schritt im Verfahren wäre die erste Lesung im Rat der Europäischen Union.

Am 29. Juni erzielte die lettische Präsidentschaft im Rat der Europäischen Union eine Einigung mit dem Europäischen Parlament über die wichtigsten Prinzipien des Entwurfs der Richtlinie zur Netzund Informationssicherheit[18]. Dabei wurden die Grundzüge einer europaweiten Meldepflicht für IT-Sicherheitsvorfälle festgelegt. Die Mitgliedsländer müssen einen nationalen IT-Sicherheitsplan erarbeiten und zuständige Behörden festlegen.

Fazit

Für Unternehmen und Behörden gewinnt die Nutzung der Informations- und Kommunikationstechnik zunehmend an Bedeutung. Damit nimmt auch die Abhängigkeit von deren Funktionstüchtigkeit stetig zu. Es ist daher unerlässlich,

14 BR-Drs. 634/14.

15 An dieser Stelle wird der Gesetzentwurf fehlerhaft zitiert. Der Bezug auf „Telemedien" in einem Änderungsvorschlag des § 100 TKG macht so keinen Sinn. Das Zitat stammt aus einem älteren Entwurf eines IT-Sicherheitsgesetzes (Entwurf vom 18.8.2014) und war in einem Änderungsvorschlag zur Einfügung eines Abs. 9 in § 15 TMG enthalten. Dieser Vorschlag war im aktuellen Gesetzentwurf nicht mehr enthalten.

16 Http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1666; abgerufen am 6.6.2015.

17 Http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2014-0244&language=DE; abgerufen am 06.06.2015.

18 Https://eu2015.lv/de/nachrichten/pressemitteilungen/2512-lettische-eu-ratspraesidentschaft-erzielt-einen-durchbruch-bei-den-gespraechen-mit-dem-europaeischen-parlament-ueber-die-netz-und informationssicherheit: Abgerufen am 02.07.2105.

umfassende Sicherheitsmaßnahmen zu ergreifen. Hierzu muss man ein Lagebild der Bedrohungen haben, um die Sicherheitsmaßnahmen zielgerichtet und effizient zu gestalten.

Ein umfassendes Lagebild kann aber nur zentral in möglichst vollständiger Kenntnis der Angriffe erstellt werden. Deshalb muss eine zentrale Stelle über eine Meldepflicht die Übersicht haben.

Die Meldepflicht muss so gestaltet werden, dass die zentrale Stelle nicht in den Meldungen trivialer Vorfälle untergeht, aber gleichzeitig das Wesentliche ankommt. Außerdem müssen die Unternehmen und Behörden, die Meldungen machen, auch etwas zurückbekommen. Die aufgrund der Meldungen erstellten Lagebilder und Sicherheitsinformationen müssen zeitnah an die meldenden Unternehmen und Behörden zurückfließen.

Die Verpflichtung zur Einführung von Mindeststandards der IT-Sicherheit für Unternehmen der sog. „kritischen Infrastruktur" ist sicherlich sinnvoll. Der Roman „Blackout" von Marc-Elsberg[19] beschreibt das Szenario des Ausfalls kritischer Infrastruktur auf eindrucksvolle Weise. Das ZDF berichtet in der Sendung Frontal 21 vom 9.6.2015 über eine Studie des Bundesamtes für Bevölkerungsschutz und Katastrophenhilfe, in der die Folgen eines Cyberangriffes gegen die Stromversorgung untersucht wurden. Während bereits nach einem Tag große Teile des Gesundheitswesens ausfallen, dauert es maximal drei Wochen, bis es keine Treibstoffversorgung mehr gibt[20].

Der Gesetzgeber möchte die genaue Definition der kritischen Infrastruktur erst in einer Verordnung nachliefern. Es wäre besser gewesen, ein belastbarerer Verordnungsentwurf hätte bei der Verabschiedung des Gesetzes vorgelegen. Denn erst die Verordnung legt fest, wer genau von dem Gesetz betroffen ist.

Die neuen Möglichkeiten des BSI, sich zu Sicherheitslücken in Soft- und Hardware öffentlich zu äußern, dürfen begrüßt werden. Ein „responsible Disclosure" ist die einzig sinnvolle Möglichkeit, einige Hersteller zum Handeln zu bewegen.

Die Umsetzungsfrist ist extrem ehrgeizig, wenn nicht zu kurz. Der Grundschutz-Zertifizierungsprozess geht nach Erreichen der Einstiegsstufe von einer Zwei-Jahrestaktung für die Aufbaustufe und das endgültige Zertifikat aus. Für Unternehmen und Behörden, die erst neu unter den Geltungsbereich des Gesetzes fallen, wird die Übergangsfrist zu kurz sein. Nur für Unternehmen und Behörden, die bereits zertifiziert sind oder sich regelmäßig auditieren lassen, ist die Übergangsfrist leicht zu schaffen.

Da derartige Prozesse häufig sehr beratungsintensiv sind, ist nach dem In-Kraft-Treten der Verordnung mit entsprechenden Engpässen – und damit auch mit steigenden Preisen – zu rechnen.

Eine Meldepflicht allein verbessert die IT-Sicherheit nicht. Erst wenn aus dem entstandenen Lagebild Maßnahmen werden, verbessert sich auch die IT-Sicherheit. Der Auftrag zur Schaffung von Mindeststandards ist da schon sehr viel wichtiger. Dass IT-Sicherheitsstandards nicht in Gesetzen und Verordnungen festgeschrieben werden, ist dabei der richtige Weg. Der sich aus den rasanten technischen Entwicklungen ergebende Änderungsbedarf ist mit den Zeitskalen, in denen der Gesetzgeber arbeitet, nicht zu vereinbaren. Der Gesetzgeber würde den technischen Entwicklungen ständig hinterher rennen.

Durchaus kritisch zu sehen, ist die Tatsache, dass doch etliche Bundesbehörden (§ 2 Abs. 3 Satz BSIG) von den technisch-organisatorischen IT-Sicherheitsvorgaben ausgenommen werden. Die vom Bundesministerium des Innern erlassenden Verwaltungsvorschriften mit Mindeststandards zur IT-Sicherheit haben für diese nur empfehlenden Charakter (§ 8 Abs.1 BSIG neu). Auch von der Meldepflicht sind Bundesbehörden gänzlich ausgenommen.

Insgesamt ist das IT-Sicherheitsgesetz ein Schritt in die richtige Richtung, der aber viele wichtige Details auslässt. Auch wenn die Definition gerade dieser Details kompliziert und anspruchsvoll ist, sollte der Gesetzgeber nicht darauf vertrauen, dass sich dies schon irgendwie regelt. Was genau sind *„erhebliche Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit"* der IT-Systeme, -Komponenten oder -Prozesse?

19 Marc Elsberg, BLACKOUT – Morgen ist es zu spät, Blanvalet Verlag, München (2012); siehe auch ergänzend: Arbeitsbericht Bericht Nr. 141 des Büros für Technikfolgenabschätzung des Deutschen Bundestages (TAB) http://www.tab-beim-bundestag.de/de/pdf/publikationen/berichte/TAB-Arbeitsbericht-ab141.pdf; abgerufen am 29.6.2015.

20 Http://www.zdf.de/ZDF/zdfportal/blob/38806248/1/data.pdf; abgerufen am 13.6.2015.

Prof. Dr. Rainer W. Gerling

Prof. Dr. Rainer W. Gerling ist IT-Sicherheitsbeauftragter der Max-Planck-Gesellschaft und Honorarprofessor für IT-Sicherheit an der Hochschule München. Er studierte Physik an der TU Dortmund und promovierte und habilitierte an der Universität Erlangen-Nürnberg. Über 20 Jahre war er der Datenschutzbeauftragte der Max-Planck-Gesellschaft. Er ist stellvertretender Vorsitzender der GDD und war langjähriger Leiter des Erfa-Kreises Bayern.

Dr. Stefan Brink

Datenschutzgerechte Nutzung von Informations- und Kommunikationstechnik im Unternehmen

Aufsichtsbehördliche Positionen zur IuK-Nutzung und ihrer Kontrolle am Arbeitsplatz

Kaum eine Thematik betrifft so viele Beschäftigte an ihrem Arbeitsplatz wie die Nutzung – und Kontrolle! – betrieblicher Informations- und Kommunikationstechnik (IuK). Arbeitgeber, deren Beschäftigte IuK gleichermaßen zu betrieblichen oder privaten Zwecken nutzen, erheben und verarbeiten dabei personenbezogene Daten der Beschäftigten selbst sowie ihrer inner- und außerbetrieblichen Kommunikationspartner. Dabei haben die Arbeitgeber datenschutzrechtliche Anforderungen zu beachten, die sich je nach Kommunikationszweck, -partner und -mittel unterscheiden und insbesondere davon abhängen, ob den Beschäftigten neben der betrieblichen auch die private Nutzung der betrieblichen IuK ganz oder teilweise am Arbeitsplatz gestattet ist.

In der Praxis herrscht auf Grund der Vielfältigkeit der Nutzungs- und Überwachungsmöglichkeiten einerseits und der Differenziertheit der Rechtslage andererseits erhebliche Unsicherheit. Die Aufsichtsbehörden für den Datenschutz treffen regelmäßig auf Unternehmen, die trotz ihres Bemühens um faire und akzeptable Nutzungsbedingungen für die betriebliche IuK gravierende, teilweise sogar strafrechtlich relevante Fehler begehen. Andererseits kennen viele Beschäftigte häufig nicht die Grenzen zulässiger Nutzungen und fühlen sich verunsichert; auch Betriebsräte suchen immer häufiger den Rat der Aufsichtsbehörde.

Die dabei ausgesprochenen Empfehlungen der jeweiligen Datenschutzbehörden sind zwar differenziert, lassen sich aber in vielen Bereichen zusammenführen. Zwar bleibt die Vorlage einer einheitlichen und übergreifenden Orientierungshilfe aller Aufsichtsbehörden weiter ein Desiderat, eine überblicksartige Zusammenstellung der wesentlichen Aspekte der IuK-Nutzung und -Kontrolle am Arbeitsplatz ist aber schon jetzt möglich.

I. Zur Rechtslage

1. Zur Erhebung, Verarbeitung und Nutzung personenbezogener IuK-Daten

Im Betrieb wird den Beschäftigten heute standardmäßig an ihrem Arbeitsplatz Informations- und Kommunikationstechnik (IuK) wie Telefon, E-Mail und Internetzugang zur Nutzung bereit gestellt. Arbeitgeber, deren Beschäftigte IuK (zu betrieblichen oder privaten Zwecken) nutzen, erheben und verarbeiten dabei Daten der Beschäftigten selbst sowie ihrer inner- und außerbetrieblichen Kommunikationspartner und weiterer Betroffener. Diese Daten werden – abgesehen von den Sonderfällen betrieblicher Geheimnisträger (z.B. Betriebsrat, Betriebsarzt, Gleichstellungsbeauftragte oder betrieblicher Datenschutzbeauftragter, vgl. unten I.6) – nicht anonymisiert erhoben, verarbeitet und genutzt, sondern als Einzelangaben über IuK-Nutzungsverhalten bestimmter, jedenfalls aber für den Arbeitgeber bestimmbarer natürlicher Personen (vgl. § 3 Abs. 1 Bundesdatenschutzgesetz – BDSG) verwendet.

Diese personenbezogenen Daten über die Nutzung der betrieblichen IuK (IuK-Nutzerdaten) werden durch unterschiedliche Gesetze geschützt, welche die Zugriffs- und Nutzungsbefugnis des Arbeitgebers einschränken. Neben dem BDSG sind dabei insbesondere das Telekommunikationsgesetz (TKG) und das Telemediengesetz (TMG) einschlägig. Welche dieser Normen im Einzelfall zur Anwendung gelangt, bestimmt sich nach ihrem Anwendungsbereich (dazu sogleich unter 2.) und einschlägigen Kollisionsregeln. So bestimmt § 1 Abs. 3 Satz 1 BDSG, dass „andere Rechtsvorschriften des Bundes" zu personenbezogenen Daten dem BDSG vorgehen. Soweit die Anwendungsbereiche von TKG und TMG also eröffnet sind, haben deren Regelungen Vorrang vor dem BDSG.

Zu dieser durchaus komplexen Rechtslage tritt eine Praxis, bei der aufgrund der Vielfältigkeit der Nutzungs- und Überwachungsmöglichkeiten erhebliche Unsicherheit herrscht. Die Aufsichtsbehörden für den Datenschutz[1] treffen regelmäßig auf Unternehmen, die trotz ihres Bemühens um faire und akzeptable Nutzungsbedingungen für die betriebliche IuK gravierende, teilweise sogar strafrechtlich relevante Fehler begehen. Andererseits kennen viele Beschäftigte häufig nicht die Grenzen zulässiger Nutzungen und fühlen sich unsicher, weil sie vermuten, dass ihnen der Arbeitgeber oder die EDV bei der IuK-Nutzung am Arbeitsplatz „über die Schulter guckt" oder gar ihre private Kommunikation ausspäht. Betriebsräte schließlich suchen immer häufiger den Rat der Aufsichtsbehörde, weil sie zur IuK-Nutzung Betriebsvereinbarungen abschließen oder bestehende prüfen lassen wollen. In allen diesen Fällen sind die Datenschutz-Aufsichtsbehörden nicht nur Kontrollorgane, sondern zugleich zu Beratung und Unterstützung berufen[2]. Diese Beratungen beziehen sich zwar schwer-

1 Vgl. die Orientierungshilfen des ULD https://www.datenschutzzentrum.de/internet/private-und-dienstliche-internetnutzung.pdf (Stand 4/2014) und des BfDI https://www.bfdi.bund.de/SharedDocs/Publikationen/Arbeitshilfen/LeitfadenInternetAmArbeitsplatzneu.pdf;jsessionid=0883803AA925E3755034DA2774959D37.1_cid329?__blob=publicationFile&v=3 (Stand 1/2008)

2 Vgl. § 38 Abs. 1 BDSG.

punktmäßig auf das BDSG, müssen aber bereits aus Gründen der Abgrenzung hiervon auch die Vorschriften des TKG und des TMG mit einbeziehen.

2. Anwendungsbereiche des Telekommunikationsgesetzes (TKG) und des Telemediengesetzes (TMG)

Arbeitgeber, deren Beschäftigte die betriebliche IuK zu betrieblichen oder privaten Zwecken nutzen, haben bei der Verwendung anfallender personenbezogener IuK-Daten der Beschäftigten und weiterer Betroffener die Vorgaben des TKG und des TMG zu beachten.

a) Schutzzwecke von TKG und TMG

TKG und TMG bezwecken insbesondere den Schutz des traditionellen Fernmeldegeheimnisses, das sich vom Brief-/Postgeheimnis zum Telekommunikationsgeheimnis fortentwickelt hat und in Artikel 10 des Grundgesetzes (GG) mit Verfassungsrang garantiert ist. Die Kommunikationsfreiheit des Art. 10 GG gewährleistet zum einen, mit einem selbst bestimmten Personenkreis zu kommunizieren, und zum anderen, die Vertraulichkeit dieses Informations- und Gedankenaustauschs zu wahren[3]. Diese Vertraulichkeit der Kommunikation ist besonders dann gefährdet, wenn die Kommunikation nicht zwischen Anwesenden, sondern über räumliche Distanz erfolgt und so auf die Übermittlung durch Dienstleister der Post oder für Telekommunikation angewiesen ist[4]. Nicht nur der Dienstleister, auch andere Dritte könnten diesen erleichterten Zugriff auf die Kommunikation ausnutzen. Art. 10 GG soll einen Ausgleich für die technisch bedingte Einbuße an Privatheit schaffen und erstreckt sich auf den gesamten Kommunikationsinhalt und deren Umstände sowie auf den gesamten Übermittlungsvorgang. Erst mit Beendigung der Übermittlung sind die übermittelten, im alleinigen Herrschaftsbereich des Kommunikationsteilnehmers gespeicherten Informationen nicht mehr vom Fernmeldegeheimnis erfasst. Jetzt kann er eigene Schutzvorkehrungen gegen die unerwünschte Kenntnisnahme durch Dritte treffen und bedarf nicht mehr des gesetzlichen Schutzes.

b) Abgrenzung von TKG und TMG

Die Anwendungsbereiche dieser Gesetze lassen sich wie folgt abgrenzen: Während das TKG die Telekommunikation, also den technischen Vorgang des Aussendens, Übermittelns und Empfangens von Signalen mittels Telekommunikationsanlagen reguliert (§ 3 Nr. 22 TKG) und dabei insbesondere die Vertraulichkeit der Kommunikationsinhalte schützt, stehen im TMG die als Dienstleistung angebotenen Telemedien im Vordergrund (§ 1 Abs. 1 TMG). Zu den Telemedien gehören (nahezu) alle Angebote im Internet, insbesondere auch Suchmaschinen, Webmail-Dienste, Informationsdienste, Podcasts und Chatrooms. Hier werden zwar auch Signale mittels Telekommunikation ausgetauscht, weitere Dienste stehen jedoch im Vordergrund: Beim Surfen im Internet sind dies etwa Such- oder Downloadmöglichkeiten, das Merken bestimmter Seiten (Favoriten) oder besuchter Seiten (Chronik), beim Mailen sind dies Textverarbeitungsmöglichkeiten, die Speicherung empfangener oder gesendeter Mails oder Suchfunktionen.

Bei der Internet- und E-Mail-Nutzung am Arbeitsplatz handelt es sich also häufig um IuK-Dienste, die in der Übertragung von Signalen über Telekommunikationsanlagen – also dem Transport von Daten nach dem TKG – bestehen, aber sich darin nicht erschöpfen müssen (vgl. § 1 Abs. 1 TMG). Sofern darüber hinaus Telemedien zur Nutzung bereitgehalten werden (vgl. § 2 Nr. 1 TMG), unterfällt dies dem TMG. Telefonie als Teil betrieblicher IuK unterfällt demgegenüber regelmäßig dem TKG.

c) Das Fernmeldegeheimnis des § 88 TKG

Dem verfassungsrechtlich garantierten Fernmeldegeheimnis des Art. 10 GG unterfallen zunächst nur staatliche Stellen (Art. 1 Abs. 3 GG). Weil Kommunikation in der Regel aber auf die Übermittlung durch (auch private) Dritte angewiesen ist, werden alle Anbieter, die Telekommunikationsdienste erbringen, nach § 88 Abs. 2 Satz 1 TKG dem Fernmeldegeheimnis unterworfen. So genügt der Gesetzgeber seiner Schutzpflicht gegenüber allen Telekommunikationsteilnehmern.

Dem einfachgesetzlichen Fernmeldegeheimnis des § 88 TKG unterliegen der Inhalt der Telekommunikation und ihre näheren Umstände, insbesondere die Tatsache, ob jemand an einem Telekommunikationsvorgang beteiligt ist oder war (§ 88 Abs. 1 Satz 1 TKG). Zur Wahrung des Fernmeldegeheimnisses ist jeder Diensteanbieter verpflichtet (§ 88 Abs. 2 Satz 1 TKG). Diensteanbieter ist jeder, der ganz oder teilweise geschäftsmäßig Telekommunikationsdienste erbringt oder an der Erbringung solcher Dienste mitwirkt (§ 3 Nr. 6 TKG). Nach § 3 Nr. 10 TKG bedeutet „geschäftsmäßiges Erbringen von Telekommunikationsdiensten" das nachhaltige Angebot von Telekommunikation für Dritte mit oder ohne Gewinnerzielungsabsicht.

Das gegen den Diensteanbieter gerichtete Fernmeldegeheimnis untersagt es diesem, sich oder anderen über das für die geschäftsmäßige Erbringung der Telekommunikationsdienste einschließlich des Schutzes ihrer technischen Systeme erforderliche Maß hinaus Kenntnis vom Inhalt oder den näheren Umständen der Telekommunikation zu verschaffen (§ 88 Abs. 3 Satz 1 TKG).

§ 88 TKG gilt nach § 7 Abs. 2 Satz 3 TMG auch für Diensteanbieter nach dem TMG. Diese sind nach § 2 Nr. 1 TMG Personen, die eigene oder fremde Telemedien zur Nutzung bereithalten oder den Zugang zur Nutzung vermitteln. Die Bereitstellung eines Telefons, eines Internet-Zugangs oder eines Webmail-Dienstes in Gestalt eines personalisierten betrieblichen E-Mail-Accounts (z.B. Frank.Stein@Unternehmen.com) durch den Arbeitgeber für die Arbeitnehmer stellt grundsätzlich ein solches Angebot von Telekommunikationsdiensten bzw. Telemediendiensten dar. Allerdings ist der Beschäftigte dann für den Arbeitgeber kein „Dritter", wenn er diese Dienste ausschließlich zu betrieblichen Zwecken nutzen soll, denn dann nimmt er

3 Durner, in: Maunz/Dürig, GG, 2013, Art. 10 GG Rn. 42; Pagenkopf, in: Sachs, GG, 2011, Art. 10 Rn. 8; Hermes, in: Dreier, GG, 2013, Art. 10 Rn. 15.

4 Vgl. Durner, in: Maunz/Dürig, GG, 2013, Art. 10 GG Rn. 43; Hermes, in: Dreier, GG, 2013, Art. 10 Rn. 15.

diese Dienste für den Arbeitgeber und wie dieser in Anspruch. Dann ist der Arbeitgeber seinen Beschäftigten gegenüber kein Diensteanbieter, die Kommunikation unterfällt nicht dem Fernmeldegeheimnis des § 88 TKG.

d) Der Arbeitgeber als Diensteanbieter

Dies ist jedoch dann anders zu beurteilen, wenn der Beschäftigte die Telekommunikationsdienste nicht (nur) für den Arbeitgeber nutzen darf, sondern dieser deren Nutzung auch für eigene Zwecke des Arbeitnehmers freigegeben hat. Dann erbringt der Arbeitgeber nach § 3 Nr. 10 TKG geschäftsmäßig – nicht notwendig entgeltlich – Telekommunikationsdienste, indem er das nachhaltige Angebot von Telekommunikation für Dritte mit oder ohne Gewinnerzielungsabsicht macht.

Ob der Arbeitgeber ein solches Angebot macht, obliegt (zunächst) seiner eigenen Entscheidung. Da es sich bei den vom Arbeitgeber zur Verfügung gestellten Telekommunikations- und -mediendiensten um Betriebsmittel handelt, darf er die Nutzung dieser Dienste durch Beschäftigte grundsätzlich auf die betriebliche Tätigkeit beschränken. Ihre Nutzung für private Zwecke ist erst erlaubt, wenn der Arbeitgeber die Privatnutzung ausdrücklich z.B. im Arbeitsvertrag oder in einer Betriebsvereinbarung gestattet hat. Will der Arbeitgeber die gewährte private Nutzungsmöglichkeit wieder entziehen, bedarf es einer Änderungskündigung (zu Betriebsvereinbarungen vgl. § 77 Abs. 5 BetrVG) bzw. Änderungsvereinbarung.

Stellt ein Arbeitgeber seinen Beschäftigten einen Internet-Zugang und/oder ein personalisiertes E-Mail-Postfach zur Verfügung, ohne Regelungen zur Zulässigkeit der privaten Nutzung zu treffen oder überwacht er ein Verbot der privaten Nutzung nicht ausreichend, so kann dies aus Sicht des Beschäftigten als Erlaubnis gedeutet werden und dazu führen, dass eine Gestattung der privaten Nutzung gegebenenfalls sogar in Form einer sog. „betrieblichen Übung" vorliegt. Dies steht im Ergebnis einer ausdrücklichen Erlaubnis der privaten Nutzung gleich. Von einer betrieblichen Übung spricht man dann, wenn ein Arbeitnehmer aus der regelmäßigen Wiederholung bestimmter Verhaltensweisen des Arbeitgebers einen konkreten Verpflichtungswillen des Arbeitgebers ableiten kann, ihm solle eine Leistung oder Vergünstigung auf Dauer gewährt werden. Will der Arbeitgeber eine durch betriebliche Übung eingeräumte private Nutzungsmöglichkeit wieder entziehen, bedarf es ebenfalls der Änderungskündigung.

Wenn ein Arbeitgeber den Beschäftigten die private Nutzung von IuK erlaubt, ist er nach Auffassung der Aufsichtsbehörden ihnen gegenüber *Telekommunikations- bzw. Telemediendienste-Anbieter* mit der Konsequenz, dass er an das Fernmeldegeheimnis des § 88 Absatz 2 Satz 1 Telekommunikationsgesetz (TKG; i.V.m. § 7 Abs. 2 S. 3 Telemediengesetz [TMG]) gebunden ist und sich bei Verletzung des Fernmeldegeheimnisses einer Strafbarkeit nach § 206 Strafgesetzbuch (StGB) aussetzen kann. Dass der Arbeitgeber ggf. auch Drittunternehmen als Zugangsanbieter (Access Provider) zum Diensteangebot einschaltet, ist dabei unerheblich. Gegenüber den privat nutzenden Beschäftigten sind die Provider lediglich Auftragnehmer des als Anbieter zu qualifizierenden Arbeitgebers.

Der nach wie vor weitgehend herrschende Konsens[5], dass Arbeitgeber, welche die private Nutzung der betrieblichen IuK erlauben, als Diensteanbieter an das Fernmeldegeheimnis gebunden sind[6], ist auch von der Gesetzeshistorie getragen[7] und wird durch abweichende Ansichten einzelner Gerichte und Stimmen in der Literatur[8] letztlich nicht in Frage gestellt. Überzeugende Gegenargumente werden nicht vorgetragen. Praktisch relevant ist dieser zur Streitfrage heraufstilisierte Einzelaspekt zudem nur für die Strafbarkeit des Arbeitgebers. Die hier interessierenden Fragen der Verwendung der IuK-Daten zu unterschiedlichen Zwecken wird nach Maßgabe der datenschutzrechtlichen Regelungen des TKG/TMG, bei abweichender Auffassung nach denen des gleich gerichteten BDSG entschieden.

e) Grenzen des Fernmeldegeheimnisses

Das Fernmeldegeheimnis gilt nicht unbeschränkt, in ihren Anwendungsbereichen kennen sowohl das TKG als auch das TMG gesetzliche Grenzen, sei es in § 88 TKG selbst (vgl. aa), sei es in den datenschutzrechtlichen Bestimmungen von TKG (vgl. bb) und TMG (vgl. cc). Daneben sind die zeitlichen Grenzen des Fernmeldegeheimnisses zu beachten (vgl. dd). Schließlich kann das Fernmeldegeheimnis durch Einwilligung des/der Betroffenen aufgehoben werden (vgl. ee)

aa) § 88 Abs. 3 TKG

Schon § 88 TKG räumt in Abs. 3 den Diensteanbietern die Befugnis ein, sich Kenntnis vom Inhalt oder den näheren Umständen der Telekommunikation zu verschaffen, soweit die geschäftsmäßige Erbringung der Telekommunikationsdienste einschließlich des Schutzes ihrer technischen Systeme dies erfordert.

aaa) Virenfilter

Aus Gründen der Datensicherheit dürfen etwa Teilinhalte oder Anlagen von E-Mails unterdrückt werden, wenn sie Inhalte aufweisen, die zu Sicherheitsrisiken auf Rechnern oder im Netzwerk führen können (Virenfilterung). Dies setzt voraus, dass konkrete und dokumentierbare Anhaltspunkte dafür vorliegen, dass bei der Verbreitung der Viren Störungen oder Schäden der Telekommunikations- und Datenverarbeitungssysteme eintreten. Wird die Untersuchung von virenverseuchten E-Mails von der Kenntnisnahme des Inhalts der E-Mail, etwa durch den Systemadministrator, begleitet, so ist der Adressat, also der Beschäftigte, einzubeziehen (vgl. § 33 BDSG).

5 Vgl. Seifert, in Simitis: BDSG, 8. Aufl. 2014, § 32 Rn. 90; Gola/Schomerus, BDSG, 11. Aufl. 2012, § 32 Rn. 18; Hassemer in Weth/Herberger/Wächter, Daten- und Persönlichkeitsschutz im Arbeitsverhältnis, 2014, 549, 571 Rn. 91.

6 Z.B. Stamer/Kuhnke, in: Plath, BDSG, 2013, § 32 Rn. 79; Seifert, in: Simitis, BDSG, § 32 Rn. 92; Zöll, in: Taeger/Gabel BDSG, 2010, § 32 Rn. 34; Sassenberg/Mantz, BB 2013, S. 889; Panzer-Heemeier, DuD 2012, S. 48 (50).

7 BT-Drs. 13/3609, 33 (53).

8 Hessischer VGH, Beschluss vom 19.5.2009, AZ: 6 A 2672/08.Z; LAG Niedersachsen, 31.5.2010, AZ: 12 Sa 875/09; LAG Berlin-Brandenburg, 16.2.2011, AZ: 4 Sa 2132/10; VG Karlsruhe, 27.5.2013, AZ: 2 K 3249/12; VGH Baden-Württemberg, 30.7.2014, 1 S 1352/2013; Wybitul, NJW 2014, 3605 ff. m.w.N.

bbb) Spamfilter

Davon zu unterscheiden ist die Ausfilterung bzw. Veränderung von an den Beschäftigten adressierten „Spam-Mails", also unerwünschte Zusendungen mit zumeist werbendem Inhalt. Diese gefährden nicht das technische System selbst, sondern die Nützlichkeit des Kommunikationsmittels E-Mail, wenn aufgrund der Vielzahl von Spam-Mails relevante Nachrichten für den Empfänger nur noch schwer erkennbar sind. Hier greift § 88 Abs. 3 TKG nicht als Befugnisnorm, bei Herausfilterung und/oder Löschung droht ein Eingriff ins Fernmeldegeheimnis bzw. eine strafbare Unterdrückung von Daten (§ 206 Abs. 1 und Abs. 2 Nr. 2, § 303 a StGB). Bei gestatteter privater Nutzung schließt eine Einwilligung in die Filterung von E-Mail die Strafbarkeit aus; umstritten ist allerdings, ob dafür die Einwilligung des Empfängers ausreicht oder auch der Absender zustimmen muss.

Generell sind die Beschäftigten darüber zu unterrichten, wenn an sie gerichtete oder von ihnen abgesendete E-Mails ganz oder teilweise unterdrückt werden oder virenverseucht sind (§ 33 BDSG). Die Information allein des Betriebsrats genügt hingegen nicht, kann jedoch auf Grundlage einer Betriebsvereinbarung erfolgen.

bb) Telekommunikationsdatenschutzrecht (§§ 91-107 TKG)

Nach § 97 Abs. 1 TKG dürfen Verkehrsdaten von Nutzern verwendet werden, soweit die Daten zur Ermittlung des Entgelts und zu dessen Abrechnung benötigt werden. Diese Einschränkung des Fernmeldegeheimnisses spielt in der Praxis der IuK-Nutzung am Arbeitsplatz eine untergeordnete Rolle. War die Nutzung des Diensttelefons in früheren Zeiten noch kostenpflichtig, so ist in Zeiten von Flatrates der Zugriff aufs IuK in aller Regel kostenfrei. Damit scheidet eine Nutzung der Verkehrsdaten für den Arbeitgeber aber aus. Sie sind vom Diensteanbieter nach Beendigung der Verbindung unverzüglich zu löschen (§ 96 Abs. 1 Satz 3 TKG). Eine Erhebung oder Verwendung der Verkehrsdaten zu anderen Zwecken ist unzulässig (§ 96 Abs. 2 TKG).

Das Gleiche gilt für die Regelung des § 100 Abs. 3 TKG, der zur Sicherung des Entgeltanspruchs gegen die rechtswidrige Inanspruchnahme des Telekommunikationsdienstes eine Verwendung der Bestands- und Verkehrsdaten erlaubt.

Allerdings gestattet es § 100 Abs. 1 TKG dem Diensteanbieter, zum Erkennen, Eingrenzen oder Beseitigen von Störungen oder Fehlern an Telekommunikationsanlagen die Bestands- und Verkehrsdaten der Nutzer zu erheben und zu verwenden. Für diesen Zweck kann daher die Protokollierung der Internetnutzung an der Firewall oder durch ein Überwachungsprogramm zulässig sein.

Die Verarbeitung von Standortdaten (§ 3 Nr. 19 TKG) – etwa eines mobilen Endgerätes – ist nach § 98 Abs. 1 TKG (nur) auf Einwilligungsbasis zulässig und erfordert die jeweilige Benachrichtigung des Nutzers (§ 98 Abs. 1 Satz 2 TKG).

cc) Telemediendatenschutzrecht (§§ 11-15 TMG)

Gestattet der Arbeitgeber die private Nutzung betrieblicher Telemedien, so ist er ein „Diensteanbieter" im Sinne des TMG (vgl. § 2 Nr. 1 TMG), der Arbeitnehmer ist „Nutzer" (§ 2 Nr. 3 TMG). Die datenschutzrechtlichen Vorschriften des TMG sind dann anwendbar, soweit die IuK-Nutzung nicht nur ausschließlich zu betrieblichen Zwecken erfolgt (vgl. § 11 Abs. 1 Nr. 1 TMG). Ist letzteres der Fall, kommt subsidiär das BDSG zur Anwendung.

Im Geltungsbereich des TMG darf der Diensteanbieter personenbezogene Daten zur Bereitstellung von Telemedien nur erheben und verwenden, soweit dieses Gesetz oder eine andere Rechtsvorschrift, die sich ausdrücklich auf Telemedien bezieht, es erlaubt oder der Nutzer eingewilligt hat (§ 12 Abs. 1 TMG). Danach ist die Protokollierung der privaten Nutzung nur zulässig, soweit sie die Inanspruchnahme des Telemediums ermöglicht oder zu Abrechnungszwecken erforderlich ist (§ 15 Abs. 1 TMG). Letzteres ist regelmäßig nicht der Fall, da die Nutzung betrieblicher Telemedien zumeist kostenlos erfolgt. Im Übrigen hat der Diensteanbieter durch technische und organisatorische Vorkehrungen sicherzustellen, dass die anfallenden personenbezogenen Daten über den Ablauf des Zugriffs unmittelbar nach dessen Beendigung gelöscht werden (§ 13 Abs. 4 Nr. 2 TMG).

Damit steht die Einwilligung des Nutzers beim Zugriff auf IuK-Daten im Vordergrund.

dd) Zeitliche Grenzen des Fernmeldegeheimnisses

Solange der Kommunikationsvorgang dauert, unterfällt er dem Fernmeldegeheimnis. Auch nach seiner Beendigung sind Informationen über die Umstände der Kommunikation, die beim Diensteanbieter gespeichert sind, nach Maßgabe des TKG/TMG geschützt (Verwendungsverbote). Die Nutzung dieser Daten lässt sich nur unter Rückgriff auf Ermächtigungsgrundlagen des TKG/TMG rechtfertigen. Informationen, die nach Beendigung des Kommunikationsvorgangs bei den Kommunikationspartnern verbleiben (der vom Empfänger geöffnete Brief, die gelesene E-Mail in seinem Postfach) unterfallen nicht mehr dem Fernmeldegeheimnis. Der Zugriff auf diese Informationen ist – mangels anderweitig einschlägiger Rechtsgrundlage – an den Bestimmungen des BDSG zu messen.

Dies gilt insbesondere für den Zugriff auf das E-Mail-Postfach des Arbeitnehmers. Bei der E-Mail-Nutzung, die sich als zeitlich gestreckte Kommunikation beschreiben lässt, sind dabei die folgenden Unterscheidungen zu beachten:

Solange eine E-Mail noch im Kommunikationsaustausch begriffen ist, ist ein Zugriff nur im Einklang mit spezialgesetzlichen Eingriffsvoraussetzungen des TKG/TMG möglich. Erst wenn die E-Mail beim Empfänger angekommen und sich im ausschließlichen Herrschaftsbereich des Betroffenen befindet – also insbesondere von ihm gelöscht werden könnte –, der Übertragungsvorgang also beendet ist, greift das Fernmeldegeheimnis nicht mehr.

Dieser Umstand ist im Arbeitgeber-Arbeitnehmerverhältnis jedoch regelmäßig nicht gegeben. Zum einen weil der Arbeitgeber in der Praxis eine Kopie der E-Mail auf seinem Zentral-Server gespeichert hat, zum anderen weil der Arbeitnehmer bei einem Dienst-PC nicht die gleiche Dispositionsbefugnis hat, wie bei seinem privaten PC und häufig E-Mails nicht endgültig löschen kann.

Der Schutz des Fernmeldegeheimnisses endet in diesen Fällen daher nicht, er erstreckt sich auch auf E-Mails, die auf einem Server des Diensteanbieters zwischen- oder endgespeichert sind. Es gilt damit auch beim „ruhenden" E-Mail-Verkehr, bei dem ein Telekommunikationsvorgang in einem dynamischen Sinn zwar nicht (mehr) stattfindet, er aber auch noch nicht abgeschlossen ist (BVerfG, Beschluss vom 16. Juni 2009 – 2 BVR 902/06 –). Abgeschlossen ist der schutzbedürftige Telekommunikationsvorgang erst dann, wenn der Kommunikationsteilnehmer dergestalt die alleinige Herrschaft über ihn erlangt hat, dass er selbst jederzeit und unabhängig vom Diensteanbieter die Teile und Ergebnisse der Kommunikation in seinem Herrschaftsbereich vernichten könnte.

ee) Die Einwilligung des Beschäftigten

Bieten TKG/TMG keine Ermächtigungsgrundlage, die dem Arbeitgeber einen Zugriff auf IuK-Daten des Mitarbeiters gestatten könnte, so kann ein Zugriff doch mit Einwilligung des Beschäftigten erfolgen[9].

Zwar fehlt es dem TKG an § 4a BDSG vergleichbaren Normen, die den Umgang mit personenbezogenen Daten auf Grundlage einer Einwilligung gestatten. Die Möglichkeit einer wirksamen Einwilligung im Anwendungsbereich von TKG ergibt sich jedoch bereits aus der Dispositivität des Fernmeldegeheimnisses[10] und wird in einzelnen Vorschriften des TKG vorausgesetzt (vgl. §§ 94, 95 Abs. 5 TKG). Hinsichtlich der an eine Einwilligung zu stellenden Anforderungen kann auf § 4a BDSG zurückgegriffen werden, die bestehende Regelungslücke der §§ 91 ff. TKG löst die Subsidiarität des BDSG nicht aus (§ 1 Abs. 3 BDSG)[11]. § 12 Abs. 1 TMG sieht demgegenüber die Datenverwendung aufgrund Einwilligung ausdrücklich vor.

Eine Aufhebung des Fernmeldegeheimnisses durch eine Betriebsvereinbarung ist hingegen nicht möglich, da insoweit Individualrechte der einzelnen Arbeitnehmer in Rede stehen. Über diese disponiert der einzelne Arbeitnehmer, nicht der Betriebsrat (es sei denn – was jedoch unpraktisch wäre – jeder einzelne Arbeitnehmer ermächtigt den Betriebsrat hierzu).

IuK-Daten sind allerdings nur dann für den Arbeitgeber zugänglich, wenn die Einwilligung sämtlicher Kommunikationspartner vorliegt. Auch der oder die Kommunikationspartner des Arbeitnehmers müssen zuvor wirksam auf den Schutz des Fernmeldegeheimnisses verzichtet haben. Dies erfordert dessen bzw. deren Einwilligungserklärung, die formfrei – auch mündlich – wirksam abgegeben werden kann, zu Nachweiszwecken aber dokumentiert werden sollte. Ohne eine solche Erklärung darf der Arbeitgeber also nur auf Daten zurückgreifen, wenn es um betriebliche Kommunikation zwischen Beschäftigten seines Betriebes geht und die Privatnutzung untersagt ist.

Die grundsätzliche Problematik mangelnder Freiwilligkeit von Einwilligungen in Arbeitsverhältnissen[12], die die immer auch soziale Abhängigkeitsverhältnisse sind, stellt sich bei Einwilligungen in die Aufhebung oder Begrenzung des Fernmeldegeheimnisses nicht. Da der Arbeitgeber die private Nutzung nicht zulassen muss, stellt seine entsprechende Bereitschaft eine Ausweitung der Handlungsmöglichkeiten der Arbeitnehmer dar, die ihre Entscheidungsfreiheit nicht einschränkt. Anders wäre dies nur, wenn die Arbeitnehmer auf die Privatnutzung aufgrund arbeitsvertraglicher Regelung oder betrieblicher Übung bereits einen arbeitsrechtlichen Anspruch hätten – dann ist für Einwilligungserklärungen kein Raum mehr.

Da der Arbeitgeber bei der Erlaubnis der privaten Nutzung seiner IuK frei ist, kann er diese Erlaubnis an einschränkende Voraussetzungen knüpfen. So kann er insbesondere die Erlaubniserteilung an die Bedingung knüpfen, dass der Beschäftigte in die Einschränkung seines Fernmeldegeheimnisses einwilligt. So kann der Arbeitgeber zulässige Nutzungsarten vorgeben und sich Rechte zur Datenverwendung zu Kontrollzwecken einräumen lassen. Auch kann er beispielsweise festlegen, dass die private Nutzung nur in den Arbeitspausen oder nach Dienstende erfolgen darf.

Allerdings muss der Arbeitgeber als Diensteanbieter nach dem TKG/TMG den Beschäftigten transparent erklären, auf welche Art und Weise eine Kontrolle des Umfangs der privaten Nutzung stattfindet (vgl. § 93 TKG, Grundsatz der Transparenz).

3. Abgrenzung der Anwendungsbereiche von TKG/TMG/BDSG

Die Anwendungsbereiche von TKG/TKG einerseits und BDSG andererseits lassen sich hinsichtlich der Nutzung betrieblicher IuK durch Beschäftigte zu betrieblichen bzw. auch privaten Zwecken wie folgt voneinander abgrenzen:

a) Verbot der privaten IuK-Nutzung

Gestattet der Arbeitgeber die Nutzung der betrieblichen IuK ausschließlich zu betrieblichen Zwecken, richtet sich die Erhebung, Verarbeitung und Nutzung von Daten über das Nutzungsverhalten der Beschäftigten nach dem Bundesdatenschutzgesetzes (BDSG) unter Berücksichtigung der jeweils einschlägigen Vorschriften zur Regelung des Arbeitsverhältnisses (dazu unter 4.).

b) Gestattung der privaten IuK-Nutzung

Sobald ein Arbeitgeber seinen Beschäftigten die private Nutzung von IuK ganz oder teilweise erlaubt, erbringt er ihnen gegenüber geschäftsmäßig Telekommunikationsdienste (§ 3 Nr. 6 TKG) bzw. Telemediendienste (§ 2 Nr. 1 TMG) und ist somit zur Einhaltung des Fernmeldegeheimnisses verpflichtet. Die Speicherung und Nutzung von Verkehrs- bzw. Nutzungsdaten ist danach grundsätzlich nur zu Abrechnungszwecken erlaubt; auf Kommunikationsinhalte darf nicht zugegriffen werden. Weitergehende Verwendungen von IuK-Daten sind nur mit Einwilligung des Beschäftigten zulässig. Diese Einwilli-

9 Jenny, in: Plath, BDSG, 2013, § 88 TKG Rn. 11.

10 Elschner, in: Hoeren/Sieber/Holznagel, Multimedia-Recht, 2014, Teil 22.1 Rn. 88; Eckhardt, in: Spindler/Schuster, Recht der elektronischen Medien, 2011, § 94 TKG Rn. 2.

11 Elschner, in: Hoeren/Sieber/Holznagel Multimedia-Recht, 2014, Teil 22.1 Rn. 89; vgl. allgemein zum Verhältnis des BDSG zum TKG Munz, in: Taeger/Gabel, BDSG, 2010, § 88 TKG Rn. 7.

12 Vgl. zum Streitstand Riesenhuber, in: Wolff/Brink, Datenschutzrecht in Bund und Ländern, 2013, § 32 Rn. 35 ff.

gungserklärung kann durch eine Betriebsvereinbarung zwar nicht ersetzt werden, dennoch empfiehlt es sich, über die Nutzung der betrieblichen IuK und die zulässigen Kontrollmaßnahmen eine Betriebsvereinbarung abzuschließen (vgl. dazu unter II.)

Die Aufsichtsbehörden verfolgen das Ziel, eine Muster-Betriebsvereinbarung zur IuK-Nutzung vorzulegen.

Ohne wirksame Einwilligung des Beschäftigten sperrt sich der Arbeitgeber also vom Zugriff auf die IuK-Daten vollständig aus – auch von denen aus betrieblicher Kommunikation, sofern er diese nicht eindeutig von privater unterscheiden kann. Damit schafft er durch die Gestattung der Privatnutzung eine prinzipiell inakzeptable Situation für seinen Betrieb und seine eigenen Interessen.

4. Das Regelungsregime des BDSG

Das BDSG kommt wie gezeigt zur Anwendung, soweit TKG und TMG nicht einschlägig sind – etwa falls nur die betriebliche Nutzung der betrieblichen IuK gestattet ist – oder Regelungslücken enthalten, die eine Subsidiarität des BDSG nach § 1 Abs. 3 nicht auslösen. Darüber hinaus ist das BDSG als höherrangiges Recht Maßstab für Betriebsvereinbarungen zur Datenverwendung aus der IuK-Nutzung und ist bei der Beurteilung der Wirksamkeit von Einwilligungen heranzuziehen.

Überlässt der Arbeitgeber den Beschäftigten die betriebliche IuK alleine zur betrieblichen Nutzung und schließt er, etwa durch entsprechende wiederholte und auf ihre Einhaltung hin kontrollierte Weisungen, eine gegenläufige betriebliche Übung aus, so wird er nicht zum Anbieter von Telekommunikations- oder Telemediendiensten. Dies erlaubt es ihm, ohne Einschränkungen durch das Fernmeldegeheimnis auf Kommunikationsinhalte und -ergebnisse zugreifen zu können – soweit dies arbeitsrechtlich und datenschutzrechtlich gestattet ist. Arbeitsrechtlich hat er dabei die Einschränkungen seines Kontrollrechts zu beachten, datenschutzrechtlich insbesondere das Erforderlichkeitsprinzip, wie es in §§ 32 Abs. 1 Satz 1 und in § 28 Abs. 1 Satz 1 Nr. 2 BDSG zum Ausdruck kommt.

Innerhalb des BDSG wiederum ist zu differenzieren, welchen Zweck der Arbeitgeber mit seinem Zugriff verfolgt: ob er mit Blick auf ein bestimmtes Arbeitsverhältnis vorgenommen wird (§ 32 Abs. 1 Satz 1), ggf. sogar auf einen Verstoß des Arbeitnehmers (dann § 32 Abs. 1 Satz 2 BDSG) oder ob er erfolgt, um allgemeinere betriebliche Interessen zu wahren (vgl. § 28 Abs. 1 Satz 1 Nr. 2 BDSG).

Im Mittelpunkt aller Überlegungen zur Rechtfertigung von Datenverwendungen steht daher die konkrete und korrekte Bestimmung des vom Arbeitgeber *verfolgten Zwecks*.

a) § 32 Abs. 1 Satz 1 BDSG

Dient die Erhebung, Verarbeitung oder Nutzung personenbezogener IuK-Daten des Arbeitnehmers solchen des einzelnen Arbeitsverhältnisses, so richtet sich die Zulässigkeit von Datenverwendungen nach § 32 BDSG. Dessen Absatz 1 Satz 1 erlaubt den Umgang mit personenbezogenen Daten, wenn dies für die Begründung, Durchführung oder Beendigung eines Beschäftigungsverhältnisses erforderlich ist.

aa) Erforderlichkeit der Mitarbeiterkontrolle

Allgemeine Kontrollmaßnahmen zur Feststellung, ob Arbeitnehmer sich an ihre vertraglichen Verpflichtungen und betrieblichen Weisungen halten, kann der Arbeitgeber grundsätzlich auf § 32 Abs. 1 S. 1 BDSG stützen, da sie zur Durchführung des Beschäftigungsverhältnisses erforderlich sind. So ist ein Zugriff auf IuK-Daten etwa zulässig, um die Einhaltung des Verbots, das betriebliche E-Mail-System zu privaten Zwecken zu nutzen, zu verifizieren. Schließlich hat der Arbeitgeber ein berechtigtes Interesse daran zu kontrollieren, ob ein Verbot der privaten Nutzung befolgt wird bzw. eine erlaubte private Nutzung sich in dem vorgesehenen Rahmen bewegt. Eine solche Kontrollmaßnahme ist als datenschutzrechtlich erforderlich einzustufen.

Erforderlich können nach datenschutzrechtlichen Maßstäben allerdings nur solche Datenverwendungen sein, die auch im Übrigen rechtmäßig sind. Der Einsatz rechtswidriger Mittel ist niemals erforderlich. Daher ist an dieser Stelle insbesondere auch zu prüfen, ob die Maßnahmen des Arbeitgebers mit dem Arbeitsrecht im Einklang stehen. Zu erwähnen ist hier ein zentraler und praxisrelevanter Aspekt des Arbeitsrechts: Arbeitsrechtswidrig ist die unverhältnismäßige Ausübung des Direktions- und Kontrollrechts des Arbeitgebers. Daher ist eine Vollkontrolle des Arbeitnehmers, die über die stichprobenartige Ausübung der Kontrollbefugnis des Arbeitgebers zu klar definierten und eingegrenzten Kontrollzwecken hinausgeht und sämtliche seiner Arbeitsleistungen erfasst und bewertet, rechtswidrig. Daher ist der Arbeitgeber im Rahmen von Leistungs- und Verhaltenskontrollen nur zu Stichproben[13] befugt, die generelle Durchleuchtung des Arbeitnehmers ist hingegen unzulässig[14].

bb) Beispiele für erforderliche Kontrollmaßnahmen

aaa) Beispiel Telefonnutzung

Nutzt der Beschäftigte das ihm ausschließlich zu betrieblichen Zwecken überlassene Telefon – unabhängig davon, ob es sich um einen Festnetzanschluss oder ein Mobiltelefon handelt -, so kann der Arbeitgeber dessen Nutzung stichprobenartig überprüfen. Dies gilt sowohl für Verkehrsdaten, als auch für Inhaltsdaten (soweit dabei keine Persönlichkeitsrechte des Beschäftigten verletzt werden). Inhaltsdaten sind allerdings nur dann für ihn zugänglich, wenn auch der Kommunikationspartner auf den Schutz des Fernmeldegeheimnisses wirksam verzichtet. Dies erfordert dessen Einwilligungserklärung. Eine vollständige Aufzeichnung aller Telefonate zu Kontrollzwecken wäre unverhältnismäßig und daher nicht erforderlich gem. § 32 Abs. 1 Satz 1 BDSG.

bbb) Beispiel E-Mail-Nutzung

Ein- und ausgehende betriebliche E-Mails seiner Beschäftigten darf der Arbeitgeber im selben Maße zur Kenntnis nehmen wie

13 Unter einer Stichprobe wird dabei eine Verfahrensweise der Auswahl einer zu kontrollierenden Person aus einer Mehrzahl von Beschäftigten zu klar definierten Kontrollzwecken verstanden, bei der zufallsartig und ohne weitere Einflussmöglichkeit des Arbeitgebers oder Dritter die Auswahlentscheidung getroffen wird (Beispiel: Taschenkontrolle von Beschäftigten am Werksausgang, Auswahl durch Würfeln einer bestimmten Zahl).

14 Vgl. Zöll, in: Taeger/Gabel, BDSG, 2010, § 32 Rn. 24; Hilbrans, in: Däubler/Hjort/Schubert/Wolmerath, Arbeitsrecht, 2013, § 32 BDSG Rn. 20.

dessen übrigen betrieblichen Schriftverkehr. Beispielsweise kann er verfügen, dass ihm seine Beschäftigten jede für den Geschäftsgang relevante oder fest definierte ein- oder ausgehende E-Mails einzeln zur Kenntnis zuleiten. Dies ist zur Durchführung des Arbeitsverhältnisses, insbesondere zur Wahrnehmung der Direktions- und Kontrollbefugnis des Arbeitgebers erforderlich. Eine durch den Arbeitgeber eingerichtete automatisierte Weiterleitung aller ein- und ausgehenden E-Mails an den Vorgesetzten wäre allerdings arbeitsrechtlich als dauerhafte Vollkontrolle unzulässig.

ccc) Beispiel Internetnutzung

Der Arbeitgeber hat grundsätzlich das Recht, anhand von Protokolldaten stichprobenartig zu prüfen, ob das Surfen des Beschäftigten betrieblicher Natur ist, ob sich der Beschäftigte also an die Untersagung der privaten Nutzung auch tatsächlich hält. Eine Vollauswertung des Surfverhaltens der Beschäftigten wäre arbeitsrechtswidrig und daher nicht erforderlich i.S.v. § 32 Abs. 1 Satz 1 BDSG.

b) § 32 Abs. 1 Satz 2 BDSG

Absatz 1 Satz 2 ermächtigt zu Datenverwendungen des Arbeitgebers, um einem dokumentierten, auf tatsächlichen Anhaltspunkten beruhenden Verdacht auf eine im Beschäftigungsverhältnis begangene Straftat eines bestimmten Mitarbeiters auf verhältnismäßige Weise nachzugehen.

Liegen dokumentierte konkrete Anhaltspunkte für eine durch den Beschäftigten im Arbeitsverhältnis begangene Straftat vor, kann der Arbeitgeber etwa das betriebliche Postfach gemäß § 32 Abs. 1 S. 2 BDSG sichten, wenn dies für die Aufklärung der Straftat erforderlich und in Anbetracht möglicher schutzwürdiger Interessen des Betroffenen nicht unverhältnismäßig erscheint. Um die Verhältnismäßigkeit eines solchen Zugriffs zu wahren, ist insbesondere die Schwere des in Rede stehenden Delikts in die Abwägung einzubeziehen. Eine personenbezogene Vollkontrolle durch den Arbeitgeber ist als schwerwiegender Eingriff in das informationelle Selbstbestimmungsrecht der Beschäftigten hingegen regelmäßig unverhältnismäßig zulässig. Auch bei Straftatverdacht wird der Arbeitgeber daher immer nur schrittweise und differenzierend auf IuK-Nutzerdaten des betroffenen Beschäftigten zugreifen dürfen.

Ausdrücklich ist darauf hinzuweisen, dass die Bestimmung des § 32 Abs. 1 Satz 2 BDSG einen dokumentierbaren Anfangsverdacht gegen einen bestimmten Beschäftigten voraussetzt, also niemals Rechtsgrundlage für allgemeine Aufklärungsmaßnahmen sein kann, bei denen etwa ein Straftatverdacht besteht, dieser aber noch keinem bestimmten Beschäftigten zugeordnet werden kann.

Umgekehrt bedeutet die Regelung des § 32 Abs. 1 Satz 2 BDSG, dass Aufklärungsmaßnahmen des Arbeitgebers in Bezug auf vermutete Regelverstöße unterhalb der Straftatschwelle (Ordnungswidrigkeiten, Compliance-Verstöße gegen Unternehmensregeln oder Einzelweisungen) nicht auf § 32 Abs. 1 Satz 2 BDSG gestützt werden können. Ob hierfür auf § 28 Abs. 1 Satz 1 Nr. 2 BDSG zurückgegriffen werden kann, ist umstritten. Eine personenbezogene Kontrolle darf jedenfalls nur durchgeführt werden, wenn zu dokumentierende tatsächliche Anhaltspunkte den konkreten Verdacht eines Verstoßes gegen Verhaltensvorschriften bzw. den in der Betriebsvereinbarung festgelegten Umfang der erlaubten Privatnutzung begründen und soweit die Kontrollmaßnahme verhältnismäßig ist. Das Schutzniveau des § 32 Abs. 1 Satz 2 BDSG darf also keinesfalls unterlaufen werden.

c) § 28 Abs. 1 Satz 1 Nr. 2 BDSG

Diese Vorschrift – deren Anwendbarkeit neben § 32 BDSG umstritten ist[15] – gestattet die Datenverwendung zur Wahrung berechtigter Interessen des Unternehmens, soweit dies hierfür erforderlich ist und schutzwürdige Interessen des Betroffenen nicht überwiegen. In der Regel wird es hierbei um Zwecke gehen, die nicht in Bezug auf das einzelne Arbeitsverhältnis (dann wäre § 32 Abs. 1 BDSG einschlägig), sondern mit Blick auf die gesamte Belegschaft umgesetzt werden. Hierzu zählen etwa allgemeine verdachtslose (präventive) Kontrollen in Bezug auf vermutete, aber noch nicht dokumentierbare (vgl. § 32 Abs. 1 Satz 2 BDSG) Compliance-Verstöße im Unternehmen oder um Maßnahmen zur Aufrechterhaltung der betrieblichen Geschäftsabläufe.

Die Zulässigkeit des Zugriffs des Arbeitgebers auf IuK-Nutzerdaten ergibt sich aus einer Prüfung der Erforderlichkeit der Maßnahme zur Wahrung definierter betrieblicher Interessen und aus einer Gegenüberstellung und Abwägung mit schutzwürdigen Interessen der betroffenen Beschäftigten. Diese Interessen werden dann immer überwiegen, wenn die Maßnahme arbeitsrechtswidrig ist, etwa nicht stichprobenartig und mit klar definierten Kontrollzwecken, sondern als Vollkontrolle (alle Beschäftigte, alle möglichen Kontrollzwecke) durchgeführt wird.

aa) Präventive Compliance

Der stichprobenartige Zugriff etwa auf das E-Mail-Postfach von Arbeitnehmern mit definierten Kontrollzweck kann als präventive Maßnahme zulässig sein, um regel- oder gesetzwidriges Verhalten frühzeitig zu erkennen und zukünftig zu verhindern. Rechtmäßig gewonnene Ergebnisse solcher Präventivmaßnahmen können im Rahmen des BDSG (vgl. § 28 Abs. 2) zweckändernd auch für die Sanktionierung im Einzelfall aufgedeckter Regelverstöße genutzt werden.

Nicht als Ermächtigungsgrundlage zur Verfügung steht hingegen § 32 Abs. 1 S. 2 BDSG, da in dieser Konstellation ein konkreter Tatverdacht gegen einen bestimmten Arbeitnehmer noch nicht besteht. Bei nicht stichprobenartig, sondern allgemein auf alle Beschäftigte oder ganze Beschäftigtengruppen bezogenen präventiven Kontrollmaßnahmen (Compliance-Maßnahmen) steht einer zweckändernden Nutzung der Kontrollergebnisse zu Sanktionszwecken (repressive Nutzung) die Regelung des § 32 Abs. 1 Satz 2 BDSG entgegen, der ansonsten umgangen würde.

15 Zum Streitstand Riesenhuber, in: Wolff/Brink, Datenschutzrecht in Bund und Ländern, 2013, § 32 Rn. 16 ff.

bb) Zugriff auf Geschäftskorrespondenz in Abwesenheit des Beschäftigten

Bei vorübergehender Abwesenheit oder Ausscheiden eines Mitarbeiters darf der Arbeitgeber zur Wahrnehmung berechtigter Geschäftsinteressen i.S. des § 28 Abs. 1 S. 1 Nr. 2 BDSG auf das (ausschließlich zu betrieblichen Zwecken zu nutzende) E-Mail-Postfach dieses Arbeitnehmers zugreifen, um dort vermutete Geschäftsinformationen zu erlangen. Zur Wahrung des arbeitsrechtlichen Verhältnismäßigkeitsgrundsatzes hat der Arbeitgeber zuvor zu prüfen, ob weniger schwerwiegende Maßnahmen – Nachfrage beim Arbeitnehmer selbst, dessen Vertreter oder beim Geschäftspartner – ebenso zielführend wären und ob dem Zugriff keine überwiegenden schutzwürdigen Belange des Beschäftigten entgegenstehen.

d) Betriebsvereinbarung

Um die mit der Verwendung von IuK-Daten verfolgten Zwecke und die hierbei zu beachtenden Verfahrensweisen konkret und transparent festzulegen, empfiehlt sich der Abschluss einer Betriebsvereinbarung. Auch die Betriebsvereinbarung ist eine Rechtsvorschrift im Sinne von § 4 Abs. 1 BDSG, sie darf jedoch nicht gegen höherrangiges Recht, insbesondere gegen §§ 32, 28 und 31 BDSG verstoßen, sonst wäre sie (teil-) unwirksam.

Zwar muss sich die Betriebsvereinbarung bei ausgeschlossener Nutzung der IuK darauf beschränken, die einschlägigen Erlaubnistatbestände des BDSG konkretisierend auszugestalten und wird weitgehend deklaratorischer Natur sein, dies kann mit Blick auf die besonderen Verhältnisse des Unternehmens und zur Förderung der Rechtssicherheit bei der IuK-Nutzung jedoch von Vorteil sein.

Die Aufsichtsbehörden verfolgen das Ziel, eine Muster-Betriebsvereinbarung zur IuK-Nutzung vorzulegen.

e) Einwilligung

Für eine Einwilligung des Beschäftigten in (Kontroll-)Maßnahmen des Arbeitgebers unter Verwendung von IuK-Daten ist bei ausschließlich betrieblich zu nutzender IuK regelmäßig kein Raum: Es besteht zum einen kein Bedürfnis nach einer Einwilligung, da der Arbeitgeber bereits über hinreichende rechtliche Grundlagen seiner Kontrollmaßnahmen verfügt. Zum anderen ist die datenschutzrechtliche Einwilligungsbefähigung des Beschäftigten mangels Freiwilligkeit der Einwilligung (vgl. § 4a BDSG) im sozialen Abhängigkeitsverhältnis zum Arbeitgeber stark eingeschränkt. Anders als bei der Einwilligung in die Bedingungen für die private Nutzung betrieblicher IuK findet hier auch keine Ausweitung der Handlungsmöglichkeiten des Arbeitnehmers statt, die für die Freiwilligkeit seiner Einwilligung streiten könnte.

Sollten ausnahmsweise keine Zweifel an der Wirksamkeit der Einwilligung des Arbeitnehmers bestehen, etwa weil ihm neben der Einwilligungsoption weitere nachteilsfreie Handlungsmöglichkeiten vom Arbeitgeber eröffnet werden, so ist beim Zugriff auf Kommunikationsdaten auch die Einwilligung des Kommunikationspartners einzuholen. Die Einwilligungserklärung des außerbetrieblichen Kommunikationspartners bedarf dabei keiner bestimmten Form, sie kann insbesondere auch vorab (etwa zu Beginn eines Telefonats) mündlich abgegeben werden. Der Arbeitgeber sollte allerdings für eine hinreichende Dokumentation dieser Einwilligungserklärung Sorge tragen.

5. Protokollierung der IuK-Nutzung

Eine Protokollierung der IuK-Nutzung, also die Speicherung von Verkehrsdaten (§ 3 Nr. 30 TKG) über den Zeitraum der Diensteerbringung hinaus, kann aus Gründen der Systemsicherheit, der Kostenabrechnung oder der Missbrauchskontrolle erforderlich und nach Maßgabe der Vorschriften des TKG, TMG und BDSG (s.o.) zulässig sein. Bei gestatteter privater Nutzung kommt darüber hinaus eine Protokollierung auf Basis erteilter Einwilligungen in Betracht.

a) Grundsatz der Datensparsamkeit

Hierbei ist der *Grundsatz der Datensparsamkeit* (§ 3a BDSG) zu beachten. Dieser hat Auswirkungen auf die Art und Weise der Kontrolle der IuK-Nutzung und auf den Zugriff auf IuK-Protokolldaten. So ist es beispielsweise bei der Kontrolle der betrieblichen Internetnutzung in einem ersten Schritt völlig ausreichend, wenn zunächst nur eine Auswertung des allgemeinen Surfverhaltens im Betrieb ohne Personenbezug erfolgt, insbesondere ohne Einbeziehung der IP-Adresse und anderer Daten zur Identifizierung einzelner Beschäftigter. Treten dabei Hinweise auf eine missbräuchliche Nutzung auf, so kann der Arbeitgeber in einem nächsten Schritt stichprobenartig das Nutzungsverhalten einzelner Beschäftigter überprüfen. Stichprobenartig bedeutet dabei, dass er keinen Einfluss auf die Auswahl der zu überprüfenden Beschäftigten nehmen darf. In der Regel geschieht dies durch eine zufallsartige Auswahl unter den Beschäftigten, etwa durch Los. Kommt diese Zufallskontrolle zum Ergebnis, dass der überprüfte Beschäftigte keinen Verstoß begangen hat, so kann der Arbeitgeber weitere Kontrollen anschließen. Vollkontrollen aller Beschäftigten sind regelmäßig unverhältnismäßig.

Präventive Maßnahmen (etwa Vorgaben zu zulässigen oder unzulässigen Nutzungen, die technisch umgesetzt werden [white lists/black lists]), lassen regelmäßig die Erforderlichkeit von Protokollierungen entfallen und sind damit unter dem Aspekt des § 3a BDSG vorzugswürdig.

b) Vorgaben des § 9 BDSG

Darüber hinaus sind bei der Protokollierung der IuK-Nutzung insbesondere auch die Vorgaben des § 9 BDSG zu beachten. Dies bedeutet im Einzelnen:

- Die Erhebung und Verwendung von Protokolldaten muss an genau definierte Zwecke gebunden werden, etwa zur Aufrechterhaltung der Systemsicherheit, zur Analyse und Korrektur technischer Fehler im Netz, zur Optimierung der Rechnerleistungen im Netzwerk, zur Ermittlung der Kosten verbrauchter Ressourcen zwecks interner Leistungsverrechnung sowie zur Kontrolle der Einhaltung dienst-/arbeitsrechtlicher Vorgaben erfolgen. Diese Zweckbindung – etwa

zur Missbrauchskontrolle – schließt weitergehende Nutzungen – etwa zur Leistungskontrolle aus.
- Zugriffe auf Protokolldaten sind nur auf Grundlage von Berechtigungskonzepten zulässig (§ 9 Satz 1 BDSG i.V.m. Anlage Ziff. 3), die vorgeben, unter welchen Umständen durch welche Stelle Zugriffe erfolgen dürfen. Zugriffe auf Protokolldaten sind zu dokumentieren (§ 9 Satz 1 BDSG i.V.m. Anlage Ziff. 5).
- Aufbewahrungs- und Löschfristen von Protokolldaten richten sich nach § 35 Abs. 2 Satz 2 Nr. 3 BDSG. Sie sind zu löschen, wenn ihre Kenntnis für die Erfüllung des Zwecks der Speicherung nicht mehr erforderlich ist.
- Zugriffe auf Protokolldaten sind zu dokumentieren (§ 9 Satz 1 BDSG i.V.m. Anlage Ziff. 5). Aufbewahrungs- und Löschfristen von Protokolldaten richten sich nach § 35 Abs. 2 Satz 2 Nr. 3 BDSG. Sie sind zu löschen, wenn ihre Kenntnis für die Erfüllung des Zwecks der Speicherung nicht mehr erforderlich ist.

6. IuK-Nutzerdaten zu Geheimnisträgern

Bei Beschäftigten, denen in ihrer Tätigkeit persönliche Geheimnisse anvertraut werden (z.B. Betriebsrat, Betriebsarzt, Gleichstellungsbeauftragte, Schwerbehindertenbeauftragte, betriebliche Datenschutzbeauftragte) und die deshalb in einem besonderen Vertrauensverhältnis zu den betroffenen Personen stehen, muss eine Kenntnisnahme des Arbeitgebers von den Verkehrs- und Inhaltsdaten der IuK-Nutzung ausgeschlossen werden. Dementsprechend müssen Vorkehrungen getroffen werden, dass auch E-Mails, die der Kommunikation der Beschäftigten mit Geheimnisträgern dienen (erkennbar etwa anhand des Empfängers oder Betreffs), vom Arbeitgeber nicht zur Kenntnis genommen werden. Es empfiehlt sich, für diese Stellen nicht-personalisierte funktionsbezogene Postfächer (z.B. Betriebsrat@Unternehmen.de) einzurichten und diese von Kontrollen bzw. Auswertungen auszunehmen.

7. Verwertbarkeit von IuK-Daten

IuK-Nutzerdaten können auch im Rahmen von (arbeits-)gerichtlichen Auseinandersetzungen zwischen Arbeitgeber und Beschäftigtem Bedeutung erlangen. Hierbei ist die Rechtsprechung zu sog. Beweisverwertungsverboten zu beachten[16].

Hat der Arbeitgeber Kenntnis von IuK-Nutzerdaten auf unzulässige Weise erlangt, ist ihre prozessuale Einführung und Verwertung nicht ohne weiteres möglich. Insoweit ist eine Verletzung des Rechts auf informationelle Selbstbestimmung anzunehmen, welches durch das BDSG und die Datenschutzbestimmungen von TKG und TMG einfachgesetzlich konkretisiert wird. Beweise, die unter Verletzung dieses Individualrechts gewonnen wurden, unterliegen einem prozessualen Verwertungsverbot, sofern nach Güterabwägung mit dem Beweisinteresse des Arbeitgebers eine Verwertung nicht ausnahmsweise gerechtfertigt erscheint[17]. Besondere Umstände des Einzelfalls müssen die an sich rechtswidrige Informationsbeschaffung und Beweiserhebung als ausnahmsweise schutzwürdig erscheinen lassen[18], was insbesondere dann der Fall sein kann, wenn der Beweisführer sich in einer notwehrähnlichen Lage befindet[19]. Angesichts der verfassungsrechtlichen Garantie der informationellen Selbstbestimmung muss ein Verstoß gegen datenschutzrechtliche Bestimmungen – das Fernmeldegeheimnis zählt zu den von § 39 Abs. 1 BDSG erfassten Amtsgeheimnissen[20] – jedenfalls dann regelmäßig zu einem Beweisverwertungsverbot führen, wenn die Voraussetzungen einer Eingriffsnorm nicht beachtet wurden[21]. Die jüngste Rechtsprechung des BAG zur Unverwertbarkeit datenschutzwidrig erhobener Beweismittel in Zivilverfahren stützt die Annahme von Beweisverwertungsverboten[22].

II. Ausblick

Die rasant fortschreitende technische Entwicklung und die damit nur bedingt Schritt haltende Rechtsentwicklung weisen den Aufsichtsbehörden für den Datenschutz die Aufgabe zu, für Orientierung in diesem komplexen Rechtsgebiet zu sorgen. Eine Reihe von Aufsichtsbehörden hat deshalb bereits entsprechende Orientierungshilfen vorgelegt, etwa der ULD Schleswig-Holstein[23] oder der BfDI[24]. Zuletzt hat der LfDI Rheinland-Pfalz eine aktuelle Orientierungshilfe zur datenschutzgerechten Ausgestaltung und Kontrolle der Nutzung von Informations- und Kommunikationstechnik des Unternehmens durch Beschäftigte zu betrieblichen und zu privaten Zwecken[25] vorgestellt. Ziel aller Aufsichtsbehörden in Deutschland muss es bleiben, durch die Koordinierung und Konsolidierung der bislang eigenständig vorgelegten Orientierungshilfen eine länderübergreifend vereinheitlichte, gemeinsame Orientierungshilfe vorzulegen.

16 Greger, in: Zöller, ZPO, 2014, § 286 Rn. 15a; OLG Karlsruhe NJW 2000, 1577 (1578).

17 Siehe etwa OLG Karlsruhe NJW 2000, 1577 (1578).

18 BAG NJW 2008, 2732 (2735).

19 So auch Thüsing/Pötters, in: Thüsing, Beschäftigtendatenschutz und Compliance, 2014, § 21 Rn. 32.

20 Plath, in: Plath, BDSG, 2013, § 39 Rn. 7.

21 Thüsing/Pötters, in: Thüsing, Beschäftigtendatenschutz und Compliance, 2014, § 21 Rn. 30 m.w.N.

22 Dazu ausführlich Brink/Wybitul, ZD 2014, 225 ff.

23 Https://www.datenschutzzentrum.de/internet/private-und-dienstliche-internetnutzung.pdf (Stand 4/2014).

24 Https://www.bfdi.bund.de/SharedDocs/Publikationen/Arbeitshilfen/LeitfadenInternetAmArbeitsplatzneu.pdf;jsessionid=0883803AA925E3755034DA2774959D37.1_cid329?__blob=publicationFile&v=3 (Stand 1/2008).

25 Https://www.datenschutz.rlp.de/downloads/oh/oh_iuk_arbeitsplatz.pdf

Dr. Stefan Brink
Leiter Privater Datenschutz beim Landesbeauftragten für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz.

Dr. iur. Lorenz Franck

Datenhehlerei nach dem künftigen § 202d StGB

Am 27. Mai 2015 beschloss das Bundeskabinett den Entwurf eines Gesetzes zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten. Neben den Vorschriften zur Vorratsdatenspeicherung wird hierin en passant ein neuer Straftatbestand der Datenhehlerei geschaffen.

I. Tatbestand

Der neue Straftatbestand der Datenhehlerei schützt das sog. „formelle Datengeheimnis", welches durch eine rechtswidrige Vortat bereits verletzt worden ist, vor einer Aufrechterhaltung und Vertiefung (sog. „Perpetuierung") dieser Verletzung[1]. Der Entwurfstext[2] der Bundesregierung lautet konkret:

(1) Wer Daten (§ 202a Abs. 2), die nicht allgemein zugänglich sind und die ein anderer durch eine rechtswidrige Tat erlangt hat, sich oder einem anderen verschafft, einem anderen überlässt, verbreitet oder sonst zugänglich macht, um sich oder einen Dritten zu bereichern oder einen anderen zu schädigen, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

(2) Die Strafe darf nicht schwerer sein als die für die Vortat angedrohte Strafe.

(3) Abs. 1 gilt nicht für Handlungen, die ausschließlich der Erfüllung rechtmäßiger dienstlicher oder beruflicher Pflichten dienen. Dazu gehören insbesondere

1. solche Handlungen von Amtsträgern oder deren Beauftragten, mit denen Daten ausschließlich der Verwertung in einem Besteuerungsverfahren, einem Strafverfahren oder einem Ordnungswidrigkeitenverfahren zugeführt werden sollen, sowie
2. solche beruflichen Handlungen der in § 53 Abs. 1 Satz 1 Nummer 5 der Strafprozessordnung genannten Personen, mit denen Daten entgegengenommen, ausgewertet oder veröffentlicht werden.

Ursprünglich handelte es sich bei der Datenhehlerei um einen eigenständigen Gesetzentwurf. Das Land Hessen brachte einen entsprechenden Antrag bereits 2013 in den Bundesrat ein[3]. Die Frage, warum die Datenhehlerei nunmehr mit der Vorratsdatenspeicherung verknüpft wird, beantwortet das Bundesministerium für Justiz und Verbraucherschutz nur vage: Dem Anliegen, in einer immer stärker von Informations- und Kommunikationstechnologie geprägten Gesellschaft effektive Strafverfolgung zu ermöglichen, stehe die Notwendigkeit gegenüber, den strafrechtlichen Schutz von Informationssystemen und der in ihnen gespeicherten Daten vor Angriffen und Ausspähungen ausreichend zu gewährleisten[4]. Es fällt jedoch zugegebenermaßen schwer, sich das Gegenüberstehen von Anliegen und Notwendigkeit bildlich vorzustellen[5].

Seit dem 12. Juni 2015 befindet sich der Gesetzentwurf in der Beratungsphase. Während der ersten Lesung im Bundestag wurde die Datenhehlerei neben dem Großprojekt Vorratsdatenspeicherung nur stiefmütterlich behandelt[6]. Im September folgen voraussichtlich die zweite und dritte Lesung.

II. Einzelerläuterungen

1. Tatobjekt

Der Tatbestand der Datenhehlerei erfasst ausschließlich Daten im Sinne von § 202a StGB. Geschützt werden nicht sämtliche erdenklichen Informationen, sondern lediglich solche, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden (§ 202a Abs. 2 StGB).

Einschränkend verlangt § 202d Abs. 1 StGB-E zudem, dass die Daten nicht allgemein zugänglich sind. Sofern die Daten aus allgemein zugänglichen Quellen entnommen werden können (nicht: entnommen wurden!), sei die formelle Verfügungsbefugnis nicht in strafwürdiger Weise beeinträchtigt[7]. Die Entscheidungsgewalt über die Preisgabe der Daten liegt insoweit nicht ausschließlich beim Berechtigten. Allgemein zugänglich sind Daten (entsprechend § 10 Abs. 5 S. 2 BDSG[8]), die jedermann mit oder ohne vorherige Anmeldung, Zulassung oder Entrichtung eines Entgelts nutzen kann.

2. Vortat

Ausweislich des Wortlauts von § 202d Abs. 1 StGB-E kann jede rechtswidrige Tat taugliche Vortat einer Datenhehlerei sein. Hiermit sind ausschließlich Straftaten gemeint. Dies ergibt sich bereits aus der Verwendung des Begriffes „Tat" als strafrechtlicher Grundfeste (vgl. § 11 Abs. 1 Nr. 5 StGB). Zudem ist das Strafmaß in § 202d Abs. 2 StGB-E durch dasjenige der Vortat gedeckelt. Anderweitig rechtswidriges Handeln, wie etwa eine datenschutzrechtliche Ordnungswidrigkeit, genügt hingegen nicht[9].

Dies deckt sich mit der Intention der Bundesregierung: Die Sachhehlerei nach § 259 StGB betreffe nicht nur das verletzte Eigentum, indem sie den herbeigeführten rechtswidrigen Ver-

1 Regierungsentwurf (RegE) vom 27.05.2015, S. 28, online unter http://www.bmjv.de/SharedDocs/Downloads/DE/pdfs/Gesetze/RegE_Hoechstspeicherfrist.pdf; zweifelnd hingegen Golla/von zur Mühlen, JZ 2014, 668, 670 f.

2 RegE (Fn. 1), S. 20.

3 BR-Drs. 284/13.

4 BMJV, Frage- und Antwortenpapier, S. 8, online unter http://www.bmjv.de/SharedDocs/Downloads/DE/pdfs/20150527_FAQ_Hoechstspeicherfrist.pdf.

5 Ähnlich ratlos EAID, Stellungnahme vom 25.5.2015, S. 7, online unter http://www.eaid-berlin.de/wp-content/uploads/2015/05/EAID_Stellungnahme_GE_VDS_25_.pdf.

6 Gedächtnisprotokoll unter https://netzpolitik.org/2015/live-blog-erste-lesung-zur-vorratsdatenspeicherung-im-bundestag/.

7 RegE (Fn. 1), S. 29/54.

8 RegE (Fn. 1), S. 54.

mögenszustand perpetuiert, sondern auch das allgemeine Sicherheitsinteresse, welches durch den von der Hehlerei geschaffenen Anreiz zur Verübung von Vortaten beeinträchtigt werde[10]. Entsprechendes gelte für die Datenhehlerei.

Nicht aus dem Normtext, sondern lediglich aus dem Schutzzweck der Norm ergibt sich die Einschränkung, dass die Vortat zumindest auch die formelle Verfügungsbefugnis an den Daten schützen muss. Sind rein öffentliche Interessen durch die Vortat betroffen (wie etwa bei § 184d StGB[11]), bleibt für die Datenhehlerei kein Raum.

3. Tathandlungen

Datenhehler ist, wer die Daten sich oder einem anderen verschafft, einem anderen überlässt, verbreitet oder sonst zugänglich macht. Die Begehungshandlungen unterscheiden sich von denjenigen der Sachhehlerei nach § 259 Abs. 1 StGB („… ankauft oder sonst sich oder einem Dritten verschafft, sie absetzt oder absetzen hilft") und sind stattdessen an § 202c StGB angelehnt. Die Daten sind erst dann verschafft, wenn die tatsächliche Verfügungsmacht über sie erlangt wurde[12]. Für die Zugänglichmachung genügt bereits die Möglichkeit des Zugriffs auf die Daten[13].

4. Ausnahmen

§ 202d Abs. 1 StGB-E gilt nicht für Handlungen, „die ausschließlich der Erfüllung rechtmäßiger dienstlicher oder beruflicher Pflichten dienen". Exemplarisch führt Abs. 3 S. 2 Nr. 1 Handlungen von Amtsträgern oder deren Beauftragten auf, mit denen Daten ausschließlich der Verwertung in einem Besteuerungsverfahren, einem Strafverfahren oder einem Ordnungswidrigkeitenverfahren zugeführt werden sollen. Gemeint ist hierbei insbesondere der Ankauf illegal beschaffter Steuer-CDs[14]. Zu beachten ist allerdings, dass diese Ausnahme keinen datenschutzrechtlichen Erlaubnistatbestand im Sinne von § 4 Abs. 1 BDSG darstellt und auch nicht als Ausschließungsgrund für eine etwaige Strafbarkeit nach § 44 Abs. 1 i.V.m. § 43 Abs. 2 Nrn. 1-5 BDSG bzw. entsprechenden landesdatenschutzrechtlichen Strafvorschriften herangezogen werden kann[15].

§ 202d Abs. 3 S. 2 Nr. 1 StGB-E stellt berufliches Handeln der in § 53 Abs. 1 S. 1 Nr. 5 StPO genannten Personen frei, wenn durch sie Daten entgegengenommen, ausgewertet oder veröffentlicht werden. Die Vorschrift meint all diejenigen Personen, die bei der Vorbereitung, Herstellung oder Verbreitung von Druckwerken, Rundfunksendungen, Filmberichten oder der Unterrichtung oder Meinungsbildung dienenden Informations- und Kommunikationsdiensten berufsmäßig mitwirken. Der Passus ist nachträglich eingefügt worden und eine Reaktion auf befürchtete Einschränkungen der Pressefreiheit sowie den damit einhergehenden Verstoß gegen Art. 5 Abs. 1 S. 2 GG.

5. Vorsatz

Die Datenhehlerei kann nur vorsätzlich begangen werden (§ 15 StGB). Der Täter muss daher mindestens billigend in Kauf nehmen, dass die Daten nicht öffentlich zugänglich sind und aus einer rechtswidrigen Vortat stammen (sog. „dolus eventualis"). Er muss zudem die Absicht verfolgen, sich oder einen Dritten zu bereichern oder einen anderen zu schädigen (besondere Form des Vorsatzes, sog. „dolus directus"). Die Schädigungsabsicht umfasst nicht nur materielle, sondern auch immaterielle Schäden.

6. Strafmaß

Die Tat soll mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft werden. Die Strafdrohung orientiert sich damit am Ausspähen von Daten nach § 202a StGB und liegt im oberen Bereich der im 15. Abschnitt („Verletzung des persönlichen Lebens- und Geheimbereichs", §§ 201-206 StGB) ausgeworfenen Sanktionen. Die Strafe darf allerdings gem. § 202d Abs. 2 StGB-E nicht schwerer sein als die für die Vortat angedrohte Strafe. Bei der Strafzumessung wägt das Gericht die Umstände ab, die für und gegen den Täter sprechen (§ 46 Abs. 2 StGB).

7. Versuchsstrafbarkeit

Gemäß § 23 Abs. 1 StGB ist der Versuch eines Vergehens im Sinne von § 12 Abs. 2 StGB nur dann strafbar, wenn das Gesetz dies ausdrücklich vorgibt. Eine Versuchsstrafbarkeit der Datenhehlerei ist im aktuellen Entwurf nicht mehr enthalten[16].

8. Strafantrag

Nach § 205 Abs. 1 S. 2 StGB-E wird die Tat nur auf Antrag verfolgt, es sei denn, dass die Strafverfolgungsbehörde wegen des besonderen öffentlichen Interesses an der Strafverfolgung ein Einschreiten von Amts wegen für geboten hält[17]. Antragsberechtig ist gem. § 77 Abs. 1 StGB nur der Verletzte selbst[18]. Sind mehrere Personen antragsberechtigt, so kann jeder den Antrag selbständig stellen (§ 77 Abs. 4 StGB).

9. Konkurrenzen

Eine Beteiligung (Anstiftung, § 26 StGB; Beihilfe, § 27 StGB) an der Vortat oder gar Mittäterschaft (§ 25 Abs. 2 StGB) dürfte ausscheiden, da die Vortat zum Zeitpunkt der Hehlerei bereits beendet sein wird. Mittäterschaft und Teilnahme sind hingegen bei Folgetaten denkbar.

Die Weitervermittlung gestohlener Daten steht an sich bereits gem. § 202c Abs. 1 Nr. 1 StGB unter Strafe, sofern es sich um Passwörter oder sonstige Sicherungscodes handelt und dadurch eine weitere Straftat nach den §§ 202a, 202b StGB vorbereitet wird.

Der Handel mit Geschäfts- und Betriebsgeheimnissen ist gem. § 17 Abs. 2 UWG umfassend mit Strafe bedroht. Der Regierungsentwurf übersieht insoweit, dass es dem Täter

9 RegE (Fn. 1), S. 55.

10 RegE (Fn. 1), S. 29.

11 RegE (Fn. 1), S. 54.

12 RegE (Fn. 1), S. 55.

13 Graf, in: Münchener Kommentar StGB, Bd. 4., 2. Aufl. 2012, § 202c Rn. 23.

14 Vgl. BVerfG, Beschl. v. 9.11.2010, Az. 2 BvR 2101/09, online unter http://dejure.org/2010,53; mit guten Gründen gegen einen entsprechenden Ausnahmetatbestand Klengel/Gans, ZRP 2013, 16, 17 ff.

15 A.A. wohl EAID, Stellungnahme (Fn. 5), S. 12.

16 Anders zuvor Abs. 4 des Entwurfs, BR-Drs. 284/13, S. 2 bzw. BT-Drs. 18/1288, S. 8.

17 RegE (Fn. 1), S. 21.

18 Vgl. anders im BDSG, § 44 Abs. 2 S. 2 („der Betroffene, die verantwortliche Stelle, der BfDI und die Aufsichtsbehörde").

nach § 17 Abs. 2 Nr. 2 UWG durchaus möglich ist, auf rechtswidrige Vortaten Dritter aufzubauen.

Die unerlaubte Vervielfältigung und die gewerbsmäßige Verwertung urheberrechtlich geschützter Werke werden von den §§ 106 ff. UrhG erfasst. Dies gilt unabhängig davon, ob die Werke öffentlich zugänglich sind oder nicht.

Der illegale Handel mit personenbezogenen Daten unterfällt § 44 Abs. 1 iVm § 43 Abs. 2 Nrn. 1-5 BDSG bzw. landesrechtlichen Datenschutzvorschriften[19].

An Begünstigung nach § 257 StGB und ggf. Strafvereitelung nach § 258 StGB ist ebenfalls zu denken.

Beschafft sich der Täter die Daten, um selbst eine weitere Straftat (z.B. Betrug, § 263 StGB; Computerbetrug, § 263a StGB) zu begehen, dürfte es sich bei der Datenhehlerei um eine mitbestrafte Vortat handeln. Sieht der Täter unterdessen reuig von der Verwirklichung der Nachtat ab, stellt § 202d StGB-E eine Ausweitung der Vorfeldstrafbarkeit dar.

III. Kritik

1. Strafbarkeitslücken

In der Entwurfsbegründung werden Strafbarkeitslücken angeführt, die die Schaffung einer neuen Strafnorm erforderlich machten[20]. Eine Strafbarkeitslücke ist jedoch nicht bereits deswegen gegeben, weil ein bestimmtes missbilligtes Verhalten nicht unter Strafe steht. Insoweit ist das gesamte Strafrecht auf Lückenhaftigkeit angelegt (vgl. Art. 103 Abs. 2 GG, § 1 StGB, „nulla poena sine lege"). Inwieweit die oben in Pkt. II. 3. genannten bestehenden einschlägigen Deliktsarten nicht geeignet sein sollen, die Weitergabe illegal beschaffter Daten wirksam zu unterbinden, wurde durch die Bundesregierung zu keinem Zeitpunkt belegt[21]. Es bedarf einiger Geistesanstrengung, einen Fall zu konstruieren, der nicht bereits von § 44 BDSG bzw. § 17 UWG erfasst ist, aber dennoch uneingeschränkt strafwürdig erscheint. So bleibt es vorerst bei der Note Montesquieues: „Wenn es nicht notwendig ist, ein Gesetz zu machen, dann ist es notwendig, kein Gesetz zu machen."

2. Presse- und Wissenschaftsfreiheit

Die Pressefreiheit stellt eines der wertvollsten Güter in einem demokratischen Rechtsstaat dar. Der Entwurfstext der Bundesregierung enthält mittlerweile immerhin eine Tatbestandsausnahme für „ausschließlich berufliche Pflichten" von Journalisten und Reportern[22]. Dieser Passus erfordert jedoch Nachbesserung.

Unklar ist einerseits, was Journalismus zum Beruf im Sinne der Vorschrift qualifiziert. Immerhin ist gerichtlich festgestellt, dass der Besitz eines Presseausweises nicht Voraussetzung ist, um die Segnungen des Art. 5 Abs. 1 S. 2 GG zu empfangen[23]. Fraglich ist aber, ob sich auch Blogger, Podcaster und Whistleblower-Plattformen mit redaktionellem Unterbau auf die Ausnahme in § 202d Abs. 3 Nr. 2 StGB-E berufen dürfen.

Unklar ist ferner, was genau eine berufliche Pflicht insbesondere bei Freiberuflern ausmacht. Zwar stellt der Regierungsentwurf fest, dass auch selbstauferlegte Pflichten genügen sollen[24], handhabbarer wird die Vorschrift dadurch jedoch nicht. Die Dogmatik zum ähnlich lautenden § 184b Abs. 5 Nr. 3 StGB fordert außerdem eine journalistische Tätigkeit im Zusammenhang mit einer konkreten Veröffentlichung[25]. Ein Journalist, der Daten zugspielt bekommt, kann jedoch erst nach der Sichtung wirklich beurteilen, ob daraus eine Veröffentlichung werden soll. Aus ebenjenem Grund trifft der Entwurf vielfach auf Ablehnung[26].

Die wissenschaftliche Forschung nach Art. 5 Abs. 3 S. 1 GG findet überhaupt keine Berücksichtigung in § 202d Abs. 3 StGB-E[27]. Sicherheitsforscher werden sich insoweit in der Beweisnot wiederfinden, dass sie die tatbestandliche Handlung nicht mit Bereicherungs- oder Schädigungsabsicht vorgenommen haben[28]. Eine ähnlich beschämende Situation trat zuvor schon bei Einführung des § 202c StGB auf.

3. Rechtsunsicherheit

Die stillschweigende Beschränkung möglicher Vortaten auf solche, die zumindest auch die formelle Verfügungsgewalt schützen[29], schafft Rechtsunsicherheit und ist dem juristischen Laien kaum zuzumuten. Hier findet sich ein unnötiges Einfallstor für Tatbestands- und Verbotsirrtümer nach den §§ 16 f. StGB[30].

Völlig irregeleitet ist schließlich die Vorstellung der Bundesregierung, der datenschutzrechtlich Betroffene könne sich gemäß § 202d Abs. 1 StGB-E strafbar machen, wenn er Daten vom Vortäter erhält[31]. Der Betroffene dürfte kaum Schädigungs- oder Bereicherungsabsicht aufweisen. Abgesehen davon besitzt er ein Arsenal an Auskunfts- und Einsichtsrechten[32], das er gegen die verantwortliche Stelle und damit den formell Verfügungsberechtigten ins Feld führen kann. Die Situation gleicht ihm gegenüber eher derjenigen bei öffentlich zugänglichen Daten[33]. Der Verletzte hat gegenüber dem datenschutzrechtlich Betroffenen kein ausschließliches Verfügungsrecht über die Daten. Der Verweis der Bundesregierung auf § 202a StGB[34] verkennt insoweit den strukturellen Unterschied zwischen Vortat und Perpetuierungsdelikt.

19 Diese sind z.T. subsidiär ausgestaltet, vgl. § 33 Abs. 2 DSG NRW.

20 RegE (Fn. 1), S. 27 f.; ebenso zuvor der 69. Deutsche Juristentag, Beschlüsse vom 18. bis 21.09.2012, S. 9.

21 Ebenso Golla/von zur Mühlen, JZ 2014, 668, 671 ff.

22 Anders zuvor Abs. 5 in BR-Drs. 284/13, S. 2 bzw. BT-Drs. 18/1288, S. 8.

23 VG Lüneburg, Urt. v. 22.05.2014, Az. 5 A 120/13.

24 RegE (Fn. 1), S. 57.

25 Hörnle, in: Münchener Kommentar StGB, Bd. 3, 2. Aufl. 2012, § 184b Rn. 41.

26 DAV, Pressemitteilung vom 21.5.2015, online unter http://anwaltverein.de/de/newsroom/pm-17-15-dav-lehnt-vorratsdatenspeicherung-ab; EAID, Stellungnahme (Fn. 5), S. 13; Härting, http://www.cr-online.de/blog/2015/05/18/indiskretionen-werden-zur-strafbaren-datenhehlerei/.

27 In § 184b Abs. 5 StGB ist sie hingegen enthalten, vgl. Hörnle in: Münchener Kommentar StGB, Bd. 3, 2. Aufl. 2012, § 184b Rn. 41.

28 Zur Tatbestandskorrektur auf subjektiver Ebene zugunsten von Journalisten bereits Golla/von zur Mühlen, JZ 2014, 668, 669.

29 Siehe oben Pkt. II. 2.

30 Die fehlende Bestimmtheit rügen auch Golla/von zur Mühlen, JZ 2014, 668, 670.

31 So ausdrücklich RegE (Fn. 1), S. 55.

32 Überblick bei Franck, RDV 2015, 137, 139 ff.

33 Siehe oben Pkt. II. 1.

34 RegE (Fn. 1), S. 55.

IV. Zusammenfassung

Der Gesetzentwurf zur Datenhehlerei ist unsauber gearbeitet und unzureichend begründet. Behauptete Strafbarkeitslücken sind keineswegs nachgewiesen, die Erforderlichkeit der Vorschrift steht damit insgesamt in Frage. Die verfassungsrechtlich verbriefte Pressefreiheit von nebenberuflichen und Amateurjournalisten wird in unzulässiger Weise eingeschränkt, hauptberufliche Journalisten werden mit rechtlichen Unwägbarkeiten konfrontiert. Insgesamt kann der Regierungsentwurf nur als fehlgeschlagener Versuch bewertet werden.

Dr. Lorenz Franck
Mitarbeiter der GDD-Geschäftsstelle sowie Lehrbeauftragter für Datenschutzrecht an der Fachhochschule Köln.

Kurzbeiträge

Datenschutzrechtliche Aspekte des Tarifeinheitsgesetzes

Prof. Peter Gola, Königswinter*

1. Das Mehrheitsprinzip entscheidet über Tarifvertrag

Am 22. Mai und nachfolgend am 12. Juni hat das Gesetz zur Tarifeinheit (Tarifeinheitsgesetz) den Bundestag und den Bundesrat passiert. Die gesetzlichen Regelungen sind nach wie vor umstritten. Verfassungsklagen sind u.a. von Berufsgewerkschaften angekündigt.

Mit der Einfügung eines § 4a in das TVG soll der Grundsatz der Tarifeinheit wiederhergestellt werden, den das BAG mit seiner Entscheidung vom 7.7.2010 (NZA 2010, 1068) aufgegeben hatte. Infolge der damit bestehenden Tarifpluralität konnten für dieselbe Beschäftigtengruppe unterschiedliche Tarifverträge konkurrierender Gewerkschaften zur Anwendung kommen.

Nach § 4a Abs. 2 S. 2 TVG sind bei kollidierenden Tarifverträgen nur noch die Normen des Tarifvertrages maßgebend, der von der mitgliederstärkeren Gewerkschaft abgeschlossen wurde.

Dieses Mehrheitsprinzip ist nach der Auffassung des Gesetzgebers in besonderer Weise geeignet, das wieder angestrebte Ziel der Tarifeinheit zu erreichen. Der Tarifvertrag soll zur Anwendung kommen, dessen Interessenausgleich die größte Akzeptanz in der Belegschaft besitzt. Das Mehrheitsprinzip gebe dem durch Art. 9 Abs. 3 des Grundgesetzes (GG) ermöglichten Koalitionswettbewerb, d.h. dem Wettbewerb der Gewerkschaften um Mitglieder, Raum. Indem im Fall konkurrierender Tarifverträge der effektiv im Betrieb gestaltende Tarifvertrag nach dem Mehrheitsprinzip ausgewählt wird, werde diese Auswahlentscheidung den organisierten Arbeitnehmerinnen und Arbeitnehmern und damit letztlich dem Koalitionswettbewerb anvertraut.

§ 4a Abs. 2 TVG regelt wie folgt:
„Der Arbeitgeber kann nach § 3 an mehrere Tarifverträge unterschiedlicher Gewerkschaften gebunden sein. Soweit sich die Geltungsbereiche nicht inhaltsgleicher Tarifverträge verschiedener Gewerkschaften überschneiden (kollidierende Tarifverträge), sind im Betrieb nur die Rechtsnormen des Tarifvertrags derjenigen Gewerkschaft anwendbar, die zum Zeitpunkt des Abschlusses des zuletzt abgeschlossenen kollidierenden Tarifvertrags im Betrieb die meisten in einem Arbeitsverhältnis stehenden Mitglieder hat. Kollidieren die Tarifverträge erst zu einem späteren Zeitpunkt, ist dieser für die Mehrheitsfeststellung maßgeblich. ……"

Über die Gültigkeit von konkurrierenden Tarifverträgen entscheidet also die Mitgliederzahl, die die jeweilige Gewerkschaft bei Abschluss des Vertrages hat.

2. Beweisführung über die Mitgliederstärke

Damit liegt das Interesse des Arbeitgebers, der in einem tarifpluralen Betrieb in Tarifverhandlungen steht, zu erfahren, welche Gewerkschaft letztlich der maßgebende Tarifpartner ist, auf der Hand. Andererseits ist eindeutig, dass die Gewerkschaftszugehörigkeit des Beschäftigten im Bewerbungs- und auch im Beschäftigungsverhältnis grundsätzlich nicht vom Fragerecht des Arbeitgebers erfasst wird. Das BAG hat sich nunmehr (Beschluss vom 18. 11. 2014 – 1 AZR 257/13 –) mit

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

der besonderen Konstellation bei Tarifvertragsverhandlungen mit konkurrierenden Gewerkschaften befasst und auch hier das Fragerecht im konkreten Fall von Tarifverhandlungen verneint.

Die Leitsätze lauten wie folgt:
„1. Art. 9 Abs. 3 GG schützt eine Gewerkschaft auch darin, der Arbeitgeberseite in einer konkreten Tarifvertragsverhandlungssituation Angaben über ihren Organisationsgrad und die Verteilung ihrer Mitglieder in bestimmten Betrieben vorzuenthalten. 2. Verlangt ein Arbeitgeber während laufender Tarifvertragsverhandlungen von seinen Arbeitnehmern die Offenlegung ihrer Gewerkschaftszugehörigkeit, handelt es sich um eine gegen die gewerkschaftliche Koalitionsbetätigungsfreiheit gerichtete Maßnahme“.

Andererseits kann es nach Auffassung des Bundesarbeitsgerichtes aber Fälle geben, in denen der Arbeitgeber zu Recht nach der Gewerkschaftsmitgliedschaft seiner Arbeitnehmer fragt, was dann zur Zurückweisung des pauschalen Unterlassungsantrags der Gewerkschaft führte. Dazu, ob eine derartige Situation nach Abschluss konkurrierender Tarifverträge besteht, hat sich das BAG nicht geäußert.

Jedoch hat die Rechtsprechung bereits zuvor in einer gleichgelagerten Situation nach einer datenschutzkonformen Lösung gesucht, bei der die Art der Nachweisung der Gewerkschaftsmitgliedschaft den unterschiedlichen Interessen des Arbeitgebers einerseits und der Gewerkschaft und der Arbeitnehmer andererseits Rechnung trägt (BAG vom 25.3.1992 – 7 AZR 65/90 –). Dabei ging es darum, dass das Betriebsverfassungsgesetz den Gewerkschaften zahlreiche Aufgaben und Befugnisse im Betrieb zuweist; dies jedoch unter der Voraussetzung, dass die Gewerkschaft im Betrieb vertreten ist (vgl. u.a. §§ 2 Abs. 1 und 2, 14 Abs. 7, 16 Abs. 2, 17 Abs. 3, 18 Abs. 1 und 2, 19 Abs. 2 BetrVG etc.) (vgl. die Aufstellung bei Fitting, BetrVG, § 2, Rn. 52).

Die Vertretung ist bereits anzunehmen, wenn nur ein Arbeitnehmer des Betriebes der betreffenden Gewerkschaft angehört; fraglich ist jedoch, wie die Gewerkschaft den ggf. erforderlichen Nachweis der Vertretung erbringen kann, d.h., ob sie hierzu zumindest die Mitgliedschaft eines Beschäftigten dem Arbeitgeber offenbaren muss oder ob zutreffend auch insoweit dem Datenschutz der betroffenen Arbeitnehmer Vorrang einzuräumen ist. Gemäß der h.M. in Rechtsprechung und Literatur (vgl. Richardi, BetrVG, § 2 Rn. 71) kann sie den erforderlichen Beweis führen, ohne den Namen eines betriebsangehörigen Mitglieds zu nennen. Es genügt die Vorlage einer notariellen Erklärung, in der bescheinigt wird, dass eine Person, deren Personalien hinterlegt sind, einem Betrieb und einer bestimmten Gewerkschaft angehört.

Der Leitsatz Nr. 2 der oben genannten Entscheidung des BAG lautet: 2.
Die Gewerkschaft kann den erforderlichen Beweis auch durch mittelbare Beweismittel, z.B. durch notarielle Erklärungen führen, ohne den Namen ihres im Betrieb des Arbeitgebers beschäftigten Mitglieds zu nennen. Ob diese Beweisführung ausreicht, ist eine Frage der freien Beweiswürdigung. Die Tatsachengerichte müssen dem geringeren Beweiswert mittelbarer Beweismittel durch besonders sorgfäItige Beweiswürdigung und Begründung ihrer Entscheidung Rechnung tragen.

Zwar könne, wie das LAG Düsseldorf (DB 1989, 1036) festhält, ein für den Arbeitgeber eindeutig nachprüfbarer Nachweis letztlich nur durch die Nennung des Mitglieds erfolgen. Dem stehe aber entgegen, dass es der Gewerkschaft schon aus datenschutzrechtlichen Gründen versagt sei, den Namen des Mitglieds ohne dessen Einwilligung weiterzugeben. Ferner folge aus der grundsätzlichen Unzulässigkeit der Erhebung des Datums im Rahmen des Fragerechts des Arbeitgebers, dass die Gewerkschaftszugehörigkeit auch im Wege der Zeugenvernehmung nicht offenbart werden dürfe. Das damit für den Nachweis des »Vertretenseins« gerechtfertigte »Geheimverfahren« gewährt dem einzelnen Arbeitnehmer dem seinem Recht auf informationelle Selbstbestimmung und Koalitionsfreiheit angemessenen Schutz.

Auch wenn es bei § 4a TVG nicht um ein konkretes einzelnes Gewerkschaftsmitglied, sondern um deren Gesamtzahl zu einem bestimmten Zeitpunkt geht, hat der Gesetzgeber obige Überlegungen im Zusammenhang mit der Nachweisführung im Rahmen des § 4a TVG aufgegriffen und nunmehr als generelle Regelung in entsprechenden Fällen in § 58 Abs. 3 ArbGG die Möglichkeit des Urkundenbeweises gesetzlich geregelt.

§ 58 Abs. 3 ArbGG lautet: „Insbesondere über die Zahl der in einem Arbeitsverhältnis stehenden Mitglieder oder das Vertretensein einer Gewerkschaft in einem Betrieb kann Beweis auch durch die Vorlegung öffentlicher Urkunden angetreten werden.“

Nach § 415 Abs. 1 ZPO liegt dann eine öffentliche Urkunde vor, wenn sie von einer öffentlichen Behörde innerhalb des zugewiesenen Geschäftskreises in der vorgeschriebenen Form aufgenommen ist. Mit öffentlichem Glauben versehene Personen sind diejenigen, die durch Gesetz zu Beurkundungen ermächtigt sind. Dazu zählen insbesondere die Notare. Zu den Amtsbefugnissen der Notare gehört die Erstellung einer Tatsachenbescheinigung der vorliegenden Art. Zu ihren Aufgaben gehört auch die Ausstellung einer Bescheinigung über amtlich von ihnen wahrgenommene Tatsachen (§ 20 Abs. 1 Satz 2 BNotO). Die Wahrnehmung ist amtlich, wenn der Notar auftragsgemäß in seiner Eigenschaft als Notar tätig geworden ist. Zu den von ihm wahrgenommenen Tatsachen zählen auch nichtrechtsgeschäftliche Erklärungen. Nach § 415 Abs. 1 ZPO begründet eine öffentliche Urkunde den vollen Beweis des von Notar beurkundeten Vorganges, die hier darin bestehen kann, dass die Gewerkschaft ihm eine pseudonymisierte Mitgliederliste zur Einsicht vorgelegt hat, deren Inhalt er bestätigt (vgl. jedoch auch die diesbezüglichen Bedenken bei Fischer, Die DGB-Gewerkschaften und das Tarifeinheitsgesetz, NZA 2015, 662). Natürlich könnte die Gewerkschaft den unmittelbaren Beweisantritt auch durch Vorlage ihrer Mitgliederbücher führen, was jedoch das Einverständnis der Mitglieder voraussetzt.

Zulässigkeit von Teilnehmerverzeichnissen

RA Dr. Georg Wronka, Bonn*

1. Sachverhalt

Die Veranstalter von Seminaren, Workshops und sonstigen Informationsveranstaltungen registrieren die Namen und Kontaktdaten derjenigen, die sich als Teilnehmer anmelden, zu verschiedenen Zwecken. Im Vordergrund dürften die ordnungsgemäße Abrechnung und der Versand organisatorischer Hinweise stehen. Dass die Speicherung und Nutzung der Teilnehmerdaten für diese Zwecke datenschutzrechtlichen Bedenken begegnen, lässt sich wohl schwerlich behaupten; § 28 Abs. 1 Satz 1 Nr. 1 BDSG sollte eine ausreichende Rechtsgrundlage bieten. Die Anbieter solcher Veranstaltungen drucken die Namen der Registrierten aber häufig auch in Teilnehmerlisten aus, die zur Feststellung der Anwesenheit der Angemeldeten und zur Erleichterung der Kommunikation innerhalb des Teilnehmerkreises dienen sollen. Die Handhabung solcher Listen erfolgt in unterschiedlicher Weise – und stößt nicht selten auf Vorbehalte der Teilnehmer, die überhaupt nicht daran interessiert sind, dass ihre Namen und ggf. weitere Merkmale z.B. gegenüber ihnen unbekannten Dritten offen gelegt werden. Kaum ein Veranstalter bedenkt die Reichweite seiner Befugnisse beim Umgang mit Teilnehmerlisten und informiert über ihren geplanten Einsatz vorab die Betroffenen. In Ermangelung einer Einwilligung – die erkennbar so gut wie nie (rechtswirksam) eingeholt wird – muss die datenschutzrechtliche Zulässigkeit der Verarbeitung und Nutzung in § 28 BDSG gesucht (und gefunden) werden.

2. Inhalte der Listen – Datenumgangsformen

Manche der üblichen Verzeichnisse beschränken sich auf alphabetisch sortierte Namenswiedergaben. Einige enthalten zusätzliche Hinweise auf das den Betroffenen entsendende Unternehmen bzw. seine Dienststelle, ggf. angereichert durch eine Abteilungszugehörigkeit oder die dort ausgeübte Funktion. Bei anderen werden diese Angaben noch um individuelle Kontaktdaten wie Anschrift oder Email-Adresse ergänzt.

Dient das Verzeichnis dem Veranstalter bzw. einem seiner Mitarbeiter zur Anwesenheitskontrolle, so liegt sowohl in der Erstellung der Liste auf der Basis der Anmeldungen als auch in ihrem Gebrauch „vor Ort“ eine Datennutzung (§ 3 Abs. 5 BDSG). Soll die Datenzusammenstellung aus organisatorischen Gründen zum gleichen Zweck einem Dritten – etwa dem Referenten – ausgehändigt werden, ist darin entweder eine Datenübermittlung oder ein nach § 11 BDSG zu beurteilender Auftragsprozess zu sehen. Werden die Verzeichnisse allen Teilnehmern zugänglich gemacht, etwa durch Auslegen oder Zirkulation, erfahren diese die dort abgebildeten Daten der übrigen Gelisteten, so dass der gesetzliche Tatbestand der Übermittlung erfüllt ist – wiederum mit der Folge des Erfordernisses einer Zulässigkeitsprüfung durch die verantwortliche Stelle.

3. Erlaubnisrahmen

Eine verbindliche, allgemeingültige Regel, welche (Detail-)Angaben zu den Betroffenen in einer Teilnehmerliste vermerkt werden dürfen, lässt sich nicht treffen. Maßgeblich sind die Zwecke, die im konkreten Fall mit den ausgewiesenen Daten verfolgt werden und der Personenkreis, der sie zur Kenntnis nehmen soll.

Die Zulässigkeit richtet sich, wie gesagt, danach, ob der Einsatz mehr oder weniger gegliederter Listen vereinbar ist mit § 28 Abs. 1 Satz 1 Nr. 1, Abs. 1 Nr. 2 und/oder Abs. 2 Nr. 1 bzw. Nr. 2a BDSG. Dabei ist zu unterscheiden:

Eine mit der Liste erfolgende Datennutzung und ggf. -übermittlung zum Zweck der bloßen Anwesenheitskontrolle ist als für die Durchführung des Veranstaltungsvertrages „erforderlich“ gem. § 28 Abs. 1 Satz 1 Nr. 1 BDSG anzusehen. Schließlich soll die Feststellung der Präsenz dem Nachweis der Inanspruchnahme der bestellten Leistung dienen und evtl. auch den Anspruch auf die Erteilung entsprechender Bescheinigungen begründen. Allerdings ist für diesen Zweck eine Liste ausreichend, in der nur die Daten vermerkt sind, die eine eindeutige Identifizierung ermöglichen, d.h. ein Verzeichnis ist in aller Regel auf die Namensangaben zu reduzieren, weitere Zusatzmerkmale sind nicht „erforderlich“.

Sollen die Teilnehmer ihr Erscheinen eigenhändig auf einem ausliegenden oder zirkulierenden Namensverzeichnis (ohne Zusatzmerkmale) dokumentieren (abhaken, Unterschrift), wird die damit verbundene Datenübermittlung nur dann als „erforderlich“ im Rahmen der vertraglichen Zweckbestimmung anzusehen sein, wenn der Veranstalter die Anwesenheitskontrolle nicht oder nur unter sehr erschwerten Bedingungen durchführen kann. Eine solche Situation kann z.B. bei großen Teilnehmerzahlen entstehen. Im Zweifel kann man bei solchen Konstellationen auch auf § 28 Abs. 1 Satz 1 Nr. 2 bzw. Abs. 2 BDSG „ausweichen“. Berechtigte Interessen des Veranstalters an einer solchen Vorgehensweise liegen fraglos vor. Für die Annahme ihr entgegen stehender stärker zu gewichtender schutzwürdiger Interessen der Betroffenen gibt es auch keinen Anlass – Veranstaltungsteilnehmer müssen schon auf Grund ihres Erscheinens damit rechnen, erkannt zu werden, und können sich schwerlich auf ein besonderes Geheimhaltungs- oder Vertraulichkeitsinteresse berufen.

Differenzierter zu beurteilen ist ein Teilnehmerverzeichnis, in dem ohne Kenntnis des Betroffenen diverse Zusatzangaben hinter seinem Namen vermerkt sind, z.B. Beruf, Funktion, Anschrift, Tel.-Nr. oder Email-Adresse – Merkmale, die der Veranstalter (ob rechtmäßig oder datenschutzrechtlich fragwürdig, mag dahinstehen) bei der Anmeldung erhoben hatte. Die un-

* Der Autor ist Rechtsanwalt mit dem Tätigkeitsschwerpunkt Datenschutzrecht.

gefragte Ausweisung eines Teilnehmers als Geschäftsführer, Leiter der Personalabteilung oder Betriebsratsmitglied gegenüber dem ihm unbekannten Teilnehmerkreis findet nicht zwangsläufig seine Billigung, im Gegenteil: Die Annahme von der Übermittlung entgegen stehenden Interessen kann keineswegs von vornherein ausgeschlossen werden. Das gilt umso mehr, wenn ohne seine Beteiligung auch Kontaktdaten ausgedruckt werden. Vielleicht ist es für den Referenten hilfreich, seine Zuhörer besser einordnen und seinen Vortrag ggf. spezifischer ausrichten zu können, und viele Teilnehmer würden nähere Informationen über ihr Umfeld wohl auch begrüßen, weil dadurch ein persönlicher Erfahrungsaustausch gefördert werden könnte.[1] Es ist aber mitnichten sicher, dass dies jeder für wünschenswert hält – und spätere Kontaktaufnahmen nach Abschluss einer Veranstaltung können auch als lästig empfunden werden.

4. Empfehlungen

Will ein Veranstalter Teilnehmer-qualifizierende Angaben im Zusammenhang mit einer Schulung, einem Vortrag, einem Seminar o.ä. bekannt machen, sollte er unbedingt die Betroffenen einbeziehen. Dazu benötigt er keine förmliche Einwilligung, es reicht aus, wenn er einen entsprechenden Hinweis in den Anmeldebestätigungen oder schon in der Ausschreibung (z.B. auf Prospekten und Anmeldeformularen) platziert. Der Interessent hat dann Gelegenheit, sich darauf einzustellen: Entweder akzeptiert er die Vorgehensweise, oder er äußert seine Ablehnung – ggf. durch Verzicht auf eine Anmeldung. Prinzipiell ist es irrelevant, ob „angereicherte" Teilnehmerverzeichnisse ausgelegt werden, den Veranstaltungsunterlagen beigefügt sind, unter den Teilnehmern zirkulieren oder ihnen gezielt ausgehändigt werden, entscheidend ist der stets ja gleiche Effekt, nämlich die Einräumung von Verfügungsmacht über die Daten und damit die Eröffnung von Missbrauchsmöglichkeiten. Hinweise der Veranstalter darauf, dass die Daten nur für veranstaltungsinterne Zwecke genutzt werden dürfen, dürften mangels effizienter Kontrolle in der Praxis leer laufen.

Eine abschließende Bemerkung: Dem Veranstalter ist es natürlich unbenommen, in den Teilnehmerlisten Rubriken vorzusehen, in die die Teilnehmer nähere Angaben zu ihrer Person selbst eintragen können. Volenti non fit iniuria.

1 Eine Berufung auf § 28 Abs. 1 Satz 1 Nr. 1 BDSG als Legitimationstatbestand, so Bergmann/Möhrle/Herb, BDSG, § 28 Rn. 170, überstrapaziert die Norm, namentlich das Erforderlichkeitsmerkmal.

Neue gesetzliche Anforderungen an den Personendatenschutz und die Lokalisierung von Datenbanken in Russland

Dr. Thomas Söbbing, LL.M., Frankfurt a.M.

In der Russischen Föderation wurde das föderale Gesetz Nr. 242-FS vom 21.07.2014 – nachfolgend nur „FS-242" – im Juli 2014 zum Datenschutz verabschiedet, welches nun zum 1. September 2015 in Kraft tritt. Das Gesetz ist auch deshalb so bedeutend für ausländische Unternehmen, weil bei der Verarbeitung personenbezogener Daten russischer Staatsbürger, das verarbeitende Unternehmen verpflichtet wird, diese Daten künftig auf Servern innerhalb der Russischen Föderation zu speichern. Da viele Unternehmen heute ihre Serverlandschaften virtualisiert haben und die Server auf der ganzen Welt verteilt sind (Stichwort „Cloud Computing"), stellt dieses neue Gesetz internationale Konzerne vor erheblichen Herausforderungen.

Die meisten russischen Gesetze zum Datenschutz wurden in den Jahren 2005 und 2006 erlassen. So auch das russische Bundesgesetz über die persönlichen Daten (Föderales Gesetz Nr. 152-FS nachfolgend „FS-152"), welches am 27. Juli 2006 in Kraft gesetzt wurde. Das FS-152 bildet das Rückgrat der russischen Datenschutzgesetze und fordert vom Operator (siehe Art. 3.2), *„alle für den Schutz der personenbezogenen Daten gegen unrechtmäßigen oder versehentlichen Zugriff die notwendigen organisatorischen und technischen Maßnahmen zu ergreifen"*. Dabei ist der Operator gem. Art. 3.2 jede Behörde, natürliche oder juristische Person, die allein oder gemeinsam mit anderen die Verarbeitung organisiert und/oder Personenbezogene Daten verarbeitet sowie über die Zwecke der Verarbeitung, die Bestandteile der zu verarbeitenden Personenbezogenen Daten und das Vorgehen in Bezug auf die Personenbezogenen Daten entscheidet. Der Russia's Federal Service for Supervision of Communications, Information Technology and Mass Media (russisch: *Роскомнадзор oder „Roskomnadsor"*) ist dabei die Regierungsbehörde, die mit der Überwachung beauftragt worden ist.

Nun hat die Verabschiedung des FS-242 vom 21.07.2014 *„Über die Änderung einzelner Gesetzgebungsakte der Russischen Föderation über die Verarbeitung von personenbezogenen Daten in Informations- und Telekommunikationsnetzwerken"* Auswirkungen auf folgende Russische Datenschutzgesetze:

- Föderales Gesetz Nr. 152-FS „Über personenbezogene Daten" vom 27.07.2006

- Föderales Gesetz Nr. 149-FS „Über Informationen, Informationstechnologien und den Schutz von Informationen“ vom 27.06.2006 nachfolgend „FS-149“
- Föderales Gesetz Nr. 294-FS „Über den Schutz der Rechte von juristischen Personen und Einzelunternehmern bei der Ausübung der staatlichen Kontrolle (Aufsicht) und der kommunalen Kontrolle“ vom 26.12.2008 nachfolgend „FS-294“

Nach Änderungen in FS-152 ist der Operator von personenbezogenen Daten (ab dem 1. September 2015) bei der Erhebung dieser Daten (auch per Internet) verpflichtet, die Aufnahme, Systematisierung, Erhebung, Speicherung, Anpassung (Aktualisierung, Änderung) und Abfrage von personenbezogenen Daten russischer Staatsbürger mit Hilfe von Datenbanken, die sich auf dem Hoheitsgebiet der Russischen Föderation befinden, sicherzustellen. Mit der Änderung des FS-149 wird ein Register eingeführt, welches Personen, die die Rechte von Subjekten in Bezug auf deren personenbezogene Daten verletzt haben, registriert. Die Änderung in FS-294 hat zur Folge, dass Unternehmen eine Reihe von Verfahrensgarantien, die bisher bei Prüfungen durch Roskomnadsor gewährt wurden, verlieren.

Gemäß den Änderungen in FS-242 ist der Operator von personenbezogenen Daten (FS-242) ab dem 1. September 2015 bei der Erhebung dieser Daten (auch per Internet) verpflichtet, die Aufnahme, Systematisierung, Anhäufung und Speicherung, Anpassung und Abfrage von personenbezogenen Daten russischer Staatsbürger mit Hilfe von Datenbanken, die sich auf dem Hoheitsgebiet der Russischen Föderation befinden, sicherzustellen. Dabei muss ab dem 1. September 2015 die Benachrichtigung u.a. Angaben über den Standort der Datenbanken enthalten, auf denen die personenbezogenen Daten russischer Staatsbürger gespeichert werden. Die Operatoren von personenbezogenen Daten müssen diese Angaben ab der ersten Übermittlung der Benachrichtigung nach dem 1. September 2015 übermitteln, oder auf Verlangen von Roskomnadsor innerhalb der von der Behörde genannten Fristen, wenn die Benachrichtigung vor dem 1. September 2015 übermittelt wurde. Diese Lokalisierungsanforderungen finden keine Anwendung, wenn die Verarbeitung der personenbezogenen Daten erforderlich ist:

- um die durch einen internationalen Vertrag der Russischen Föderation oder ein Gesetz vorgesehenen Ziele zu erreichen, um die dem Operator durch die gesetzlichen Vorschriften der Russischen Föderation auferlegten Funktionen, Befugnisse und Pflichten auszuüben und zu erfüllen
- zur Rechtsprechung und zur Vollstreckung von Gerichtsentscheidungen
- bei der Erbringung von staatlichen und kommunalen Leistungen
- zur Ausübung der Berufstätigkeit eines Journalisten und/oder der legalen Tätigkeit von Massenmedien oder einer schöpferischen Tätigkeit

Nach einer Aussage der in Russland tätigen Kanzlei Beiten und Burkhart sollen eBay, PayPal, AliExpress, Google und andere Unternehmen bereits ihre Zustimmung zur Verarbeitung von personenbezogenen Daten russischer Staatsbürger auf Servern in Russland erklärt haben.

Aus den aktuellen Berichten der Aufsichtsbehörden (20): Weitere Anmerkungen zum betrieblichen/behördlichen Datenschutzbeauftragten

Ausgewählt und kommentiert von Prof. Peter Gola*

Interessenkonflikte des DSB

Inwieweit bei einem „nebenamtlichen“ DSB auf Grund seiner sonstigen Aufgaben durch Interessenkonflikte die gesetzlich geforderte Zuverlässigkeit beeinträchtigt sein kann, beschäftigt die Aufsichtsbehörden immer wieder.

Probleme der Interessenkollision können sich auch bei der Bestellung behördlicher Datenschutzbeauftragter ergeben. Vor diese Frage sah sich der bayerische Landesbeauftragte für den Datenschutz gestellt, nachdem er feststellte, dass kleinere Gemeinden zunehmend den Hauptamtsleiter zum behördlichen DSB bestellen. Hiervon rät er jedoch mit u.a. folgen Argumenten ab *(26. TB, 2014, Ziff. 2.3.11):* Als selbstverständlich sieht er es zunächst an, dass die datenschutzrechtlich Verantwortlichen (z.B. der Bürgermeister) nicht zu Datenschutzbeauftragten bestellt werden, da sie sich selbst nicht wirksam kontrollieren können. Außerdem ist der Datenschutzbeauftragte der Leitung der öffentlich Stelle oder deren ständiger Vertretung bzw. in Gemeinden ggf. auch einem berufsmäßigen Gemeinderatsmitglied zu unterstellen. Ein Hauptamtsleiter sei zwar bereits in dieser Funktion dem Bürgermeister direkt unterstellt, allerdings aber auch in der Regel Interessenkonflikten ausgesetzt, da er gleichzeitig in verantwortlicher Position Aufgaben

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

in anderen Bereichen wahrnehme. So entscheide er im Regelfall über die Einstellung, Einstufung, Beförderung oder Entlassung von Bediensteten zumindest mit. Überdies dürfte der Hauptamtsleiter häufig nicht über genügend Zeit auch noch zur Ausübung der Tätigkeit eines Datenschutzbeauftragten verfügen.

Bestellpflicht bei kleinem Webbetreiber

Keine Verpflichtung zur Bestellung eines DSB sah der Betreiber eines webbasierten Firmenverzeichnisses, da er nach seiner Ansicht keine personenbezogenen Daten erhebe oder verarbeite. Über die Webseite könnten ausschließlich Adressen und Kontaktdaten von Unternehmen recherchiert werden. Das Unabhängige Landeszentrum Datenschutz Saarland (25. TB, 2013/14, Ziff. 12.4.1) machte jedoch deutlich, dass der Personenbezug der Daten allein schon dadurch bestehen könne, dass bei einer Einzelfirma oder bei einem Einzelkaufmann gewerbliche Informationen und personenbezogene Daten des Inhabers deckungsgleich seien. Darüber hinaus können beispielsweise auch von dem Namen einer „Ein-Mann-GmbH" Rückschlüsse auf den dahinter stehenden Gesellschafter gezogen werden.

Für die Anwendung des BDSG ist nicht entscheidend, wie groß der Anteil personenbezogener Daten an der Gesamtmenge der Firmendaten ist; ausschlaggebend für die Bewertung ist allein, dass überhaupt personenbezogene Daten erhoben und verarbeitet werden.

Folge des geschäftsmäßigen Umgang mit personenbezogenen Daten nach § 29 BDSG ist damit auch die Verpflichtung, das Verfahren der automatisierten Verarbeitung personenbezogener Daten nach § 4d Abs. 1 in Verbindung mit Abs. 4 Nr. 1 BDSG der Aufsichtsbehörde zu melden und für das Unternehmen nach § 4f Abs. 1 Satz 6 BDSG einen Beauftragten für den Datenschutz zu bestellen.

Eingeräumt wurde von der Aufsichtsbehörde, dass die erfolgte Anordnung der Bestellung eines Datenschutzbeauftragten für eine verantwortliche Stelle, die ohnehin lediglich einige wenige Mitarbeiter beschäftigt, im Hinblick auf den in § 9 Satz 2 BDSG normierten Verhältnismäßigkeitsgrundsatz auf den ersten Blick unverhältnismäßig erscheinen mag. Faktoren wie die mit der Bestellung verbundenen Kosten, die Unternehmensgröße oder die Art der betroffenen Daten, mit denen umgegangen wird, spielen bei der Bestellpflicht jedoch keine Rolle, wenn die Voraussetzungen des § 4f Abs. 1 Satz 6 BDSG vorliegen.

Trotz entsprechender Aufforderung wurde von der verantwortlichen Stelle weder das Verfahren im Sinne der Vorschrift gemeldet noch die Bestellung eines Beauftragten für den Datenschutz nachgewiesen, so dass schließlich gegenüber dem Betreiber der Webseite eine Anordnung auf Grundlage des § 38 Abs. 5 Satz 1 BDSG erlassen wurde. Erst nachdem ein Zwangsgeld fällig gestellt wurde, wurde seitens des Betreibers ein Beauftragter für den Datenschutz bestellt, welcher sodann auch das Verfahren im Sinne des § 4 Abs. 1 in Verbindung mit Abs. 4 BDSG meldete.

Keine Bestellpflicht bei „normaler" Videoüberwachung

Bei einer Videoüberwachung ist auch unabhängig von der Anzahl der bei der Verarbeitung personenbezogener Daten beschäftigten Personen zur Wahrnehmung der zumeist erforderlichen Vorabkontrolle ein Datenschutzbeauftragter zu bestellen *(vgl. Gola/Schomerus, BDSG, 12. Aufl. Rdn. 32)*. Das BayLDA sieht diese Verpflichtung bei „einfacher" Videoüberwachung einer kleinen Tankstelle noch nicht, d.h. es geht beim Einsatz einer Videoüberwachung nicht generell von einer Vorabkontrollpflicht nach § 4d Abs. 5 und 6 BDSG aus. Für eine Vorabkontrollpflicht wegen des Einsatzes von Videokameras müssten weitere Umstände, z. B. besonders intensive Überwachungsformen, hinzukommen, damit von besonderen Risiken für die Rechte und Freiheiten der Betroffenen im Sinne von § 4d Abs. 5 BDSG durch die Videoüberwachung gesprochen werden könne. Beispiele nennt das LDA jedoch keine.

Die fehlende Bestellung eines DSB entlässt den Tankstellenbetreiber jedoch nicht aus der Verpflichtung, die Videoüberwachung in einem Verfahrensverzeichnis zu dokumentieren und einsehbar zu halten (§ 4g Abs. 2 BDSG). Das BayLDA äußert sich hierzu zu dem vorliegenden Fall nicht. Die von der BfDI Niedersachsen (21. Tätigkeitsbericht, 2011/12 • 2. Datenschutz in der Wirtschaft, S. 75) gemachte Erfahrung zeigt auf, dass es hieran in kleineren Betrieben durchweg fehlt, wobei hinzukomme, dass der Mehrzahl der Unternehmen die Vorschriften des BDSG nicht einmal bekannt waren. Wünschenswert wäre es nach Ansicht der NdsBfDI, bei der Gründung von Unternehmen zum Beispiel bei der Gewerbeanmeldung oder auch bei Schulungen für Existenzgründer auf die entsprechenden Vorschriften hinzuweisen.

Widerruf der Bestellung bei langfristiger Erkrankung

Erkrankt der DSB längerfristig, so besteht zweifelsohne Handlungsbedarf der verantwortlichen Stelle. Die Lösung wird zunächst regelmäßig in der Bestellung eines befristet berufenen Stellvertreters *(BayLDA, TB 2013/14, Ziff. 4.3)* liegen. Eine über viele Monate andauernde langfristige Erkrankung mit nicht absehbarem Rückkehrzeitpunkt kann jedoch die zuverlässige Aufgabenerfüllung des Datenschutzbeauftragten im Sinne von § 4f Abs. 2 Satz 1 BDSG ausschließen, so dass für die verantwortliche Stelle ein Widerruf der Bestellung aus wichtigem Grund und eine Neubestellung einer anderen Person geboten sein kann.

Einsicht in Personalakten

Bestätigt wird durch das BayLDA *(TB 2013/14, Ziff. 4.4)*, dass auch Personalakten von dem betrieblichen Datenschutzbeauftragten im Rahmen seiner Kontrollbefugnisse auf ihre korrekte Führung überprüft werden können. Das gilt auch für behördliche DSB *(Gola/Schomerus, BDSG, 12. Aufl., § 4g Rdn. 10f)*. Das LDA verweist insoweit auf eine Entscheidung des BAG *(RDV 1990, 184)*, nach der die Revisionsstellen einer Sparkasse im

Rahmen ihres Prüfungsauftrags als befugt angesehen werden, im Einzelfall Personalakten stichprobenartig zur Nachprüfung der Personalaufwendungen einzusehen, d.h. auch hier gilt der Grundsatz der Verhältnismäßigkeit, d.h. der Beauftragte nimmt Stichproben vor oder wird anlassbezogen tätig. Das BAG weist auch darauf hin, dass sofern besonders vertrauliche Informationen in der Personalakte enthalten sind, besondere Vorkehrungen erforderlich sind, um den besonderen Schutz für sensible Daten zu gewährleisten. Konkret bedeutet dies: Enthalten die Personalakten Gesundheitszeugnisse, so kann des DSB die Tatsache selbst auf ihre Korrektheit prüfen, nicht aber vom Inhalt des Vorgangs Kenntnis nehmen.

Auditierung der DSB-Tätigkeit

Das BayLDA *(TB 2013/14, Ziff. 4.1)*. betont zur derzeitigen Rechtslage zutreffend, dass sich ein Datenschutzbeauftragter anlässlich der Auditierung seines Unternehmens durch externe Prüfer nicht uneingeschränkt dem Auditierungsverfahren unterziehen lassen muss. Aufgrund der besonderen Rechtsstellung des Datenschutzbeauftragten nach § 4f BDSG, insbesondere der weisungsfreien Ausübung der Fachkunde auf dem Gebiet des Datenschutzes gemäß § 4f Abs. 3 Satz 2 BDSG und der besonderen Verschwiegenheitspflicht gemäß § 4f Abs. 4 BDSG sei eine Auditierung seiner Tätigkeit nur in allgemeiner Form möglich. Ausgeschlossen sein muss u.a. die Möglichkeit einer inhaltlichen Kenntnisnahme der beim Datenschutzbeauftragten anhängigen oder bearbeiteten Eingaben und Beschwerden.

Mangelhafte Datenschutzorganisation einer Gewerkschaft

Der Bericht des Berliner Beauftragten für Datenschutz und Informationsfreiheit über die Überprüfung der Datenschutzorganisation der Dienstleistungsgewerkschaft Ver.di (BlnBDI 2014, Ziff. 6.6) zeigt ein Beispiel dafür, dass das, was man von anderen fordert, für sich selbst nicht gelten muss. Aus den festgestellten organisatorischen und strukturellen Mängeln seien zwei berichtet.

Gerügt wurde, dass es alleine einem betrieblichen Datenschutzbeauftragten nebst einem Sachbearbeiter in der Zentrale in Berlin übertragen war, auf den datenschutzkorrekten Umgang mit den Daten von über zwei Millionen Mitgliedern und mehreren tausend Beschäftigten in einer Vielzahl von Geschäftsstellen „hinzuwirken". Als erforderlich angesehen wurde eine ergänzende dezentrale Organisation mit „Vertrauensleuten" vor Ort bei den Landesverbänden.

Eine weitere Beanstandung betraf die Tatsache, dass allen Beschäftigten, die mit der Mitgliederbetreuung betreut sind, ein unbeschränkter Lesezugriff zur Mitgliederdatei eingeräumt ist. Erreicht werden sollte dadurch, dass Mitgliedern unabhängig von deren originär zuständiger Geschäftsstelle bundesweit ein allgemeiner Service geboten werden könne. Der legitime Servicegedanke befreit nach dem BlnBDI nicht davon, durch geeignete Maßnahmen missbräuchlichen Datenabrufen vorzubeugen. Dies kann durch die Protokollierung aller getätigten Leseabrufe und regelmäßige Stichprobenkontrollen durch den betrieblichen Datenschutzbeauftragten geschehen.

Zum Schluss ein Fall, in dem ein DSB wohl zu viel Eifer an den Tag legte.

Amtsanmaßung eines selbstständigen Datenschutzbeauftragten

Der Fall eines selbständigen Datenschutzbeauftragten, der in seiner Aufgabenwahrnehmung weit über das Ziel hinausgeschossen ist, beschäftigte das Unabhängige Datenschutzzentrum Saarland *(23. TB, 2013/14, Ziff. 2.4.2)*. Anlass war der Anruf eines sehr erbosten Einzelhändlers, der sich über das seines Erachtens ungerechtfertigte und ungewöhnliche Vorgehen eines angeblichen Mitarbeiters der Aufsichtsbehörde erregte. Der Anrufer erklärte, er habe hinsichtlich der in seinem Laden angebrachten Videoüberwachungsmaßnahme und wegen des Impressums seiner Webseite mehrfach E-Mails von einem Mitarbeiter der Datenschutzaufsicht erhalten, in denen Bußgelder und Abmahnungen angedroht würden.

Da das Datenschutzzentrum bislang mit dem Ladeninhaber nicht in Kontakt gestanden hatte, geschweige denn ein Verwaltungsverfahren gegen diesen führte, wurde der Ladeninhaber um Zurverfügungstellung der besagten E-Mails gebeten. Aus diesen ging hervor, dass ein selbstständiger Datenschutzbeauftragter diese E-Mails an den Ladeninhaber adressierte und darin, entsprechend der Schilderung des Ladeninhabers, Bußgelder androhte. Zudem vermittelte der Verfasser der E-Mails durch seine Wortwahl bewusst den Eindruck, dass er im gesetzlichen Auftrag handelt und einer staatlichen Stelle Meldung über das Verhalten des Ladeninhabers erstatten müsse.

Auf Grundlage dieser E-Mails wurde der Vorgang wegen Verdachts der Amtsanmaßung an die Staatsanwaltschaft weitergegeben. Die Staatsanwaltschaft folgte der rechtlichen Bewertung des Sachverhalts durch das Datenschutzzentrum und beantragte im Hinblick auf die im Raum stehende Amtsanmaßung den Erlass eines Strafbefehls.

Das zuständige Amtsgericht beraumte die Hauptverhandlung an, um dem Datenschutzbeauftragten Gelegenheit zur Stellungnahme zu geben. Das Gericht sah jedoch abschließend den Tatvorwurf der Amtsanmaßung bestätigt und verurteilte den Datenschutzbeauftragten zu einer Geldstrafe. Der Datenschutzbeauftragte legte gegen dieses Urteil Berufung ein, über dessen Ergebnis der Tätigkeitsbericht nicht mehr vermeldet.

Rechtsprechung

Bildveröffentlichung zufällig mit erfasster nicht prominenter Personen

(**Bundesgerichtshof**, Urteil vom 21. April 2015 – VI ZR 245/14 –)

Zur Frage der Zulässigkeit der Veröffentlichung von Bildern, die eine sich zufällig in der Nähe eines Prominenten befindliche nicht prominente Person identifizierbar zeigen.

Sachverhalt:

Die Klägerin nimmt die Beklagten wegen unzulässiger Veröffentlichung eines Fotos in Anspruch, das sie in Badekleidung (Bikini) auf einer Liege am Strand von El Arenal auf Mallorca zeigt.

Die Print-Ausgabe der Zeitung „BILD", deren Herausgeberin die Beklagte zu 1 ist, berichtete am 10. Mai 2012 über einen Raubüberfall auf den Profifußballer A. in El Arenal („Am Ballermann"). Darin heißt es u.a.:

„Sonne, Strand, Strauchdiebe. Gestern sahen wir ... – Star A. (25) in pikanter Frauen-Begleitung am Ballermann. Jetzt wurde er Opfer einer Straftat."

Diesem Artikel war das beanstandete Foto beigefügt, das im Vordergrund A. am Strand von El Arenal vor einer Mülltonne zeigt, in die er einen Eimer leert. In dem Bildabschnitt, der die Mülltonne zeigt, findet sich der Text:

„Strohhut, dunkle Sonnenbrille: A. am Strand von El Arenal. Vorbildlich entsorgt er seinen Abfall".

Im Hintergrund sind mehrere Personen auf Strandliegen zu sehen. Am rechten Bildrand, auf der Liege unmittelbar hinter A., ist die Klägerin in einem Bikini zu erkennen.

Ein Artikel mit demselben Berichtsgegenstand und einem größeren Ausschnitt desselben Fotos wurde bis zum 9. Mai 2013 im Internet-Portal www.bild.de veröffentlicht, das von der Beklagten zu 2 betrieben wird.

Aus den Gründen:

Das Berufungsgericht hat ohne Rechtsfehler einen Unterlassungsanspruch der Klägerin gegen die Beklagte zu 1 aus § 1004 und § 823 Abs. 2 BGB i.V.m. § 22, 23 KUG bejaht.

1. Dabei ist es 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. 26, vom 28. Mai 2013 – VI ZR 125/12, VersR 2013, 1178 Rn. 10, und vom 8. April 2014 – VI ZR 197/13, VersR 2014, 890 Rn. 8; jeweils m.w.N.), das sowohl mit verfassungsrechtlichen Vorgaben (vgl. BVerfGE 120, 180, 210) als auch mit der Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte im Einklang steht (vgl. EGMR NJW 2004, 2647 Rn. 57 ff.; 2006, 591 Rn. 37 ff., sowie NJW 2012, 1053 Rn. 95 ff., und 1058 Rn. 75 ff.). Danach dürfen Bildnisse einer Person grundsätzlich nur mit deren Einwilligung verbreitet werden (§ 22 Satz 1 KUG). Die Veröffentlichung des Bildes von einer Person begründet grundsätzlich eine rechtfertigungsbedürftige Beschränkung ihres allgemeinen Persönlichkeitsrechts (vgl. BVerfG NJW 2011, 740 Rn. 52 m.w.N.). Die nicht von der Einwilligung des Abgebildeten gedeckte Verbreitung seines Bildes ist nur zulässig, wenn dieses Bild dem Bereich der Zeitgeschichte oder einem der weiteren Ausnahmetatbestände des § 23 Abs. 1 KUG positiv zuzuordnen ist und berechtigte Interessen des Abgebildeten nicht verletzt werden (§ 23 Abs. 2 KUG). Dabei ist schon bei der Beurteilung, ob ein Bild dem Bereich der Zeitgeschichte zuzuordnen ist, eine Abwägung zwischen den Rechten des Abgebildeten aus Art. 1 Abs. 1, Art. 2 Abs. 1 GG, Art. 8 Abs. 1 EMRK einerseits und den Rechten der Presse aus Art. 5 Abs. 1 GG, Art. 10 EMRK andererseits vorzunehmen (vgl. z.B. Senatsurteil vom 19. Juni 2007 – VI ZR 12/06, VersR 2007, 1135 Rn. 17; ausführlich dazu v. Pentz, AfP 2013, 20, 23 f.).

a) Nach den von den Revisionen nicht angegriffenen Feststellungen des Berufungsgerichts hat die Klägerin in die Veröffentlichung der Fotos nicht eingewilligt (§ 22 Satz 1 KUG).

b) Das Foto ist auch nicht dem Bereich der Zeitgeschichte (§ 23 Abs. 1 Nr. 1 KUG) zuzuordnen. Maßgebend für die Frage, ob es sich um ein Bildnis aus dem Bereich der Zeitgeschichte handelt, ist der Begriff des Zeitgeschehens.

aa) Der Begriff des Zeitgeschehens darf nicht zu eng verstanden werden. Im Hinblick auf den Informationsbedarf der Öffentlichkeit umfasst er nicht nur Vorgänge von historisch-politischer Bedeutung, sondern ganz allgemein das Zeitgeschehen, also alle Fragen von allgemeinem gesellschaftlichem Interesse. Er wird mithin vom Interesse der Öffentlichkeit bestimmt. Zum Kern der Presse- und der Meinungsbildungsfreiheit gehört es, dass die Presse innerhalb der gesetzlichen Grenzen einen ausreichenden Spielraum besitzt, in dem sie nach ihren publizistischen Kriterien entscheiden kann, was öffentliches Interesse beansprucht, und dass sich im Meinungsbildungsprozess herausstellt, was eine Angelegenheit von öffentlichem Interesse ist, wobei unterhaltende Beiträge davon nicht ausgenommen sind (vgl. BVerfGE 101, 361, 389 ff.; BVerfG, AfP 2008, 163, 166 f. Nr. 61 ff.; Senatsurteile vom 19. Juni 2007 – VI ZR 12/06, a.a.O.; vom 3. Juli 2007 – VI ZR 164/06, a.a.O. und vom 24. Juni 2008 – VI ZR 156/06, BGHZ 177, 123 Rn. 15 ff.; jeweils m.w.N.).

bb) Nach diesen Grundsätzen ist die Beurteilung des Berufungsgerichts, die Veröffentlichung eines Fotos, das einem Millionenpublikum die – identifizierbar abgebildete – Klägerin im Bikini zeigt, sei durch den Anlass der Berichterstattung nicht gerechtfertigt, nicht zu beanstanden. Die veröffentlichten Bilder zeigen die Klägerin in einer erkennbar privaten Situation, die in keinem Zusammenhang mit einem zeitgeschichtlichen Ereignis steht (vgl. – zu einer ähnlichen Fallgestaltung – Senatsurteil vom 19. Juni 2007 – VI ZR 12/06, VersR 2007, 1135 Rn. 26).

cc) Soweit die Revisionen meinen, das Berufungsgericht habe nicht geprüft, wie der Leser den Bericht interpretiere, sondern ausschließlich auf das Foto abgestellt und den Zusammenhang zum zugehörigen Text ignoriert, aus welchem sich ergebe, dass sich die Abbildung allein auf den Fußballer A. beziehe, kann dem nicht gefolgt werden. Das Bildnis zeigt auch die Klägerin, wie sie

sich mit dem Betrachter halb zugewandtem Gesicht auf der Strandliege sonnt.

dd) Entgegen der Auffassung der Revisionen der Beklagten hat das Berufungsgericht auch nicht den Begriff des zeitgeschichtlichen Ereignisses im Sinne von § 23 Abs. 1 Nr. 1 KUG verkannt und diesen Begriff zu eng gefasst. Das beanstandete Foto als solches hatte mit dem Umstand, dass der bekannte Fußball-Star A. am „Ballermann" überfallen und ausgeraubt wurde, ersichtlich nichts zu tun. Das Berufungsgericht hat gleichwohl zugunsten der Beklagten unterstellt, dass die Veröffentlichung des Bildnisses von Herrn A. im Kontext des Berichts zulässig war und für die Entscheidung des Streitfalles zutreffend darauf abgestellt, ob der Gegenstand dieses Berichts auch die Veröffentlichung einer Abbildung der Klägerin rechtfertigt. Dies hat es mit Recht verneint. Denn es besteht außer dem zufälligen Zugegensein keine Verknüpfung zwischen der als „Urlauberin" gezeigten Klägerin und dem – unterstellt – als Ereignis der Zeitgeschichte zu qualifizierenden Raubüberfall auf den Nationalspieler A.

ee) Der Revisionen der Beklagten ist weiter nicht darin zu folgen, dass im Hinblick auf das Informationsinteresse der Öffentlichkeit an einem Bericht über ein zeitgeschichtliches Ereignis die Interessen von unbekannten Personen, die zufällig mit abgebildet werden, stets zurücktreten müssen. Vielmehr ist auch in solchen Fällen grundsätzlich eine Interessenabwägung erforderlich, bei der insbesondere der Informationswert für die Öffentlichkeit, die berechtigten Erwartungen des Betroffenen und die Möglichkeiten einer das Persönlichkeitsrecht wahrenden Modifikation des Fotos zu berücksichtigen sind. Dies steht in Einklang mit der Rechtsprechung des Senats, nach der selbst die Abbildung von Begleitpersonen nicht ohne weiteres zulässig ist. Wollte man dies anders sehen, würde dies zu dem (widersinnigen) Ergebnis führen, dass Begleitpersonen, die in einem gewissen Zusammenhang mit dem Gegenstand der Berichterstattung stehen (vgl. etwa Senatsurteil vom 19. Juni 2007 – VI ZR 12/06, VersR 2007, 1135 Rn. 28), vor einer Veröffentlichung eher geschützt wären, als Personen, die ohne jeden Zusammenhang Gegenstand einer „zufälligen" Bildaufnahme geworden sind.

c) Entgegen der Auffassung der Revisionen der Beklagten hat das Berufungsgericht auch ohne Rechtsfehler im Streitfall eine unmittelbare oder analoge Anwendung des § 23 Abs. 1 Nr. 2 KUG verneint.

aa) Nach § 23 Abs. 1 Nr. 2 KUG ist die Veröffentlichung eines Bildnisses ohne Einwilligung der abgebildeten Person grundsätzlich zulässig, wenn diese Person nur als „Beiwerk" neben einer Landschaft oder sonstigen Örtlichkeit erscheint. Hiervon kann nach dem Sinn und Zweck der Vorschrift nur dann ausgegangen werden, wenn die Abbildung einer Landschaft oder sonstigen Örtlichkeit das Bild prägt und nicht selbst „Beiwerk" ist. Im Streitfall bezog sich die Abbildung indes – wovon die Revisionen der Beklagten selbst ausgehen – in erster Linie auf Herrn A. Das Strandleben am „Ballermann" bildete lediglich den Hintergrund des Fotos.

Die Erwägungen der Revisionen der Beklagten zu der Frage, ob eine Abbildung von Badegästen im Zusammenhang mit einer Schilderung des Strandlebens zulässig wäre, sind im Streitfall unerheblich. Im unmittelbaren Anwendungsbereich von § 23 Abs. 1 Nr. 2 KUG kann ein Interesse an der Wiedergabe einer Landschaft oder sonstigen Örtlichkeit zwar unabhängig von einem konkreten Ereignis der Zeitgeschichte bestehen. Die Revisionen der Beklagten gehen jedoch selbst davon aus, dass Zweck des Bildes die Berichterstattung über den Fußballer A. im Zusammenhang mit dem auf diesen erfolgten Überfall gewesen sei.

bb) Entgegen der Auffassung der Revisionen kommt eine entsprechende Anwendung des § 23 Abs. 1 Nr. 2 KUG nicht in Betracht. Es fehlt bereits an einer Gesetzeslücke als Voraussetzung einer analogen Anwendung dieser Vorschrift. Denn dem von den Revisionen der Beklagten angeführten Interesse an der Berichterstattung über eine bestimmte Person unter Einbeziehung von Abbildungen anderer „zufällig" anwesender Personen wird bereits durch § 23 Abs. 1 Nr. 1 KUG und die dort erforderliche Interessenabwägung hinreichend Rechnung getragen.

d) Selbst wenn eine entsprechende Anwendung des § 23 Abs. 1 Nr. 2 KUG in Betracht käme, erstreckte sich die Befugnis nicht auf eine Verbreitung und Schaustellung, durch die ein berechtigtes Interesse des Abgebildeten verletzt wird (§ 23 Abs. 2 KUG).

Das Berufungsgericht hat bei seiner Beurteilung mit Recht nicht nur auf das Foto, sondern auch auf den dazugehörigen Text abgestellt und dabei angenommen, dass die Erwähnung einer „pikanten Frauenbegleitung" zumindest bei einem Teil der Leserschaft zum Anlass für Spekulationen in Bezug auf die Klägerin genommen werden könnte. Eine andere Beurteilung ist auch nicht im Hinblick auf die Formulierung geboten: „Gestern sahen wir ... – Star A. (25) in pikanter Frauen-Begleitung am Ballermann. Jetzt wurde er Opfer einer Straftat." Denn die Revisionen der Beklagten zeigen keinen (übergangenen) Sachvortrag dazu auf, dass das Foto vom Folgetag stamme und dies für den Leser ersichtlich gewesen sei.

e) Das Berufungsgericht hat auch zutreffend die Unkenntlichmachung der Klägerin durch Verpixelung oder Augenbalken für möglich und den Beklagten zumutbar erachtet. Die Revisionen berufen sich demgegenüber ohne Erfolg auf angebliche Redaktionsabläufe und die Gefahr der Verhinderung einer atmosphärischen Illustration. Eine Verpixelung hätte an der Aussagekraft des Berichts im Hinblick auf das Anliegen der Beklagten, die Urlaubsgestaltung des Fußballprofis zu illustrieren, nichts geändert. Darüber hinaus hat die Beklagte zu 2 nach den Feststellungen des Berufungsgerichts bei den im Internet im Zusammenhang mit der vorliegenden Berichterstattung veröffentlichten Bildern die Gesichter anderer dort mit dem Fußballprofi abgebildeter Frauen gepixelt, was dagegen spricht, dass ihr eine entsprechende Vorgehensweise im Hinblick auf die Abbildung der Klägerin nicht möglich oder unzumutbar gewesen wäre.

B) Revision der Klägerin:

Die Revision der Klägerin ist ebenfalls unbegründet.

1. Das Berufungsgericht hat mit Recht eine Haftung der Beklagten zu 1 hinsichtlich der Veröffentlichung der beanstandeten Bilder im Internet abgelehnt, weil nicht ersichtlich sei, dass die Beklagte zu 1 willentlich und adäquat kausal durch die Veröffentlichung der – rechtlich selbständigen – Beklagten zu 2 im Internet zu einer Persönlichkeitsrechtsverletzung der Klägerin beigetragen hätte. Allein die Tatsache, dass beiden Beklagten dieselben Lichtbilder zugänglich waren, vermag noch keine wechselseitige Haftung hinsichtlich der Veröffentlichung der Fotos zu begründen. Die Revision der Klägerin zeigt keinen vom Berufungsgericht übergangenen Sachvortrag auf, wonach die Beklagte zu 1 der Beklagten zu 2 die Lichtbilder zur Verfügung gestellt hat. Die von der Revision der Klägerin in Bezug genommene Entscheidung des I. Zivilsenats vom 11. März 2009 (I ZR 114/06, BGHZ 180, 134 Rn. 16 ff.) betrifft eine andere Fallgestaltung (Verletzung von Schutzrechten durch Pflichtverletzung des Kontoinhabers bei der Verwahrung von Zugangsdaten).

2. Entgegen der Auffassung der Revision der Klägerin hat das Berufungsgericht auch ohne Rechtsfehler den Antrag der Klägerin auf Zahlung einer Geldentschädigung für unbegründet erachtet.

a) Nach der ständigen Rechtsprechung des erkennenden Senats begründet eine Verletzung des allgemeinen Persönlichkeitsrechts einen Anspruch auf eine Geldentschädigung, wenn es sich um einen schwerwiegenden Eingriff handelt und die Beeinträchtigung nicht in anderer Weise befriedigend aufgefangen werden kann. Ob eine schwerwiegende Verletzung des Persönlichkeitsrechts vorliegt, die die Zahlung einer Geldentschädigung erfordert, hängt insbesondere von der Bedeutung und Tragweite des Eingriffs, ferner von Anlass und Beweggrund des Handelnden sowie von dem Grad seines Verschuldens ab (vgl. Senatsurteile vom 15. November 1994 – VI ZR 56/94, BGHZ 128, 1, 12; vom 30. Januar 1996 – VI ZR 386/94, BGHZ 132, 13, 27; vom 5. Oktober 2004 – VI ZR 255/03, BGHZ 160, 298, 306; vom 24. November 2009 – VI ZR 219/08, BGHZ 183, 227 Rn. 11; vom 17. Dezember 2013 – VI ZR 211/12, BGHZ 199, 237 Rn. 38 ff.; vom 22. Januar 1985 – VI ZR 28/83, VersR 1985, 391, 393; vom 15. Dezember 1987 – VI ZR 35/87 – VersR 1988, 405; vom 12. Dezember 1995 – VI ZR 223/94, VersR 1996, 341 f.; vgl. auch BVerfG, NJW 2004, 591, 592). Ob ein derart schwerer Eingriff anzunehmen und die dadurch verursachte nicht vermögensmäßige Einbuße auf andere Weise nicht hinreichend ausgleichbar ist, kann nur aufgrund der gesamten Umstände des Einzelfalles beurteilt werden (vgl. Senatsurteile vom 15. November 1994 – VI ZR 56/94, a.a.O., 13; vom 24. November 2009 – VI ZR 219/08, a.a.O.; vom 17. Dezember 2013 – VI ZR 211/12, a.a.O. Rn. 38; vom 17. März 1970 – VI ZR 151/68, VersR 1970, 675, 676; vom 25. Mai 1971 – VI ZR 26/70, VersR 1971, 845, 846; Senatsbeschluss vom 30. Juni 2009 – VI ZR 340/08, juris Rn. 3). Bei der gebotenen Gesamtwürdigung ist ein erwirkter Unterlassungstitel zu berücksichtigen, weil dieser und die damit zusammenhängenden Ordnungsmittelandrohungen den Geldentschädigungsanspruch beeinflussen und im Zweifel sogar ausschließen können (vgl. Senatsurteil vom 25. Mai 1971 – VI ZR 26/70, DB 1971, 1660, 1661; Senatsbeschluss vom 30. Juni 2009 – VI ZR 340/08, a.a.O.). Die Gewährung einer Geldentschädigung hängt demnach nicht nur von der Schwere des Eingriffs ab, es kommt vielmehr auf die gesamten Umstände des Einzelfalles an, nach denen zu beurteilen ist, ob ein anderweitiger befriedigender Ausgleich für die Persönlichkeitsrechtsverletzung fehlt (vgl. Senatsurteile vom 15. November 1994 – VI ZR 56/94, a.a.O., 12 ff.; vom 24. November 2009 – VI ZR 219/08, a.a.O.; Senatsbeschluss vom 30. Juni 2009 – VI ZR 340/08, a.a.O.).

b) Eine schwerwiegende Verletzung des Persönlichkeitsrechts der Klägerin hat das Berufungsgericht unter Würdigung der besonderen Umstände des Streitfalles mit Recht verneint. Selbst wenn man – was das Berufungsgericht offengelassen hat – zugunsten der Klägerin ihre Behauptung, sie sei im Zusammenhang mit der Veröffentlichung von mehreren Personen angesprochen und ihr sei von „mehreren Männern“ Geld für ein Treffen angeboten worden, als richtig unterstellt, vermag dies keine andere Beurteilung zu rechtfertigen. Denn das Berufungsgericht weist insoweit zutreffend darauf hin, dass die beanstandete Veröffentlichung des Strandbildes mit der Klägerin keine Veranlassung zu der Annahme gab, dass die Klägerin käuflich sei.

Eingriff in Persönlichkeitsrecht durch Bildaufnahmen

(**Bundesgerichtshof**, Beschluss vom 26. Februar 2015 – 4 StR 328/14 –)

Zur Verletzung des höchstpersönlichen Lebensbereichs durch Bildaufnahmen gemäß § 201a StGB.

Aus den Gründen:

Dass der Angeklagte durch das Anfertigen von Bildaufnahmen während der gynäkologischen Behandlung seiner Tatopfer jeweils deren höchstpersönlichen Lebensbereich verletzte, hat die Strafkammer auf der Grundlage der von ihr zu den Inhalten der Bilder und Videosequenzen getroffenen Feststellungen rechtsfehlerfrei bejaht.

Nach der Strafnorm des § 201a Abs. 1 StGB aF (§ 201a Abs. 1 Nr. 1 StGB in der Fassung des 49. Gesetzes zur Änderung des Strafgesetzbuchs – Umsetzung europäischer Vorgaben zum Sexualstrafrecht vom 21. Januar 2015, BGBl I, S. 10), welche dem Schutz des durch das allgemeine Persönlichkeitsrecht sowie das Recht auf informationelle Selbstbestimmung gewährleisteten höchstpersönlichen Lebensbereichs des Einzelnen vor Eingriffen durch Bildaufnahmen dient (vgl. BT-Drucks. 15/2466, S. 1; Lenckner/Eisele, in: Schönke/Schröder, StGB, 29. Aufl., § 201a Rn. 2; Fischer, StGB, 62. Aufl., § 201a Rn. 3; Kühl, in: Lackner/Kühl, StGB, 28. Aufl., § 201a Rn. 1), macht sich in der Tatbestandsvariante des Herstellens strafbar, wer von einer anderen Person, die sich in einer Wohnung oder einem gegen Einblick besonders geschützten Raum befindet, Bildaufnahmen herstellt und dadurch den höchstpersönlichen Lebensbereich der Person verletzt. Ob und gegebenenfalls unter welchen Voraussetzungen dieser Vorschrift auch Bildaufnahmen unterfallen, die allein aus sich heraus eine Individualisierung der abgebildeten Person nicht ermöglichen (vgl. Bosch, in: Satzger/Schluckebier/Widmaier, StGB, 2. Aufl., § 201a Rn. 5; Altenhain in Matt/Renzikowski, StGB, § 201a Rn. 2; Koch, GA 2005, 589, 595; Kargl, ZStW 2005, 324, 340; Ernst, NJW 2004, 1277, 1278; aA Hoyer in SK-StGB [Stand: Oktober 2005], § 201a Rn. 12; Kühl in Lackner/Kühl a.a.O., Rn. 4), braucht der Senat nicht zu entscheiden. Tatbestandlich erfasst werden jedenfalls solche Bildaufnahmen, die – wie hier vom Landgericht in den der Verurteilung zugrunde liegenden Fällen festgestellt – aufgrund hinreichend vorhandener Identifizierungsmerkmale von den jeweiligen Tatopfern der eigenen Person zugeordnet werden können (vgl. Valerius, in: LK, 12. Aufl., § 201a Rn. 11; Kargl, in: NK-StGB, 4. Aufl., § 201a Rn. 6; Fischer a.a.O., Rn. 5; auf grundsätzliche Identifizierbarkeit abstellend vgl. Lenckner/Eisele a.a.O., Rn. 4; Heuchemer, in: Heintschel/Heinegg, StGB, § 201a Rn. 16.2). Weiter gehende Anforderungen an die Erkennbarkeit der abgebildeten Personen lassen sich bei einer am geschützten Rechtsgut orientierten Auslegung weder aus dem Tatbestandsmerkmal der Bildaufnahme einer anderen Person noch aus dem tatbestandlich vorausgesetzten Erfolg einer Verletzung des höchstpersönlichen Lebensbereichs ableiten. Da der Rechtsgutsangriff bereits in der Fertigung der Bildaufnahme durch den Täter liegt, ohne dass es auf eine mögliche spätere Weitergabe oder Verbreitung der Aufnahme ankommt, besteht insbesondere kein Grund, den Eintritt des Taterfolgs davon abhängig zu machen, dass die Identifizierung der abgebildeten Person von Dritten anhand auch anderen bekannter Merkmale oder

Besonderheiten vorgenommen werden kann (so aber Graf in MK-StGB, 2. Aufl., § 201a Rn. 20).

Zur Zulässigkeit der Erhebung, Speicherung und Übermittlung von personenbezogenen Daten im Rahmen eines Arztsuche- und Arztbewertungsportals im Internet (www.jameda.de)

(**Bundesgerichtshof**, Urteil vom 23. September 2014 – VI ZR 358/13 –)

1. **Die Speicherung von Daten in einem Ärztebewertungsportal bestimmt sich nach § 29 BDSG, da die Übermittlung der Daten den eigentlichen Geschäftszweck ausmacht.**
2. **Die erforderliche Interessenabwägung hat einerseits dem Schutz des Rechts auf informationelle Selbstbestimmung nach Art. 2 Abs. 1, Art. 1 Abs. 1 GG, Art. 8 Abs. 1 EMRK und andererseits dem Recht auf Kommunikationsfreiheit nach Art. 5 Abs. 1 GG, Art. 10 Abs. 1 EMRK und zugleich der Drittwirkung des beiden Parteien zustehenden Grundrechts aus Art. 12. Abs. 1 GG Rechnung zu tragen.**
3. **Die Beeinträchtigung der berechtigten Interessen des Arztes wiegt nicht schwerer als das Recht des Betreibers auf Kommunikationsfreiheit.**

(Nicht amtliche Leitsätze)

Sachverhalt:

Die Parteien streiten über die Zulässigkeit der Aufnahme eines Arztes in ein Bewertungsportal gegen dessen Willen.

Die Beklagte betreibt unter der Internetadresse www.jameda.de ein Arztsuche- und Arztbewertungsportal, auf dem Informationen über Ärzte und Träger anderer Heilberufe kostenfrei abgerufen werden können. Als eigene Informationen der Beklagten werden die sogenannten „Basisdaten" angeboten. Zu ihnen gehören – soweit sie der Beklagten vorliegen – akademischer Grad, Name, Fachrichtung, Praxisanschrift, weitere Kontaktdaten sowie Sprechzeiten und ähnliche praxisbezogene Informationen. Daneben sind Bewertungen abrufbar, die Nutzer in Form eines Notenschemas und ggf. auch in Form von Freitextkommentaren abgegeben haben. Die Abgabe einer solchen Bewertung erfordert eine vorherige Registrierung, bei der eine E-Mail-Adresse angegeben werden muss, die im Rahmen des Registrierungsvorgangs verifiziert wird.

Der Kläger ist niedergelassener Gynäkologe. Im Portal der Beklagten wird er mit seinem akademischen Grad, seinem Namen, seiner Fachrichtung und seiner Praxisanschrift geführt. Im Jahr 2012 wurde er mehrfach bewertet.

Nachdem der Kläger Ende Januar 2012 erfahren hatte, im Portal der Beklagten bewertet worden zu sein, verlangte er von ihr – zuletzt mit Anwaltsschreiben – die vollständige Löschung seines Eintrags. Die Beklagte lehnte dies ab.

Aus den Gründen:

Das angefochtene Urteil hält der revisionsrechtlichen Nachprüfung stand. Zu Recht hat das Berufungsgericht die vom Kläger gegen die Beklagte geltend gemachten Ansprüche, die auf der Internetseite www.jameda.de über ihn veröffentlichten Daten zu löschen (I.), die Veröffentlichung eines „Persönlichkeitsprofils" des Klägers auf der genannten Internetseite zu unterlassen (II.) und ihm die vorgerichtlich angefallenen Rechtsverfolgungskosten zu erstatten (III.), für nicht gegeben erachtet.

I. Nach § 35 Abs. 2 Satz 2 Nr. 1 BDSG sind personenbezogene Daten zu löschen, wenn ihre Speicherung unzulässig ist. Dies ist vorliegend nicht der Fall.

1. § 35 BDSG findet – wie die übrigen Vorschriften des dritten Abschnitts des BDSG auch – im Streitfall grundsätzlich Anwendung.

a) Der Anwendungsbereich des BDSG ist nach § 1 Abs. 2 Nr. 3 BDSG, derjenige des dritten Abschnitts des BDSG nach § 27 Abs. 1 Satz 1 Nr. 1 BDSG eröffnet. Denn die Beklagte ist als juristische Person des privaten Rechts, die nicht unter § 2 Abs. 1 bis 3 BDSG fällt, gemäß § 2 Abs. 4 Satz 1 BDSG eine nicht-öffentliche Stelle und verarbeitet personenbezogene Daten im Sinne des § 3 Abs. 1 BDSG über den Kläger unter Einsatz von Datenverarbeitungsanlagen (vgl. Senatsurteil vom 23. Juni 2009 – VI ZR 196/08, BGHZ 181, 328 Rn. 17 f.; ferner Simitis/Dammann, BDSG, 8. Aufl., § 3 Rn. 7 ff.).

b) Das Medienprivileg (vgl. § 57 Abs. 1 Satz 1 Rundfunkstaatsvertrag, § 41 Abs. 1 BDSG) steht einer uneingeschränkten Anwendung des Bundesdatenschutzgesetzes nicht entgegen. Denn jedenfalls kann auf der Grundlage der vom Berufungsgericht getroffenen Feststellungen nicht davon ausgegangen werden, dass eine journalistisch-redaktionelle Bearbeitung der Bewertungen erfolgt (vgl. Senatsurteil vom 23. Juni 2009 – VI ZR 196/08, BGHZ 181, 328 Rn. 19 ff. m.w.N.; Buchner, in: Wolff/Brink, Datenschutzrecht, 2013, § 41 BDSG Rn. 24 ff.; Gola/Schomerus, BDSG, 11. Aufl., § 41 Rn. 10a; Plath/Frey, in: Plath, BDSG, 2013, § 41 Rn. 12; Roggenkamp, K&R 2009, 571; Westphal, in: Taeger/Gabel, BDSG, 2. Aufl., § 41 Rn. 26 m.w.N.; siehe zur Frage der Anwendbarkeit des § 41 BDSG auf Bewertungsportale auch Buchner, a.a.O., Rn. 18 f.; Greve/Schärdel, MMR 2008, 644, 647 f.; dies., MMR 2009, 613 f.; Simitis/Dix, BDSG, 8. Aufl., § 41 Rn. 11 m.w.N.; Spindler/Nink, in: Spindler/Schuster, Recht der elektronischen Medien, 2. Aufl., § 41 BDSG Rn. 1).

2. Ob die Speicherung der streitgegenständlichen Daten des Klägers zulässig ist, bestimmt sich entgegen der Auffassung der Revision nicht nach § 28 BDSG, sondern nach § 29 BDSG.

a) Entscheidend für die Abgrenzung von § 28 BDSG und § 29 BDSG ist der vom privatwirtschaftlichen Datenverarbeiter verfolgte Zweck. Erfolgt die Datenverarbeitung „als Mittel für die Erfüllung eigener Geschäftszwecke", ist sie also lediglich Hilfsmittel zur Erfüllung bestimmter anderer eigener Zwecke der datenverarbeitenden Stelle (so Gola/Schomerus, BDSG, 11. Aufl., § 28 Rn. 4), so beurteilt sich ihre Zulässigkeit nach § 28 BDSG (vgl. Senatsurteil vom 23. Juni 2009 – VI ZR 196/08, BGHZ 181, 328 Rn. 24). Werden die Daten hingegen geschäftsmäßig „zum Zwecke der Übermittlung" verarbeitet, ist die Datenübermittlung selbst also eigentlicher Geschäftsgegenstand (so Buchner, in: Wolff/Brink, Datenschutzrecht, 2013, § 29 BDSG Rn. 2; BeckOK Datenschutzrecht/Buchner [Stand: 1. Mai 2014] § 29 BDSG Rn. 2; Gola/Schomerus, BDSG, 11. Aufl., § 29 Rn. 2), so gilt § 29 BDSG (vgl. Senat a.a.O.).

Nach den vom Berufungsgericht in Bezug genommenen tatbestandlichen Feststellungen des Amtsgerichts stellt die Beklagte in dem von ihr betriebenen Portal die über Ärzte gespeicherten personenbezogenen Informationen der streitgegenständlichen Art – also die sogenannten „Basisdaten", Noten und Freitextkommentare – Nutzern zum Abruf zur Verfügung. Unmittelbarer Zweck des Portalbetriebs und mithin Gegenstand der Tätigkeit der Beklagten ist also die Übermittlung dieser Daten an Nutzer des Portals. Auch die dafür erforderliche Datenerhebung und -speicherung erfolgen damit zu diesem Zweck. Weil die Tätigkeit auf Wiederholung gerichtet und auf eine gewisse Dauer angelegt ist, erfolgen Datenerhebung und Datenspeicherung – wie für die Anwendung des § 29 BDSG erforderlich – auch geschäftsmäßig (vgl. Senat a.a.O.).

...

3. Die Speicherung der streitgegenständlichen Daten ist nach § 29 BDSG zulässig.

a) Den Prüfungsmaßstab bestimmt dabei einheitlich die Regelung des § 29 Abs. 1 Satz 1 Nr. 1 BDSG. Zwar wurden die sogenannten „Basisdaten" unstreitig allgemein zugänglichen Quellen entnommen. Bei isolierter Betrachtung wäre die Zulässigkeit ihrer Speicherung deshalb nach der – im Vergleich zu § 29 Abs. 1 Satz 1 Nr. 1 BDSG weniger strengen – Vorschrift des § 29 Abs. 1 Satz 1 Nr. 2 BDSG zu beurteilen. Die Umstände des Streitfalls erfordern aber eine Würdigung im Zusammenhang mit der Speicherung der Bewertungen, weil nur die gemeinsame Verwendung der Daten den von der Beklagten verfolgten Zweck erfüllt (vgl. Senatsurteil vom 23. Juni 2009 – VI ZR 196/08, BGHZ 181, 328 Rn. 25; siehe auch LG Hamburg, MMR 2011, 488, 489; Roggenkamp, K&R 2009, 571).

b) Nach § 29 Abs. 1 Satz 1 Nr. 1 BDSG ist die Erhebung und Speicherung personenbezogener Daten zum Zweck der Übermittlung zulässig, wenn kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Erhebung oder Speicherung hat. Der wertausfüllungsbedürftige Begriff des „schutzwürdigen Interesses" verlangt eine Abwägung des Interesses des Betroffenen an dem Schutz seiner Daten und des Stellenwerts, den die Offenlegung und Verwendung der Daten für ihn hat, mit den Interessen der Nutzer, für deren Zwecke die Speicherung erfolgt, unter Berücksichtigung der objektiven Wertordnung der Grundrechte (vgl. Senatsurteile vom 23. Juni 2009 – VI ZR 196/08, BGHZ 181, 328 Rn. 26; vom 17. Dezember 1985 – VI ZR 244/84, NJW 1986, 2505, 2506; BGH, Urteile vom 15. Dezember 1983 – III ZR 207/82, MDR 1984, 822 f.; vom 7. Juli 1983 – III ZR 159/82, VersR 1983, 1140, 1141; Gola/Schomerus, BDSG, 11. Aufl., § 29 Rn. 11). Für diese Abwägung sind die im Urteil des erkennenden Senats vom 23. Juni 2009 (VI ZR 196/08, a.a.O.) entwickelten Grundsätze heranzuziehen.

c) Im Streitfall hat eine Abwägung zwischen dem Schutz des Rechts des Klägers auf informationelle Selbstbestimmung nach Art. 2 Abs. 1, Art. 1 Abs. 1 GG, Art. 8 Abs. 1 EMRK auf der einen Seite und dem Recht der Beklagten auf Kommunikationsfreiheit nach Art. 5 Abs. 1 GG, Art. 10 Abs. 1 EMRK auf der anderen zu erfolgen, bei der auch die mittelbare Drittwirkung des beiden Parteien zustehenden Grundrechts aus Art. 12 Abs. 1 GG zu berücksichtigen ist.

aa) Die Aufnahme des Klägers in das Bewertungsportal berührt zuvörderst sein Recht auf informationelle Selbstbestimmung, das die Befugnis des Einzelnen umfasst, grundsätzlich selbst darüber zu bestimmen, ob, wann und innerhalb welcher Grenzen seine persönlichen Daten in die Öffentlichkeit gebracht werden. Es erschöpft sich nicht in der Funktion des Abwehrrechts des Bürgers gegen den Staat, sondern entfaltet als Grundrecht Drittwirkung und beeinflusst hierdurch auch die Werteordnung des Privatrechts (vgl. Senatsurteile vom 29. April 2014 – VI ZR 137/13, VersR 2014, 968 Rn. 6; vom 23. Juni 2009 – VI ZR 196/08, BGHZ 181, 328 Rn. 28).

Betroffen ist der Kläger darüber hinaus in seinem von Art. 12 Abs. 1 GG geschützten Recht auf freie Berufsausübung (vgl. Martini, DÖV 2010, 573, 579; Schröder, VerwArch 2010, 205, 226; aA Gundermann, VuR 2010, 329, 333), das mittelbar (vgl. Scholz, in: Maunz/Dürig, GG, Art. 12 Rn. 76 ff [Stand: Juni 2006]) ebenfalls Drittwirkung entfaltet. Der Schutzbereich umfasst jede Tätigkeit, die mit der Berufsausübung zusammenhängt und dieser dient, mithin auch die Außendarstellung von selbständig Berufstätigen, soweit sie auf die Förderung des beruflichen Erfolgs gerichtet ist (vgl. BVerfGE 85, 248, 256; NJW-RR 2007, 1048 f.). Das Grundrecht schützt dabei zwar nicht vor der Verbreitung zutreffender und sachlich gehaltener Informationen am Markt, die für das wettbewerbliche Verhalten der Marktteilnehmer von Bedeutung sein können, selbst wenn sich die Inhalte auf einzelne Wettbewerbspositionen nachteilig auswirken (vgl. Senatsurteil vom 22. Februar 2011 – VI ZR 120/10, VersR 2011, 632 Rn. 20; BVerfGE 105, 252, 265; NJW-RR 2004, 1710, 1711; siehe auch Martini, DÖV 2010, 573, 579). Die Aufnahme in das Bewertungsportal der Beklagten geht aber darüber hinaus. Sie zwingt den aufgenommenen Arzt dazu, sich in dem von der Beklagten vorgegebenen (engen) Rahmen einer breiten Öffentlichkeit präsentieren zu lassen sowie sich – unter Einbeziehung von Bewertungen medizinisch unkundiger Laien – einem Vergleich mit anderen im Portal aufgeführten Ärzten zu stellen, und kann erhebliche Auswirkungen auf seine beruflichen Chancen und seine wirtschaftliche Existenz haben (vgl. OLG Hamm, K&R 2011, 733, 734; Martini, a.a.O.; siehe auch BVerwGE 71, 183, 194).

bb) Zugunsten der Beklagten ist in die Abwägung das – ihr als juristischer Person des Privatrechts zustehende (BGH, Urteil vom 24. Januar 2006 – XI ZR 384/03, BGHZ 166, 84 Rn. 99 m.w.N.) – Recht auf Kommunikationsfreiheit nach Art. 5 Abs. 1 GG, Art. 10 Abs. 1 EMRK einzustellen (vgl. Senatsurteil vom 23. Juni 2009 – VI ZR 196/08, BGHZ 181, 328 Rn. 27 ff.). Art. 5 Abs. 1 Satz 1 GG schützt auch den Kommunikationsprozess als solchen. Deshalb kann die Mitteilung einer fremden Meinung oder Tatsachenbehauptung selbst dann in den Schutzbereich des Grundrechts fallen, wenn der Mitteilende sich diese weder zu eigen macht noch sie in eine eigene Stellungnahme einbindet (vgl. BVerfG, NJW-RR 2010, 470 Rn. 58; Grabenwarter, in: Maunz/Dürig, GG, Art. 5 Rn. 87 ff. [Stand: Januar 2013]; siehe auch OLG Hamburg, CR 2012, 188, 191). Ein Bewertungsportal, wie es die Beklagte betreibt, macht den Austausch über Behandlungserfahrungen bei konkreten Ärzten unter nicht persönlich miteinander bekannten Personen erst möglich. Die Beklagte ist insoweit als Portaltalbetreiberin also „unverzichtbare Mittlerperson" (so Schröder, VerwArch 2010, 205, 214). Bereits deshalb wird der Betrieb des Portals vom Schutzbereich des Art. 5 Abs. 1 Satz 1 GG erfasst. Von einer rein technischen Verbreitung, deren Schutz durch Art. 5 Abs. 1 Satz 1 GG jedenfalls fraglich ist (vgl. BVerfG, NJW-RR 2010, 470 Rn. 59), unterscheidet sich der Betrieb des Bewertungsportals jedenfalls dadurch, dass das Portal – auch über die Anzeige des Notendurchschnitts – aus Sicht des Nutzers den Anspruch erhebt, ein vollständiges Bild über die abgegebenen und den vorgegebenen Richtlinien entsprechenden Nutzerbewertungen zu zeichnen. Im Übrigen ist auch die Meinungs- und Informations-

freiheit der Portalnutzer berührt (vgl. auch Schröder, VerwArch 2010, 205, 213 f.).

Durch eine Pflicht zur Löschung von Einträgen in ihrem Bewertungsportal würde die Beklagte darüber hinaus in der Ausübung ihres Gewerbes beschränkt und damit im Schutzbereich der auch ihr als juristischer Person des Privatrechts zustehenden (BVerfGE 97, 228, 253; Scholz, in: Maunz/Dürig, GG, Art. 12 Rn. 106 [Stand: Juni 2006]) Berufsausübungsfreiheit betroffen (vgl. Schröder, VerwArch 2010, 205, 212 ff.).

d) Die vom Berufungsgericht durchgeführte Abwägung hält der rechtlichen Nachprüfung, der sie in vollem Umfang unterliegt (vgl. Senatsurteil vom 23. Juni 2009 – VI ZR 196/08, BGHZ 181, 328 Rn. 27), im Ergebnis stand. Die Auffassung des Berufungsgerichts, die Interessen des Klägers am Ausschluss der Speicherung der streitgegenständlichen Daten überwögen die Interessen der Beklagten und Nutzer am Betrieb des Portals und der damit verbunden Datenspeicherung nicht, trifft zu.

aa) Im Ausgangspunkt ist freilich festzustellen, dass ein Arzt durch seine Aufnahme in das von der Beklagten betriebene Ärztebewertungsportal nicht nur unerheblich belastet ist.

(1) Zutreffend weist die Revision insoweit zunächst darauf hin, dass es sich bei der Bewertung von Ärzten in dem von der Beklagten betriebenen Portal – anders als bei den Bewertungen von Lehrkräften auf dem Schülerportal, das Gegenstand des Senatsurteils vom 23. Juni 2009 (VI ZR 196/08, BGHZ 181, 328 [insoweit Rn. 37]) war – nicht nur um „substanzarme“, den Kläger in seiner Person und in seiner beruflichen Entwicklung nur mäßig beeinträchtigende Daten handelt. Denn die Bewertungen können nicht nur erhebliche Auswirkungen auf den sozialen und beruflichen Geltungsanspruch eines Arztes haben. Sie können vielmehr auch die Arztwahl behandlungsbedürftiger Personen beeinflussen, sich dadurch unmittelbar auf die Chancen des Arztes im Wettbewerb mit anderen Ärzten auswirken und damit im Falle von negativen Bewertungen sogar seine berufliche Existenz gefährden.

Die Breitenwirkung des Bewertungsportals der Beklagten ist ganz erheblich. Anders als im Falle des genannten Schülerportals ist die (passive) Nutzungsmöglichkeit nicht auf registrierte Nutzer beschränkt. Jeder Internetnutzer hat die Möglichkeit, die entsprechenden Daten eines im Portal aufgeführten Arztes abzurufen. Die Daten sind über Suchmaschinen – auch durch Eingabe des Namens eines Arztes – leicht auffindbar, was das Gewicht der Persönlichkeitsrechtsbeeinträchtigung weiter verstärkt (vgl. EuGH, NJW 2014, 2257 Rn. 87). Insbesondere kann über Suchmaschinen auch derjenige mit im Portal der Beklagten gespeicherten Bewertungen eines bestimmten Arztes konfrontiert werden, der nach ganz anderen Informationen, etwa nach den Sprechzeiten oder der Adresse eines Arztes, sucht.

Auch ist nicht ausgeschlossen, dass Bewerter das Portal missbrauchen. So besteht aufgrund der den Nutzern von der Beklagten eingeräumten Möglichkeit, Bewertungen auch im Freitext zu verfassen, die Gefahr, dass über das Portal unwahre, beleidigende oder sonst unzulässige Aussagen bezüglich eines Arztes ins Netz gestellt werden. Diese Gefahr wird dadurch noch verstärkt, dass Bewertungen verdeckt abgegeben werden können. Zwar ist Voraussetzung für die Abgabe einer Bewertung die vorherige Registrierung. Die Angabe des Klarnamens ist hierfür aber nicht erforderlich; es genügt vielmehr die Angabe einer E-Mail-Adresse, auf die der Registrierende Zugriff hat. Auch Mehrfachbewertungen durch ein und dieselbe Person und Bewertungen ohne realen Behandlungshintergrund sind denkbar.

(2) Allerdings berühren die von der Beklagten erhobenen und gespeicherten Informationen den Kläger nur in seiner Sozialsphäre. Die Bewertungen betreffen die berufliche Tätigkeit des Klägers, also einen Bereich, in dem sich die persönliche Entfaltung von vornherein im Kontakt mit der Umwelt vollzieht. Nach dem von der Rechtsprechung im Hinblick auf die Eigenart des allgemeinen Persönlichkeitsrechts als eines Rahmenrechts entwickelten Konzept abgestufter Schutzwürdigkeit bestimmter Sphären schützt das allgemeine Persönlichkeitsrecht zwar auch im Bereich der Sozialsphäre das Recht auf Selbstbestimmung bei der Offenbarung von persönlichen Lebenssachverhalten. Der Schutz ist aber geringer als bei Daten, die etwa der Intim- oder Geheimsphäre zuzuordnen sind (vgl. Senatsurteil vom 23. Juni 2009 – VI ZR 196/08, BGHZ 181, 328 Rn. 30 m.w.N.). Im Bereich der Sozialsphäre muss sich der Einzelne wegen der Wirkungen, die seine Tätigkeit hier für andere hat, von vornherein auf die Beobachtung seines Verhaltens durch eine breitere Öffentlichkeit und auf Kritik an seinen Leistungen einstellen (vgl. Senatsurteile vom 23. Juni 2009 – VI ZR 196/08, BGHZ 181, 328 Rn. 31; vom 11. März 2008 – VI ZR 7/07, VersR 2008, 793 Rn. 29; vom 21. November 2006 – VI ZR 259/05, VersR 2007, 511 Rn. 12 ff.). Dies gilt insbesondere auch bei freiberuflich tätigen Ärzten, die ihre Leistungen in Konkurrenz zu anderen Ärzten anbieten. Äußerungen im Rahmen der Sozialsphäre dürfen nur im Falle schwerwiegender Auswirkungen auf das Persönlichkeitsrecht mit negativen Sanktionen verknüpft werden, so etwa dann, wenn eine Stigmatisierung, soziale Ausgrenzung oder Prangerwirkung zu besorgen sind (vgl. Senatsurteile vom 20. Dezember 2011 – VI ZR 261/10, VersR 2012, 368 Rn. 14; vom 23. Juni 2009 – VI ZR 196/08, BGHZ 181, 328 Rn. 31). Dies steht im Streitfall nicht in Rede.

Im Übrigen ist der Kläger den oben dargestellten Gefahren des Bewertungsportals nicht schutzlos ausgeliefert. Insbesondere kann er unwahren Tatsachenbehauptungen und beleidigenden oder sonst unzulässigen Bewertungen dadurch begegnen, dass er sich unter Bezugnahme auf den jeweiligen Eintrag an die Beklagte wendet und dort die Beseitigung des Eintrags verlangt. Nach den vom Berufungsgericht getroffenen Feststellungen steht ihm hierzu eine entsprechende Schaltfläche auf dem Bewertungsportal zur Verfügung. Weist die Beklagte die Forderung zurück, kann der Kläger die Beklagte – worauf das Berufungsgericht zutreffend hinweist – gerichtlich, ggf. auch im Wege des einstweiligen Rechtsschutzes, in Anspruch nehmen. Entsprechendes gilt für etwaige, auch unter Berücksichtigung von § 10 des Telemediengesetzes (TMG) bestehende Schadensersatzansprüche. Zur Verhinderung von Mehrfachbewertungen und Bewertungen ohne realen Hintergrund setzt die Beklagte im Übrigen – wenn auch keine lückenlosen – Schutzmechanismen ein.

Zuletzt wiegen die vom Kläger konkret für seine Person geltend gemachten Belastungen nicht allzu schwer. Dass er Opfer einer rechtlich oder auch nur nach den Nutzungsbedingungen der Beklagten unzulässigen Bewertung geworden sei, trägt er nicht vor. Umsatzeinbußen werden vom Kläger zwar behauptet; substantiierter Vortrag dazu fehlt aber.

bb) Die dargestellten Beeinträchtigungen der berechtigten Interessen des Klägers wiegen nicht schwerer als das Recht der Beklagten auf Kommunikationsfreiheit.

(1) Auszugehen ist dabei zunächst von dem ganz erheblichen Interesse, das die Öffentlichkeit an Informationen über ärztliche Dienstleistungen hat (vgl. LG Kiel, NJW-RR 2002, 1195). Personen, die ärztliche Leistungen in Anspruch nehmen wollen, können den

Arzt grundsätzlich frei wählen. Das von der Beklagten betriebene Portal kann dazu beitragen, dem Patienten die aus seiner Sicht hierfür erforderlichen Informationen zur Verfügung zu stellen. Dass es unter Umständen auch andere Informationsquellen gibt – etwa persönliche Erfahrungen von Bekannten oder bei Fachärzten die Einschätzung des vom Patienten ggf. zuvor konsultierten Hausarztes –, ändert daran nichts.

Der grundsätzlichen Eignung des Portals, zu mehr Leistungstransparenz im Gesundheitswesen beizutragen, steht nicht entgegen, dass die in das Bewertungsportal eingestellten Bewertungen typischerweise nicht von Fachleuten herrühren und subjektiv geprägt sind. Zwar dürften wertende Aussagen zur medizinischen Qualität einer Behandlung fachlichen Maßstäben, die der Laie nicht kennt, häufig nicht entsprechen und im Einzelfall etwa von einem vom behandelnden Arzt nicht zu vertretenden Ausbleiben des – von ihm auch nicht geschuldeten – Heilungserfolges geprägt sein. Eine sinnvolle Ergänzung der bisherigen Informationsquellen kann das Angebot der Beklagten aber trotzdem sein. Die subjektive Einschätzung, die in den Bewertungen zum Ausdruck kommt, kann anderen Personen Hilfestellung bei der Entscheidung geben, welcher Arzt – insbesondere bezüglich der äußeren Umstände der Behandlung wie etwa der Praxisorganisation – den Anforderungen für die gewünschte Behandlung und auch den persönlichen Präferenzen am besten entspricht (siehe auch Hennig/Etgeton, DuD 2011, 841, 843; Martini, DÖV 2010, 573, 580; Wilkat, Bewertungsportale im Internet, 2013, S. 211 f.).

(2) Dass Bewertungen im von der Beklagten betriebenen Portal – abgesehen von der Angabe einer E-Mail-Adresse – anonym abgegeben werden können, führt nicht dazu, dass das Interesse des Klägers an der Löschung der Daten dasjenige der Beklagten an der Speicherung überwöge. Wie oben dargestellt, sind die bewerteten Ärzte und damit auch der Kläger hierdurch nicht schutzlos gestellt. Die anonyme Nutzung ist dem Internet zudem immanent. Dementsprechende Regelungen zum Schutz der Nutzerdaten gegenüber dem Diensteanbieter finden sich in den §§ 12 ff. TMG (vgl. insbesondere § 13 Abs. 6 Satz 1 TMG und Senatsurteil vom 1. Juli 2014 – VI ZR 345/13, NJW 2014, 2651 Rn. 8 ff.). Eine Beschränkung der Meinungsäußerungsfreiheit auf Äußerungen, die einem bestimmten Individuum zugeordnet werden können, ist mit Art. 5 Abs. 1 Satz 1 GG nicht vereinbar (Senatsurteil vom 23. Juni 2009 – VI ZR 196/08, BGHZ 181, 328 Rn. 38). Die Möglichkeit, Bewertungen auch anonym abgeben zu können, erlangt im Falle eines Ärztebewertungsportals im Übrigen ganz besonderes Gewicht. Denn häufig wird die Bewertung eines Arztes mit der Mitteilung sensibler Gesundheitsinformationen, etwa über den Grund der Behandlung oder die Art der Therapie, verbunden sein. Wäre die Abgabe einer Bewertung nur unter Offenlegung der Identität möglich, bestünde deshalb hier ganz besonders die Gefahr, dass eigentlich bewertungswillige Patienten im Hinblick darauf von der Abgabe einer Bewertung absehen.

(3) Dass die Beklagte den Portalbetrieb im Falle der Löschung des Profils des Klägers zunächst zwar ohne das Profil des Klägers, im Übrigen aber unverändert fortführen könnte, führt ebenfalls nicht zu einem Überwiegen der Interessen des Klägers. Ein Bewertungsportal, das von der Zustimmung der bewerteten Ärzte abhängig wäre, die ggf. bei Vorliegen einer schwächeren Bewertung zurückgenommen werden könnte, erfüllte den mit ihm verfolgten Zweck allenfalls noch eingeschränkt.

...

Der Kläger hat auch keinen Anspruch auf Unterlassung der Veröffentlichung der streitgegenständlichen Daten nach § 823 Abs. 2, § 1004 BGB analog in Verbindung mit § 4 Abs. 1 BDSG durch Übermittlung an die abfragenden Nutzer. Die Übermittlung ist vielmehr nach § 29 Abs. 2 BDSG zulässig.

1. Nach dem Wortlaut des § 29 Abs. 2 Satz 1 BDSG ist die Übermittlung personenbezogener Daten zulässig, wenn – erstens – der Dritte, dem die Daten übermittelt werden, ein berechtigtes Interesse an ihrer Kenntnis glaubhaft dargelegt hat, und – zweitens – kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse am Ausschluss der Übermittlung hat. In Bezug auf Bewertungsportale im Internet ist die Vorschrift nach der Rechtsprechung des erkennenden Senats (Senatsurteil vom 23. Juni 2009 – VI ZR 196/08, BGHZ 181, 328 Rn. 42 f.; ebenso etwa Greve/Schärdel, in: Große Ruse-Khan/Klass/v. Lewinski (Hrsg.), Nutzergenerierte Inhalte als Gegenstand des Privatrechts, 2010, S. 71, 81; siehe auch Plath, in: Plath, BDSG, 2013, § 29 Rn. 87; Iraschko-Luscher/Kiekenbeck, ZD 2012, 261, 262; Roggenkamp, K&R 2009, 571, 572 f.; kritisch etwa BeckOK Datenschutzrecht/Buchner [Stand: 1. Mai 2014], § 29 BDSG Rn. 119 f.; Taeger, in: Taeger/Gabel, BDSG, 2. Aufl., § 29 Rn. 56) verfassungskonform dahingehend auszulegen, dass die Zulässigkeit der Übermittlung der Daten an die abfragenden Nutzer aufgrund einer Gesamtabwägung zwischen dem Persönlichkeitsrecht des Betroffenen einerseits und dem Informationsinteresse desjenigen, dem die Daten über das Internet übermittelt werden, andererseits beurteilt werden muss. Dabei sind die schutzwürdigen Interessen des Betroffenen den Interessen des Abrufenden an der Kenntnis der Daten und desjenigen, der die Daten übermittelt, an deren Weitergabe gegenüberzustellen. Der vom Wortlaut der Vorschrift verlangten glaubhaften einzelfallbezogenen Darlegung des berechtigten Interesses am Abruf bedarf es hingegen nicht.

2. Im Streitfall fällt die danach vorgegebene Abwägung zugunsten der Beklagten und ihrer Nutzer aus. Dies ergibt sich aus denselben Erwägungen, die auch die Speicherung der streitgegenständlichen Daten zum Zwecke ihrer Übermittlung als zulässig erscheinen lassen.

Unkontrollierte Befragung von sachkundigen Arbeitnehmern (Ls)

(**Bundesarbeitsgericht**, Beschluss vom 20. Januar 2015 – 1 ABR 25/13 –)

1. **Die Wahrnehmung der Aufgaben einer Auskunftsperson i.S.d. § 80 Abs. 2 Satz 3 BetrVG gehört regelmäßig zu den Aufgaben, die der Arbeitgeber einem Arbeitnehmer gegenüber kraft seiner Direktionsrechts (§ 106 Satz 1 GewO) anordnen kann. Bei der Übertragung einer solchen Tätigkeit kann der Arbeitgeber Gegenstand und Umfang der zu erteilenden Auskünfte bestimmen. Dies bindet den Arbeitnehmer bei der Beantwortung der ihm vom Betriebsrat gestellten Fragen.**

2. **Andererseits ist der Betriebsrat zur unbefangenen Meinungsbildung berechtigt, Gespräche mit Auskunftspersonen i.S.d. § 80 Abs. 2 Satz 3 BetrBG zu führen, ohne dass an diesen die Arbeitgeberin oder von ihr bestimmte Personen teilnehmen.**

Initiativpflicht bei betrieblichem Eingliederungsmanagement (Ls)

(**Bundesarbeitsgericht**, Urteil vom 20. November 2014 – 2 AZR 755/13 –)

1. **Es ist Sache des Arbeitgebers, die Initiative zur Durchführung eines gesetzlich gebotenen betrieblichen Eingliederungsmanagements (bEM) zu ergreifen. Dazu gehört, dass er den Arbeitnehmer auf die Ziele des bEM sowie die Art und den Umfang der hierfür erhobenen und verwendeten Daten hinweist.**

2. **Hat der Arbeitgeber die gebotene Initiative nicht ergriffen, muss er zur Darlegung der Verhältnismäßigkeit einer auf krankheitsbedingte Fehlzeiten gestützten Kündigung nicht nur die objektive Nutzlosigkeit arbeitsplatzbezogener Maßnahmen i.S.v. § 1 Abs. 2 Satz 2 KSchG aufzeigen. Er muss vielmehr auch dartun, dass künftige Fehlzeiten ebenso wenig durch gesetzlich vorgesehene Hilfen oder Leistungen der Rehabilitationsträger in relevantem Umfang hätten vermieden werden können.**

Schadensersatz wegen verspäteter Übernahme in das Beamtenverhältnis auf Probe*

(**Oberverwaltungsgericht Nordrhein-Westfalen**, Beschluss vom 19. November 2014 – 6 A 1896/13 –)

1. **Erfolglose Klage eines Justizvollzugsobersekretärs auf Schadensersatz wegen verspäteter Übernahme in das Beamtenverhältnis auf Probe.**

2. **Zur Ablehnung einer Übernahme in das Beamtenverhältnis auf Probe, die mit fehlender charakterlicher Eignung des Bewerbers, der ein früher gegen ihn geführtes staatsanwaltschaftliches Ermittlungsverfahren verschwiegen hat, begründet wurde.**

Aus den Gründen:

I. Der am 23. August 1978 geborene Kläger begehrt Schadensersatz wegen verspäteter Übernahme in das Beamtenverhältnis auf Probe.

Der Kläger war in der Zeit vom 1. November 1999 bis zum 30. Juni 2010 Soldat auf Zeit. Am 26. November 2006 leitete die Staatsanwaltschaft Q. ein Ermittlungsverfahren (171 Js 202/07) gegen ihn wegen des Verdachts der versuchten gefährlichen Körperverletzung, der Bedrohung und des Verstoßes gegen das Waffengesetz ein. Nach den Angaben des beklagten Landes stellte die Staatsanwaltschaft dieses Verfahren am 6. November 2007 gemäß § 153a StPO ein.

Mit Schreiben vom 6. Juli 2009 bewarb sich der Kläger beim beklagten Land um einen Ausbildungsplatz zum Justizvollzugsobersekretär. Am selben Tag gab er folgende Erklärung ab: „Gegen mich sind keine – folgende – staatsanwaltschaftlichen Ermittlungsverfahren anhängig oder innerhalb der letzten drei Jahre anhängig gewesen".

Unter dem 4. Juni 2010 teilte der Leiter der Justizvollzugsanstalt C.-T. dem Kläger mit, er beabsichtigte ihn – vorbehaltlich eines beanstandungsfreien Ergebnisses der durchzuführenden Sicherheitsüberprüfung – ab dem 1. Juli 2010 in das Beamtenverhältnis auf Widerruf zu übernehmen.

Am 1. Juli 2010 ernannte das beklagte Land den Kläger unter Berufung in das Beamtenverhältnis auf Widerruf zum Justizvollzugsobersekretäranwärter.

In einem Vermerk führte der Leiter der Justizvollzugsanstalt C. -T. am 7. September 2010 aus:

„Mit Datum vom 30.08.2010 ging hier das Ergebnis der Sicherheitsüberprüfung ein; mitgeteilt wurde, dass gegen Herrn S. im Jahr 2006 ein Ermittlungsverfahren wegen gefährlicher Körperverletzung und Verstoßes gegen das Waffengesetz anhängig war. Hierbei handelte es sich um eine alkoholbedingte Auseinandersetzung mehrerer Personen vor einer Partyhütte, in deren Verlauf Herr S. die Geschädigten mit einer PTB-Waffe (Schreckschusswaffe) bedroht haben soll und mit einem Schraubenschlüssel mehrfach drohend auf einen Metallzaun schlug. Das Verfahren wurde später gem. § 153a StPO eingestellt. Im Zuge des Einstellungsverfahrens wurden von Herrn S. u.a. Angaben zu Vorstrafen, anhängigen Ermittlungsverfahren erbeten, die in Teilen unvollständig bzw. nicht wahrheitsgemäß gemacht wurden. Das erforderliche beanstandungsfreie Ergebnis der Sicherheitsüberprüfung ist nicht gegeben, die geforderten Voraussetzungen für die Übernahme in das Beamtenverhältnis liegen somit nicht vor. Im Ergebnis der Feststellungen ist zudem die notwendige Basis für eine dauerhafte vertrauensvolle Zusammenarbeit nicht vorhanden. (…)

Herrn S. wurde mitgeteilt, dass auf Grund der vorliegenden Erkenntnisse nach dem Abschluss der Ausbildung keine Übernahme in das Beamtenverhältnis auf Probe erfolgen wird. (…)".

Der Anstaltsleiter teilte dem Kläger mit Schreiben vom 27. März 2012 und 10. Mai 2012 mit, „dass aufgrund der wahrheitswidrigen Angabe und der Umstände der zu Grunde liegenden Straftat keine Übernahme in ein Beamtenverhältnis auf Probe erfolgen wird" und dass das Beamtenverhältnis auf Widerruf mit dem Ablegen der Laufbahnprüfung ende.

Am 28. Juni 2012 bestand der Kläger die Prüfung für die Laufbahn des allgemeinen Vollzugsdienstes mit der Note „vollbefriedigend".

Der Kläger hat am selben Tag Klage erhoben.

Er hat geltend gemacht, er erfülle die beamtenrechtlichen Voraussetzungen für die Übernahme in das Beamtenverhältnis auf Probe. Das beklagte Land habe nicht näher dargelegt, aus welchen Gründen er charakterlich ungeeignet sei. Die Behauptung, er habe am 26. November 2006 eine Drohung unter Zuhilfenahme einer illegalen Waffe ausgesprochen, sei unzutreffend. Zutreffend sei allein, dass die Staatsanwaltschaft Q. gegen ihn im Jahre 2006 ein Ermittlungsverfahren geführt habe. Hierüber habe er seinerzeit die „zuständigen Stellen bei der Bundeswehr" in Kenntnis gesetzt. Auf seine Nachfrage, „ob er diesbezüglich irgendetwas melden müsse", sei ihm mitgeteilt worden, „solange keine Anklage o.ä. in der Welt sei, müsse er nichts mitteilen". Der Kläger hat weiter vorgetragen, ihm sei bei der Abgabe der im Streit stehenden Erklärung vom

* Das Urteil ist durch Beschluss des BVerwG vom 20. Mai 2015 – BVerwG 2 B 4.15 – wegen eines Verfahrensmangels aufgehoben und an das OVG NRW zurückverwiesen worden.

6. Juli 2009 das angeführte Ermittlungsverfahren nicht mehr in Erinnerung gewesen.

Der Kläger hat sinngemäß beantragt, das beklagte Land unter Aufhebung der Bescheide des Leiters der Justizvollzugsanstalt C. -T. vom 27. März 2012 und 10. Mai 2012 zu verpflichten, ihn in das Beamtenverhältnis auf Probe zu übernehmen, hilfsweise, das beklagte Land unter Aufhebung der Bescheide des Leiters der Justizvollzugsanstalt C. -T. vom 27. März 2012 und 10. Mai 2012 zu verpflichten, über seinen Antrag auf Übernahme in das Beamtenverhältnis auf Probe unter Beachtung der Rechtsauffassung des Gerichts erneut zu entscheiden.

Das beklagte Land hat beantragt, die Klage abzuweisen.

Es hat die Auffassung vertreten, aufgrund der wahrheitswidrigen Angaben des Klägers vom 6. Juli 2009, dass gegen ihn innerhalb der letzten drei Jahre keine staatsanwaltschaftlichen Ermittlungsverfahren anhängig gewesen seien, mangele es ihm an der für die Übernahme in das Probebeamtenverhältnis erforderlichen charakterlichen Eignung.

Das Verwaltungsgericht Minden hat die Klage durch Urteil vom 20. Juni 2013 abgewiesen. Am 15. Februar 2014 hat das beklagte Land den Kläger unter Berufung in das Beamtenverhältnis auf Probe zum Justizvollzugsobersekretär ernannt. Mit Beschluss vom 12. August 2014, dem Kläger zugestellt am selben Tage, hat der Senat die Berufung gegen das Urteil zugelassen. Der Kläger wiederholt mit der am 4. September 2014 eingegangenen Berufungsbegründung im Wesentlichen sein bisheriges Vorbringen.

Der Kläger beantragt sinngemäß,

1. die Sache unter Aufhebung des angefochtenen Urteils an das Verwaltungsgericht zurückzuverweisen,

2. im Falle einer Sachentscheidung des Berufungsgerichts das angefochtene Urteil zu ändern

und das beklagte Land unter Aufhebung der Bescheide des Leiters der Justizvollzugsanstalt C. -T. vom 27. März 2012 und 10. Mai 2012 zu verpflichten, ihn – den Kläger – in besoldungs-, versorgungs- und laufbahnrechtlicher Hinsicht so zu stellen, als ob er zum 1. Juli 2012 in das Beamtenverhältnis auf Probe übernommen worden wäre, hilfsweise unter Aufhebung der Bescheide des Leiters der Justizvollzugsanstalt C. -T. vom 27. März 2012 und 10. Mai 2012 festzustellen, dass er – der Kläger – mit bestandener Prüfung für die Laufbahn des allgemeinen Vollzugsdienstes am 28. Juni 2012 einen Anspruch auf Übernahme in das Beamtenverhältnis auf Probe hatte, äußerst hilfsweise festzustellen, dass die Bescheide des Leiters der Justizvollzugsanstalt C. -T. vom 27. März 2012 und 10. Mai 2012 rechtswidrig gewesen sind und er – der Kläger – mit bestandener Prüfung für die Laufbahn des allgemeinen Vollzugsdienstes am 28. Juni 2012 einen Anspruch auf Übernahme in das Beamtenverhältnis auf Probe hatte.

Das beklagte Land hat keinen Antrag gestellt.

Wegen der Einzelheiten des Sach- und Streitstandes wird auf den Inhalt der Gerichtsakte, der Strafakte der Staatsanwaltschaft Q. (241 Js 137/07 A) und der beigezogenen Verwaltungsvorgänge des beklagten Landes Bezug genommen.

II. Der Senat entscheidet nach Anhörung der Beteiligten über die Berufung des Klägers durch Beschluss nach § 130a VwGO, weil er sie einstimmig für unbegründet und die Durchführung einer mündlichen Verhandlung nicht für erforderlich hält.

Das Vorbringen des Klägers gibt keinen Anlass, eine mündliche Verhandlung durchzuführen. Das vorliegende Verfahren weist keine außerordentlich großen Schwierigkeiten auf, die einer Entscheidung durch Beschluss entgegenstehen könnten.

Vgl. BVerwG, Urteil vom 30. Juni 2004 – 6 C 28.03 –, juris, Rn. 7 ff., wonach der Umstand, dass das Oberverwaltungsgericht – wie hier – die Berufung wegen besonderer tatsächlicher oder rechtlicher Schwierigkeiten im Sinne von § 124 Abs. 2 Nr. 2 VwGO zugelassen hat, nicht stets einer Entscheidung im Verfahren nach § 130a VwGO entgegensteht.

Entgegen der Auffassung des Klägers sind „in der Sache komplexe Sachverhalts- und Rechtsfragen“ nicht zu klären (Schriftsatz vom 23. Oktober 2014).

Die zulässige Berufung ist unbegründet. Die Klage hat mit den im Berufungsverfahren gestellten Haupt- und Hilfsanträgen keinen Erfolg.

Die vom Kläger beantragte Zurückverweisung an das Verwaltungsgericht nach § 130 Abs. 2 Nr. 1 VwGO kam nicht in Betracht (Hauptantrag zu 1.). Nach dieser Vorschrift darf das Oberverwaltungsgericht die Sache, soweit ihre weitere Verhandlung erforderlich ist, unter Aufhebung des Urteils und des Verfahrens an das Verwaltungsgericht nur zurückverweisen, soweit das Verfahren vor dem Verwaltungsgericht an einem wesentlichen Mangel leidet und aufgrund dieses Mangels eine umfangreiche oder aufwändige Beweisaufnahme notwendig ist. Diese Voraussetzungen sind im Streitfall nicht erfüllt. Denn es fehlt jedenfalls an der aufgrund eines wesentlichen Verfahrensmangels erforderlichen Notwendigkeit einer umfangreichen oder aufwendigen Beweisaufnahme. Einen Anlass, die Vorschrift im Sinne des klägerischen Vorbringens einschränkend auszulegen, sieht der Senat nicht.

Die Klage hat auch mit dem Hauptantrag zu 2., den Kläger im Wege des Schadensersatzes in besoldungs-, versorgungs- und laufbahnrechtlicher Hinsicht so zu stellen, als ob er zum 1. Juli 2012 in das Beamtenverhältnis auf Probe übernommen worden wäre, keinen Erfolg. Sie ist unzulässig. Die damit verfolgte Klageänderung ist nicht sachdienlich im Sinne des § 91 Abs. 1 VwGO, weil der Kläger nicht, wie es geboten ist, das beklagte Land außerprozessual mit dem Schadensersatzverlangen befasst hat – vgl. BVerwG, Beschluss vom 3. Juni 2004 – 2 B 62.03 –, juris, Rn. 9 bis 11; Urteil vom 28. Juni 2001 – 2 C 48.00 –, juris, Rn. 15 bis 16 – und das beklagte Land auch nicht im Sinne von § 91 Abs. 2 VwGO eingewilligt hat.

Davon abgesehen ist der mit dem Hauptantrag zu 2. verfolgte Schadensersatzanspruch auch unbegründet.

Ein Schadensersatzanspruch wegen verspäteter Übernahme in ein Beamtenverhältnis auf Probe setzt voraus, dass der Dienstherr den aus Art. 33 Abs. 2 GG, § 9 BeamtStG, § 15 Abs. 3 Satz 1 LBG NRW folgenden Anspruch des Beamten auf ermessens- und beurteilungsfehlerfreie Entscheidung über seine Bewerbung schuldhaft verletzt hat, dem Beamten durch diese Pflichtverletzung adäquat kausal ein Schaden entstanden ist und er es nicht schuldhaft unterlassen hat, den Schaden durch Gebrauch eines Rechtsmittels abzuwenden. Rechtsgrundlage dieses Schadensersatzanspruches ist das Beamtenverhältnis (vgl. OVG NRW, Beschluss vom 5. November 2012 – 6 A 715/11 –, juris, Rn. 35).

Diese Voraussetzungen liegen hier nicht vor.

Nach Art. 33 Abs. 2 GG, § 9 BeamtStG, § 15 Abs. 3 Satz 1 LBG NRW hat jeder Deutsche nach seiner Eignung, Befähigung und fachlichen Leistung gleichen Zugang zu jedem öffentlichen Amt. Die danach vom Dienstherrn vorzunehmende Beurteilung der erforderlichen charakterlichen Eignung ist ein Akt wertender Erkenntnis. Er ist als solcher vom Gericht nur beschränkt darauf zu überprüfen, ob die Verwaltung den anzuwendenden Begriff verkannt, einen unrichtigen Sachverhalt zugrunde gelegt, allgemein gültige Wertmaßstäbe nicht beachtet oder sachwidrige Erwägun-

gen angestellt hat (vgl. OVG NRW, Beschlüsse vom 10. Januar 2012 – 6 A 141/11 –, juris, Rn. 7, vom 4. Dezember 2008 – 6 B 1520/08 –, juris, Rn. 6).

Die Ablehnung der Übernahme in das Beamtenverhältnis auf Probe kommt nicht nur und erst dann in Betracht, wenn der Dienstherr festgestellt hat, dass der Bewerber die erforderliche charakterliche Eignung nicht besitzt, sondern schon berechtigte Zweifel daran genügen, ob der Bewerber die erforderliche charakterliche Eignung aufweist (vgl. OVG NRW, Beschluss vom 10. Januar 2012 – 6 A 141/11 –, juris, Rn. 6).

Ausgehend von diesen Grundsätzen hat das beklagte Land die Grenzen des ihm zukommenden Beurteilungsspielraums nicht überschritten. Es hat die Zweifel gegenüber der charakterlichen Eignung des Klägers maßgeblich daraus abgeleitet, dieser habe bei der Bewerbung um einen Ausbildungsplatz zum Justizvollzugsobersekretäranwärter am 6. Juli 2009 angegeben, dass gegen ihn innerhalb der letzten drei Jahre keine staatsanwaltschaftlichen Ermittlungsverfahren anhängig gewesen seien (Schriftsatz vom 3. September 2012). Das war unzutreffend. Die Staatsanwaltschaft Q. hatte gegen ihn im Jahre 2006 wegen des Verdachts der versuchten gefährlichen Körperverletzung (§ 224 StGB), der Bedrohung (§ 241 StGB) und des Verstoßes gegen das Waffengesetz (§ 53 WaffG) ein Ermittlungsverfahren eingeleitet. Es ist nichts dagegen zu erinnern, dass das beklagte Land aufgrund des Verschweigens dieses Umstandes Zweifel an der charakterlichen Eignung des Klägers hatte.

Das Vorbringen des Klägers, es habe sich bei der im Streit stehenden Erklärung vom 6. Juli 2009 um „eine einmalige und lediglich fahrlässig falsche Angabe gehandelt", ist unglaubhaft. In dem Einsatzprotokoll der Kreispolizeibehörde Q. vom 26. November 2006 (Az. 411000-049684-06/9) ist unter anderem festgestellt worden:

„Am 26.11.2006, gegen 00:27 Uhr meldete sich der Zeuge B. telefonisch bei der Leitstelle der Polizei und gab an, dass es an der Partyhütte in der U. in Schloss O. zu einer Auseinandersetzung zwischen mehreren Personen gekommen sei. Dabei soll auch mit einer Schusswaffe gedroht worden sein. (…) Durch einen der Anwesenden wurden die eingetroffenen Beamten auf die drei Beschuldigten hingewiesen, die sich unmittelbar vor dem Tor befanden. Dabei wurde geäußert, dass der [Kläger] eine Waffe mit sich führe. Die Beschuldigten wurden daraufhin zum Zwecke der Durchsuchung an den Funkstreifenwagen gestellt und anschließend durchsucht. Bei dem [Kläger] wurde durch mich in dessen rechter Gesäßtasche ein Schraubwerkzeug zum Lösen von Radmuttern gefunden. Eine Waffe wurde bei keinem der Beschuldigten gefunden. (…)

Angaben der Geschädigten (Befragung durch PHK G.):

Zur genannten Tatzeit fand auf dem o.a. Gelände eine private Feier statt. Gegen 00.15 Uhr näherten sich zunächst zwei männliche Personen (die Beschuldigten L. und S.) dem mit einem Drahtzaun umgebenen Grundstück und sprachen dort auf dem Grundstück stehende Gäste (darunter auch die zuvor genannten Geschädigten) der Feier an. Es kam schnell zu beleidigenden Äußerungen durch die Beschuldigten. Die Geschädigten näherten sich daraufhin den beiden hinter der Umzäunung stehenden Beschuldigten, und forderten sie auf, die Beleidigungen einzustellen und sich vom Zaun zu entfernen. Nun begannen beide Beschuldigten gemeinsam nach den Geschädigten zu schlagen. Durch den Zaun getrennt, konnten sie die Geschädigten jedoch nicht erreichen. Nach weiteren Beleidigungen erklärten die Beschuldigten, sie würden jetzt weggehen, kündigten aber an zurückzukommen, dann würden die Geschädigten ihr Verhalten "bereuen".

Nach ca. 10 Minuten kehrten die beiden Beschuldigten mit einer weiteren männlichen Person [dem Kläger] zu dem Grundstück zurück. Es kam erneut zu verbalen Auseinandersetzungen (Beleidigungen, Beschimpfungen). Dann versuchten die drei Beschuldigten erneut, die hinter dem Zaun stehenden Geschädigten mit Schlägen zu treffen. Hierbei benutzte der [Kläger] auch einen Schraubenschlüssel, mit dem er gezielt nach den Geschädigten schlug. Dann hielt der [Kläger] plötzlich eine Pistole in der Hand und richtete die Waffe auf die Geschädigten. Er zog den Verschluss der Waffe nach hinten und drohte verbal an, auf die ZEG zu schießen („Ich knall euch ab….")."

Angesichts der Schwere der Vorwürfe, die die im Ermittlungsverfahren vernommenen Zeugen gegen den Kläger erhoben haben, hält der Senat das Vorbringen des Klägers für nicht glaubhaft, dass ihm „im Zeitpunkt der Abgabe seiner Erklärung, in den letzten drei Jahren sei kein Ermittlungsverfahren gegen ihn anhängig gewesen, überhaupt nicht mehr bewusst bzw. präsent war, dass es ein solches gegeben hatte" (Seite 13 des Schriftsatzes vom 6. September 2013). Der Kläger ist im Zuge der Ermittlungen am 26. November 2006 von einem Polizeivollzugsbeamten durchsucht worden. Hierbei ist ein Schraubenschlüssel als „Beweismittel/Tatmittel" sichergestellt worden (vgl. Durchsuchungs- und Sicherstellungsprotokoll vom 26. November 2006). Im Anschluss an die vor Ort von der Kreispolizeibehörde Q. getroffenen Feststellungen ist dem Kläger um 1.25 Uhr eine Blutprobe entnommen worden (BAK – Mittelwert: 1,07 Promille; vgl. ärztlicher Befundbericht vom 29. November 2006). Vor diesem Hintergrund und unter Berücksichtigung der Umstände, dass der Kläger in dem staatsanwaltschaftlichen Ermittlungsverfahren eine Anwaltskanzlei mit der Wahrnehmung seiner Interessen beauftragt hatte (vgl. Schreiben der Anwaltskanzlei C1., B1. und N. vom 1. Februar 2007), gegen seinen Bruder X. S. als weiteren Beschuldigten ermittelt (241 Js 137/07 A) und seine damalige Lebensgefährtin, K. X1., am 1. Februar 2007 in dem Ermittlungsverfahren als Zeugin vernommen wurde, steht zur Überzeugung des Senats fest, dass dem Kläger dieses Verfahren bei der Abgabe seiner Erklärung vom 6. Juli 2009 „präsent" war. Hinzu kommt, dass er das Ermittlungsverfahren zum Anlass genommen hatte, „seinen Vorgesetzten bei der Bundeswehr darauf" anzusprechen (Seite 13 des Schriftsatzes vom 6. September 2013).

Das beklagte Land hat zu Recht darauf verwiesen, dass der Justizvollzugsdienst ein sicherheitsempfindlicher Bereich sei, der „notwendig eine vertrauensvolle Zusammenarbeit der Bediensteten" (Schriftsatz vom 3. September 2012) verlange. Dass es im Streitfall in der Nichtangabe des staatsanwaltschaftlichen Ermittlungsverfahrens einen charakterlichen Mangel angenommen hat, der die für eine Übernahme in das Beamtenverhältnis auf Probe erforderliche charakterliche Eignung des Klägers ausschließt, ist nicht zu beanstanden.

Der Verweis des Klägers darauf, dass sein dienstliches Verhalten seit seiner Übernahme in das Beamtenverhältnis auf Widerruf ausweislich der dienstlichen Beurteilungen „einwandfrei" sei, führt zu keiner anderen Beurteilung. Denn es ist selbstverständlich und nicht besonders hervorzuheben, dass ein Beamter im Dienst gesetzliche Vorschriften einhält und sich in diesem Sinne „einwandfrei" verhält. Diese Umstände sind nicht geeignet, die Auffassung des Leiters der Justizvollzugsanstalt C. -T. in den Schreiben vom 27. März 2012 und 10. Mai 2012, dem Kläger mangele es an der für

die Übernahme in das Probebeamtenverhältnis erforderlichen charakterlichen Eignung, durchgreifend in Zweifel zu ziehen.

Die Klage ist auch mit den Hilfsanträgen unbegründet, weil die unter dem 27. März 2012 und 10. Mai 2012 erfolgte Ablehnung der Übernahme des Klägers in das Beamtenverhältnis auf Probe aus den vorstehenden Gründen nicht zu beanstanden ist.

Anmerkung zu SächsOVG, Urteil v. 9.9.2014, 2 A 44.14 und OVG NW, Beschluss v. 19. November 2014, 6 A 1896.13

1. Einer der wesentlichen Grundsätze des Datenschutzrechts ist das Prinzip der Zweckbindung. Leider wird diesem Grundsatz, nicht selten gerade bei einer Zweckänderung innerhalb derselben Behörde, nicht immer ausreichend Rechnung getragen.

2. Das Urteil des Sächsischen OVG vom 9. September 2014 ist dafür ein Beispiel:

a) Ein Beamter der Bundespolizei sollte mit einer Tätigkeit betraut werden, für die eine Sicherheitsüberprüfung gem. § 8 des Sicherheitsüberprüfungsgesetzes des Bundes (SÜG) erforderlich ist. Im Rahmen dieser Sicherheitsüberprüfung ergaben sich Hinweise auf eine frühere Tätigkeit des Beamten für den Staatssicherheitsdienst der DDR, die der Dienststelle zum Zeitpunkt der Ernennungen zum Beamten auf Probe und auf Lebenszeit in dieser Form nicht bekannt waren. Die Dienststelle nahm „nach Anhörung und mit Einverständnis" des Beamten Einblick in die Unterlagen des Geheimschutzbeauftragten, also anscheinend in die Sicherheitsakte gem. § 18 SÜG. Das Bundesministerium des Innern kam auf Grund der im Rahmen der Sicherheitsüberprüfung angefallenen Erkenntnisse des Bundesbeauftragten für die Unterlagen des Staatssicherheitsdienstes der ehemaligen DDR (BStU) als zuständige Oberste Bundesbehörde zu dem Ergebnis, dass der Beamte seinen Dienstherren über die Tätigkeit als inoffizieller Mitarbeiter des MfS arglistig getäuscht habe und nahm die Beamtenernennungen auf Probe und auf Lebenszeit wegen arglistiger Täuschung gem. § 14 Abs. 1 Nr. 1 BBG zurück.

b) Die beamtenrechtliche Frage, ob die Voraussetzungen des § 14 BBG vorlagen, soll hier offen bleiben. Vielmehr wird nur geprüft, ob die im Rahmen der Sicherheitsüberprüfung gewonnenen Erkenntnisse überhaupt zu diesem Zweck genutzt werden durften. Das OVG kommt zutreffend zu dem Ergebnis, dass § 21 Abs. 1 SÜG einschlägig ist. Zu eng ist es allerdings, dass das Gericht allein § 21 Abs. 1 Satz 1 SÜG prüft. Vielmehr ist auch § 21 Abs. 1 Satz 3 SÜG zu beachten: Danach darf die zuständige Stelle (in der Regel die Beschäftigungs-Dienststelle) die gespeicherten personenbezogenen Daten für Zwecke der disziplinarrechtlichen Verfolgung sowie dienst- oder arbeitsrechtlicher Maßnahmen (nur) nutzen und übermitteln, wenn dies zur Gewährleistung des Verschlusssachenschutzes erforderlich ist. Dem Verschlusssachenschutz ist im vorliegenden Fall damit ausreichend Rechnung getragen, dass der Beamte künftig keinen Zugang zu Verschlusssachen mehr enthält; sofern die bisherige Tätigkeit deshalb nicht mehr ausgeübt werden konnte, war er umzusetzen oder ggf. zu versetzen. Dabei hatte die Personalverwaltung das Ergebnis der Sicherheitsüberprüfung als für sie verbindlich ihren Personalentscheidungen zugrundezulegen; vgl. LAG Köln, Urteil v. 12. November 2007, 2 Sa 904/07, Juris. Daher war die Nutzung der im Rahmen der Sicherheitsüberprüfung gewonnenen Erkenntnisse zur Begründung der Rücknahme der beamtenrechtlichen Ernennungen nicht zulässig, weil nicht das zum Verschlusssachenschutz erforderliche Mittel. Dieses Ergebnis entspricht auch dem Sinn des § 21 Abs. 1 SÜG. Er soll dem Umstand Rechnung tragen, dass im Rahmen einer Sicherheitsüberprüfung Daten anfallen, die der Dienststelle im Rahmen der allgemeinen Personalbearbeitung nicht bekannt geworden wären. Nachdem im Rahmen des Verfahrens zur Ernennung zum Beamten entsprechende Anfragen gestellt worden waren, bestand aus Sicht der Personalverwaltung kein Anlass, eine erneute Anfrage zu stellen; ohne die Sicherheitsüberprüfung wären die neuen Erkenntnisse daher nicht bekannt geworden.

c) Nicht nachzuvollziehen ist die Erwägung des OVG, da die fraglichen Erklärungen des Beamten und dessen Ernennungen vor In-Kraft-Treten des SÜG erfolgt seien, sei fraglich, ob § 21 SÜG anwendbar sei. Die Sicherheitsüberprüfung, auf deren Akte zurückgegriffen wird, war unter der Geltung des SÜG erfolgt. Daher darf eine Nutzung der dabei erhobenen Daten auch nur unter dessen Beachtung erfolgen. Der Rückgriff auf die Rechtsprechung, die sich mit dem „Schlussstrich" der Nutzung der Erkenntnisse des BStU nach der Änderung des StUG befasst haben, ist nicht überzeugend. Dort geht es darum, ob eine nachträgliche Einschränkung der Nutzung des BStU auch für Alt-Fälle gilt; bei der Frage der Anwendbarkeit der Zweckbindungsregelungen des SÜG dagegen um Beschränkungen der Nutzung angefallener Daten. Eine Nutzung beim Staat angefallener Daten für alle Zwecke ist verfassungsrechtlich unzulässig und darf im Übrigen nur auf Grund einer gesetzlichen Grundlage erfolgen. Diese liegt, wie soeben ausgeführt, gerade nicht vor.

d) Die Zustimmung des Beamten im Hinblick auf die Einsicht in die im Rahmen der Sicherheitsüberprüfung angefallenen Unterlagen BStU rechtfertigt nicht die Nutzung der im Rahmen der Sicherheitsüberprüfung angefallen Daten für personalrechtliche Zwecke. Nach dem Tatbestand des Urteils bezog sich die Einwilligung auf den Einblick in die Unterlagen des Geheimschutzbeauftragten, die im Rahmen der Sicherheitsüberprüfung angefallen waren. Der Beamte dürfte diese allein auf das Sicherheitsüberprüfungsverfahren bezogen haben. Nur so durfte die Dienststelle als Erklärungsempfänger diese auch verstehen. Es ist lebensfremd anzunehmen, dass der Beamte auf den Schutz des § 21 Abs. 1 SÜG verzichtet und einer umfassenden Nutzung der Daten auch für Zwecke der Personalverwaltung zustimmt und damit eine Rücknahme der Beamtenernennung riskiert. Selbst wenn die Einwilligung insoweit so allgemein abgefasst war, dass sie auch die Nutzung für die Durchführung von Personalmaßnahmen erfasst, wurde sie – wie die Vorinstanz richtig ausgeführt hatte – eingeholt, um

diese Erkenntnisse unter Umgehung des § 21 SÜG umfassend nutzen zu können. Dann stellt sich die Frage, ob diese Einwilligung wirksam war. Eine Einwilligung setzt gem. § 4a BDSG eine entsprechende Belehrung voraus. Deren Vorliegen erscheint aus den soeben genannten Gründen – der Beamte wird kaum sehenden Auges seine Entlassung riskieren – fraglich. Im Falle einer unzutreffenden Belehrung war die Einwilligung nicht wirksam; die auf ihrer Grundlage gewonnenen Erkenntnisse durften nicht für Zwecke der Personalverwaltung genutzt werden. Wegen der engen Zweckbindung in § 21 SÜG durften im Übrigen die angefallenen Erkenntnisse von vornherein nicht dazu genutzt werden, die Zustimmung zu einer Anfrage bei dem BStU einzuholen; die diesbezüglichen Erwägungen des OVG zu einem „rechtmäßigen Alternativverhalten" sind daher nicht überzeugend.

e) Im Übrigen hat die Beklagte auch die von ihr zitierte Entscheidung des BVerwG – Beschluss v. 6. August 2004, 2 B 68.04, Buchholz 236.1 § 47 SG Nr. 4 – zu Unrecht darauf reduziert, ob die Kenntnis des Geheimschutzbeauftragten die Ausschlussfrist von 6 Monaten beginnen lässt. Das BVerwG hat aber ausgeführt:

„Deshalb wäre es sogar unzulässig, wenn der Dienstherr das im Rahmen einer Sicherheitsüberprüfung nach Maßgabe des § 14 Abs. 1 Satz 2 SÜG etwa dennoch erlangte Wissen davon, dass ein Soldat seine Ernennung seinerzeit durch arglistige Täuschung herbeigeführt hat, dazu nutzt, den Soldaten nach § 46 Abs. 2 SG zu entlassen. Aus der Unverwertbarkeit des so erlangten Wissens von der bei der Einstellung begangenen Täuschung für eine Entscheidung nach § 46 Abs. 2 SG folgt, dass auch die Frist, innerhalb derer diese Entscheidung zu treffen ist, durch die Kenntniserlangung nach § 14 Abs. 1 Satz 2 SÜG nicht in Gang gesetzt wird."

Der Beschluss bestätigt vielmehr ausdrücklich, dass die im Rahmen der Sicherheitsüberprüfung angefallenen Daten nicht für die Rücknahme der beamtenrechtlichen Ernennungen herangezogen werden dürfen.

3. Nicht unbedenklich ist auch der Beschluss des OVG NW v. 19. November 2014, 6 A 1896/13:

Der Beamte auf Widerruf hatte im Rahmen des Einstellungsverfahrens wahrheitswidrig erklärt, dass gegen ihn in den letzten drei Jahren keine Strafverfahren anhängig gewesen waren; im Rahmen einer Sicherheitsüberprüfung waren diese aber bekannt geworden. Das OVG hat dem Dienstherren zugebilligt, er habe zu Recht aus diesen wahrheitswidrigen Angaben den Schluss gezogen, dass eine vertrauenswürdige Zusammenarbeit mit dem Beamten nicht möglich sei. Zwar erfolgte die Ernennung zum Beamten auf Widerruf ausdrücklich „vorbehaltlich eines beanstandungsfreien Ergebnisses der durchzuführenden Sicherheitsüberprüfung". Diese Formulierung erfasst zunächst den Fall, dass ein Sicherheitsrisiko vorliegt, das der Betrauung mit einer sicherheitsempfindlichen Tätigkeit entgegensteht. Hinzu kommt bei dieser weiten Formulierung zwar auch ein Ergebnis ohne Feststellung eines Sicherheitsrisikos, aber der Einschränkung, dass der Beamte mit bestimmten Funktionen nicht betraut werden darf. Das Ergebnis der Sicherheitsüberprüfung ergibt sich aus dem Urteil zwar nicht. Da der Beamte später aber in der vorgesehenen Tätigkeit verwendet wurde, ist allerdings davon auszugehen, dass aus sicherheitsrechtlicher Sicht keine Bedenken gegen seine Zuverlässigkeit bestanden. Von diesem Wortlaut nicht erfasst ist es – so aber die Personalverwaltung –, dass bereits die Tatsache, dass eine sicherheitserhebliche Erkenntnis nicht zu einer sicherheitsrechtlich bedingten Einschränkung führte, ausreicht. Unabhängig davon gilt aber auch hier das oben Ausgeführte: Gem. § 22 SÜG NW (der insoweit inhaltlich § 21 SÜG entspricht und vom Senat nicht geprüft wird), durfte der Personalverwaltung nur mitgeteilt werden, ob die Betrauung des Beamten mit einer sicherheitsempfindlichen Tätigkeit in Betracht kommt oder nicht. Dagegen durften die dabei gewonnenen Erkenntnisse – hier die Tatsache, dass der Beamte die früheren und inzwischen abgeschlossenen Strafverfahren verschwiegen hat – nicht mitgeteilt und für die Entlassung aus dem Beamtenverhältnis herangezogen werden. Diese eingeschränkte Nutzungsmöglichkeit trifft – vgl. insoweit den zitierten Beschluss des BVerwG v. 6. August 2004 – auch den Dienststellenleiter. Dieser muss sein Wissen aus der Sicherheitsüberprüfung bei Personalmaßnahmen ausblenden. Dies entspricht nicht nur den Regeln zur Zweckbindung, sondern ergibt sich auch aus dem strengen Grundsatz der Trennung von Personalverwaltung und dem für die Durchführung der Sicherheitsüberprüfung zuständigen Bereich; vgl. § 3 Abs. 1 Satz 3 SÜG und – für den hier behandelten Fall – § 4 Abs. 2 SÜG NW. Wenn aus Sicht der Personalverwaltung – verständlicherweise – für die Frage der Ernennung zum Beamten auf Widerruf frühere Strafverfahren von Bedeutung waren, hätte sie selbst entsprechende Anfragen stellen müssen und erst danach die Sicherheitsüberprüfung einleiten dürfen.

(Dr. Bernd Eicholt)

Zur Haftung des Betreibers eines Ärzteportals für Bewertungen, die unwahre Tatsachen enthalten

(**Landgericht Frankfurt am Main**, Urteil vom 5. März 2015 – 2-030 188/14 –)

1. **Der Betreiber eines Internetportals für Ärztebewertungen haftet als Störer für Persönlichkeitsrechtsverletzungen, die auf der Veröffentlichung von unwahren Tatsachen beruhen.**
2. **Auf eine Beanstandung der angeblich in ihren Rechten verletzten Person hin muss der Betreiber im Hinblick auf die angegriffene Äußerung Tatsachen vortragen, auf die der Arzt sich prozessual einlassen kann, um den Wahrheitsgehalt widerlegen zu können.**
3. **Die Tatsachenbehauptung „Behandlungsbedarf an der Stirne lag vor. Wurde nicht empfohlen" muss, wenn der Arzt sich keiner Behandlung entsinnen kann, auf welche diese Bewertung zutreffen könnte, näher belegt werden.**

(Nicht amtliche Leitsätze)

Sachverhalt:

Die Klägerin begehrt von der Beklagten die Unterlassung der Verbreitung einer Arztbewertung im Internet.

Bei der Klägerin handelt es sich um eine in … niedergelassene Hautärztin.

Die Beklagte ist ein Unternehmen mit Sitz in München. Sie betreibt unter der Adresse www.xyz.de ein Internetportal, auf dem sie Verbrauchermeinungen zu Ärzten veröffentlicht. Nach ihrer eigenen Darstellung handelt es sich dabei mit mehr als 3,5 Millionen Patienten monatlich um das größte deutsche Arztempfehlungsportal. Die Nutzer der Internetseite können sich dabei zu dem Arztbesuch äußern sowie anhand bestimmter Kriterien Schulnoten vergeben.

Unter dem Datum vom 18.12.2013 veröffentlichte die Beklagte auf ihrer Internetseite die von einem nicht näher bezeichneten Nutzer eingegebene streitgegenständliche Bewertung der Klägerin. Diese trägt den Titel

„Hautkrebsvorsorge Termin. 10 Min. flüchtige…"

und lautet wie folgt:

„… Ansehung des Körpers.
48 € kassiert und Tschüss.
Wie später erfahren. Behandlungsbedarf an der Stirne lag vor.
Wurde nicht empfohlen."
Notenbewertung dieses Patienten
Behandlung 6,0
Aufklärung 6,0
Vertrauensverhältnis 6,0
Genommene Zeit 6,0
Freundlichkeit 4,0

Am 23.12.2013 wandte sich die Klägerin persönlich gemäß Anlage B 1 mit der Bitte an die Beklagte, die aus ihrer Sicht unrichtige Bewertung zu entfernen. Dabei äußerte sie zudem den Verdacht, dass die Bewertung von einem ihrer Konkurrenten eingestellt worden sei. Mit E-Mail vom 03.01.2014 erklärte die Beklagte, dass der Autor der streitgegenständlichen Bewertung die Behandlung bestätigt habe. Insoweit nahm die Beklagte Bezug auf ein – teilweise geschwärztes bzw. geweißtes – Schreiben vom 24.12.2013 gemäß Anlage B 2, welches angeblich von dem Autor der Bewertung stamme. In dieser Anlage ist u.a. festgehalten: „Genauso wie beschrieben. war der Ablauf…., dass dies einer Behandlung bedarf. Habe mir bei einem anderen Hautarzt im neuen Jahr ein Termin geholt.". Die Beklagte erklärte ferner, keine Zweifel an der Authentizität der Bewertung zu haben.

Mit anwaltlichem Schreiben vom 04.02.2014 forderte die Klägerin die Beklagte erneut zur Löschung der streitgegenständlichen Bewertung auf. Daraufhin erklärte die Beklagte mit E-Mail vom 14.02.2014, dass sie von dem Autor der streitgegenständlichen Bewertung einen Beleg erhalten hätte, davon ausginge, dass es sich um einen authentischen Nutzer handele und sie die Bewertung im Portal wieder eingestellt habe. Mit anwaltlichem Schreiben vom 10.03.2014 forderte die Klägerin die Beklagte wiederum zur Löschung der Bewertung auf und setzte dazu eine Frist bis zum 24.03.2014, die ohne Reaktion der Beklagten verstrich. Mit anwaltlichem Schreiben vom 28.04.2014 mahnte die Klägerin die Beklagte ab und forderte sie zur Abgabe einer strafbewehrten Unterlassungserklärung auf. Die Beklagte wies diese Abmahnung mit E-Mail vom 05.05.2014 zurück.

Aus den Gründen:

Die Klage ist begründet.

Der Klägerin steht ein Anspruch gegen die Beklagte auf Unterlassung der Verbreitung der streitgegenständlichen Bewertung wegen der dort enthaltenen Äußerung „Wie später erfahren. Behandlungsbedarf an der Stirne lag vor. Wurde nicht empfohlen." aus den §§ 1004, 823 Abs. 1 BGB analog i.V.m. Art. 2 Abs. 1, 1 Abs. 1 GG zu.

Die Beklagte hat durch die Veröffentlichung der beanstandeten Äußerung das allgemeine Persönlichkeitsrecht der Klägerin verletzt. Das allgemeine Persönlichkeitsrecht wird aus Art. 2 Abs. 1, 1 Abs. 1 GG abgeleitet. Es schützt die Persönlichkeit in all ihren Ausprägungen und damit auch in ihrer Darstellung nach außen und in ihrer sozialen Geltung (vgl. BVerfG, NJW 1999, 1322, 1323).

Die Beklagte trifft hinsichtlich der von der Klägerin beanstandeten Bewertung zwar nur eine eingeschränkte Verantwortlichkeit, weil sie diese weder verfasst noch sich den Inhalt zu Eigen gemacht hat. Sie kann als sog. Hostproviderin lediglich als Störerin in Anspruch genommen werden, weil sie die technischen Möglichkeiten der Plattform zur Verfügung gestellt hat. Die Störereigenschaft scheitert nicht an § 10 TMG, weil die dort geregelte Haftungsbeschränkung nach höchstrichterlicher Rechtsprechung nicht für Unterlassungsansprüche gilt (vgl. OLG Stuttgart, Urteil vom 26.06.2013, 4 U 28/13 = BeckRS 2014, 10797 Tz. 37).

Als Störerin ist verpflichtet, wer, ohne Täter oder Teilnehmer zu sein, in irgendeiner Weise willentlich und adäquat kausal zur Beeinträchtigung des Rechtsguts beiträgt (vgl. BGH, NJW 2012, 148 – Blog-Eintrag). Indem die Beklagte das Internetportal www.xyz.de betreibt, dabei den Speicherplatz für Bewertende bereitstellt und den Abruf der Webseite über das Internet ermöglicht, trägt sie willentlich und adäquat kausal zur Verbreitung der Äußerungen bei, die gegebenenfalls das allgemeine Persönlichkeitsrecht Dritter beeinträchtigen.

Eine Haftung der Beklagten als Hostprovider für den von dem Nutzer des Bewertungsportals ihres Internetdienstes eingestellten Beitrags ist zu bejahen.

Nach den in der Entscheidung „Blog-Eintrag" des BGH vom 25.10.2011 (NJW 2012, 148) aufgezeigten Grundsätzen, die sich in ständiger Rechtsprechung verfestigt und weiterentwickelt haben (vgl. BGH, GRUR 2013, 751 – Autocomplete-Funktion) ist ein Hostprovider nicht verpflichtet, die von Nutzern in das Netz gestellten Beiträge vor der Veröffentlichung auf eventuelle Rechtsverletzungen zu überprüfen. Er ist aber verantwortlich, sobald er Kenntnis von der Rechtsverletzung erlangt. Weist ein Betroffener den Hostprovider auf eine Verletzung seines Persönlichkeitsrechts hin, kann dieser als Störer verpflichtet sein, zukünftige derartige Verletzungen zu unterbinden (vgl. BGH, GRUR 2004, 860 – Internet-Versteigerung I; BGH, GRUR 2007, 708 – Internetversteigerung II; BGH GRUR 2007, 890 – Jugendgefährdende Medien bei ebay).

Regelmäßig ist zunächst die Beanstandung des Betroffenen an den für die Bewertung Verantwortlichen zur Stellungnahme zuzuleiten. Dies ist hier – nach dem Vortrag der Beklagten – geschehen. Stellt der Bewertende die Berechtigung der Beanstandung substantiiert in Abrede und ergeben sich deshalb berechtigte Zweifel, so ist die Beklagte als Plattformbetreiberin grundsätzlich gehalten, dem Betroffenen dies mitzuteilen und gegebenenfalls Nachweise zu verlangen, aus denen sich die behauptete Rechtsverletzung ergibt (BGH, NJW 2012, 148 Rn. 27 – Blog-Eintrag).

Die Klägerin trifft als derjenigen, die die Beklagte unter dem Gesichtspunkt der Störerhaftung auf Unterlassung in Anspruch nimmt, die Darlegungs- und Beweislast hinsichtlich der tatsächlichen Voraussetzungen eben dieser Haftung. Das umfasst die Darlegung der Umstände, aus denen sich eine Verletzung der die Beklagte im Zusammenhang mit der Prüfung der Berechtigung der Beanstandung treffenden reaktiven Prüfungspflicht ergibt. Da die auf eine behauptete Rechtsverletzung hin initiierte Prüfung des Hostproviders in aller Regel interne Betriebsabläufe, vor allem den Kontakt mit dem vorliegend auch nur ihm bekannten Verfasser der Bewertung betrifft, die der Einsichtnahme durch die Klägerin ent-

zogen sind, trifft den Provider hinsichtlich der ihm zur Prüfung der Beanstandung vorgenommenen Handlungen eine Darlegungsverpflichtung. Er muss aufzeigen, dass und ggf. wie er mit dem Bewertenden in Kontakt getreten ist und welche Stellungnahme dieser ggf. zur Verteidigung der angegriffenen Bewertung/Äußerung in der Sache vorgebracht hat.

Denn nur dann ist es der betroffenen Anspruchstellerin möglich, substantiell die Berechtigung der Beanstandung „nachzuweisen" (vgl. OLG Köln, 16 U 141/14, Urteil vom 16.12.2014, Seite 6 gemäß Anlage B 6, Bl. 80 d.A.). Die Beklagte muss im Rahmen ihrer sekundären Darlegungslast Belegtatsachen für ihre Behauptungen angeben, andernfalls wäre gemäß § 138 Abs. 3 ZPO von der Unwahrheit auszugehen (vgl. BGH, NJW 2008, 2262 Rn. 22; Palandt/Sprau, BGB, 74. Aufl., Einf. v § 823 Rn. 40).

Darüber hinaus trifft aber die Beklagte nach allgemeinen Grundsätzen auch eine erweiterte Darlegungslast im Hinblick auf die Wahrheit der von ihr verbreiteten Tatsachenbehauptungen. In diesem Rahmen kann von der Beklagten verlangt werden, im Hinblick auf die angegriffene Äußerung Tatsachen vorzutragen, auf die die Klägerin sich prozessual einlassen kann. Dem ist die Beklagte vorliegend nicht in hinreichendem Umfang nachgekommen.

In der hier angegriffenen Äußerung „Wie später erfahren. Behandlungsbedarf an der Stirne lag vor. Wurde nicht empfohlen." ist eine Tatsachenbehauptung zu sehen.

Während sich Tatsachenbehauptungen auf etwas tatsächlich Geschehenes oder auf einen gegenwärtigen Zustand beziehen und deshalb grundsätzlich dem Beweis offen stehen, sind Meinungsäußerungen bzw. Werturteile durch Elemente der Stellungnahme und des Dafürhaltens bzw. Meinens geprägt und deshalb dem Beweis von vornherein nicht zugänglich (vgl. BVerfGE 94, 1, 8; BGH, NJW 1996, 1131, 1133; BGH, NJW 1998, 3047, 3048; BGH, NJW 2002, 1192, 1193). Entgegen der Einschätzung der Beklagten ist vorliegend bei der zitierten Äußerung hinsichtlich des Behandlungsverlaufs von einer dem Beweis zugänglichen Tatsachenbehauptung und nicht nur von einer (zulässigen), ggf. mehrdeutigen, Meinungsäußerung, auch unter Beachtung des Gesamtkontextes der Bewertung, auszugehen.

Auch wird der verständige Leser der Bewertung aufgrund der Angabe „Hautkrebsvorsorge" davon ausgehen, dass die Hautuntersuchung durch die Klägerin als Hautärztin dem Zweck der Krebsvorsorge diente, nämlich etwaige Hautveränderungen bzw. etwaige sog. Muttermale im Hinblick auf das Vorhandensein eines Hautkrebses oder dessen potentieller Entwicklung zu untersuchen. Auch wird der Leser daraus den Vorwurf des Bewerters gegenüber der Hautärztin entnehmen, dass die Ärztin solche Auffälligkeiten an der Stirn eines Patienten übersehen habe.

Doch auf diese Differenzierung kommt es vorliegend nicht entscheidend an. Der Vortrag der Klägerin ist erkennbar nicht darauf beschränkt, dass sie bestreitet, den Fall einer nicht erkannten Hautkrebserkrankung übersehen zu haben. Die Klägerin bestreitet vielmehr ganz allgemein, dass sich der von dem Autor der streitgegenständlichen Bewertung beschriebene Vorfall – nämlich ein von der Klägerin im Rahmen einer Hautkrebsvorsorgeuntersuchung nicht erkannter Behandlungsbedarf an der Stirn eines Patienten bzw. einer Patientin – ereignet habe.

Diese Äußerung ist nach den oben dargestellten Grundsätzen auch unwahr. Denn die Beklagte ist der ihr obliegenden sekundären Darlegungslast nicht in hinreichendem Umfang nachgekommen.

Da beklagtenseits die Identität des Bewertenden und die zum Vorwurf gemachte Behandlung durch die Übersendung der wenig aussagekräftigen Anlage B 2, die angeblich von dem Verfasser der Bewertung stammen soll, nicht offenbart wurden und auch sonst das Schreiben überwiegend geweißt und die angebliche Rechnung ebenfalls gemäß Anlage B 4 (Bl. 55 d.A.) geschwärzt wurde, ist es der Klägerin nicht möglich, die Authentizität der Bewertungen von etwaigen Patienten und den behaupteten Sachverhalt zu konkretisieren, den sie in Abrede stellt.

Die Klägerin hat dargelegt, dass sich die streitgegenständliche Bewertung mit keiner der von ihr vorgenommenen Behandlungen deckt. Ihr sei kein Fall bekannt, in dem sie eine Hautauffälligkeiten im oben ausgeführten Sinne an der Stirn eines Patienten oder einer Patientin übersehen hätte. Demgegenüber hat die Beklagte lediglich die von der Klägerin vorgenommene Interpretation der streitgegenständlichen Aussage angegriffen. Nach der Einschätzung der Beklagten müsse es sich bei der in der Bewertung geschilderten Behandlung nicht zwangsläufig um einen Fall einer nicht erkannten Krebserkrankung handeln. Es könne danach auch sein, dass die Klägerin bei dem Autor eine andere, behandlungsbedürftige Hautveränderung nicht erkannt und eine weitergehende Behandlung nicht empfohlen habe.

Auch sofern die Beklagte in ihrer Klageerwiderung auf die Schilderung des Geschehens durch den vermeintlichen Autor der Bewertung in seiner E-Mail an die Beklagte vom 24.12.2013 verweist, genügt die Beklagte nicht der ihr obliegenden Darlegungslast.

Aus der vorgelegten E-Mail des Autors geht nicht hervor, aus welchen Gründen dieser der Auffassung ist, es habe bei ihm ein von der Klägerin nicht empfohlener Behandlungsbedarf vorgelegen. Darin schildert der Autor zunächst lediglich in pauschaler Form, dass der „Ablauf wie beschrieben" war. Der weitere Inhalt der E-Mail ist weitestgehend unkenntlich gemacht. So findet sich gegen Ende der E-Mail lediglich noch der Halbsatz „… dass dies der Behandlung bedarf". Es verbleibt jedoch gänzlich unklar, worauf sich der behauptete Behandlungsbedarf bezieht und woraus der Autor zu dem Schluss gekommen ist, dass ein bestimmter Behandlungsbedarf besteht. Dabei handelt es sich bei der Frage, ob ein bestimmter Befund tatsächlich nach den Erkenntnissen der wissenschaftlichen Medizin einer ärztlichen Behandlung bedarf, um einen Umstand, der nach allgemeiner Lebenserfahrung allein von einem Arzt festgestellt werden kann. Dass der Autor der streitgegenständlichen Bewertung einen anderen Arzt konsultiert hat, geht aber aus der vorgelegten E-Mail nicht hervor. Umgekehrt wird in dem letzten Satz der E-Mail sogar ausgeführt, dass der Autor eine weitere ärztliche Konsultation erst in Zukunft wahrnehmen möchte.

Über diese E-Mail hinaus hat die Beklagte keinen tauglichen Vortrag zum Beleg der Wahrheit der angegriffenen Aussage dargelegt. Neben der vorgelegten, weitestgehend unkenntlich gemachten E-Mail hat sie lediglich Frau B, eine Mitarbeiterin aus dem Qualitätsmanagement der Beklagten, als Zeugin benannt. Es ist jedoch nicht ersichtlich, wie diese zur Aufklärung der Wahrheit oder Unwahrheit der streitgegenständlichen Aussage beitragen können soll. Die in der Bewertung geschilderten Vorgänge sind nicht Gegenstand ihrer eigenen Wahrnehmung gewesen. Es ist vielmehr anzunehmen, dass Frau B als Mitarbeiterin aus dem Qualitätsmanagement allenfalls zu der Kommunikation, die zwischen der Beklagten und dem Autor der Bewertung stattgefunden hat, aussagen könnte. Die hier zu beantwortende Frage, ob in dem streitgegenständlichen Fall tatsächlich ein von der Klägerin nicht erkannter, medizinisch relevanter Befund bestand und die Klägerin eine medizinisch indizierte Behandlung nicht empfohlen hat, wird sie dagegen nicht aufklären können.

Die Kammer teilt zumindest vorliegend aufgrund der beklagtenseits vorgelegten Unterlagen auch nicht die Einschätzung der Beklagten, dass von dieser nicht mehr an Vortrag verlangt werden könnte als die Vorlage von geschwärzten Nachweisen, da sie andernfalls unter Verstoß gegen datenschutzrechtliche Bestimmungen den Autor der Bewertungen direkt oder indirekt offenbaren müßte.

Die Beklagte ist damit ihrer Darlegungslast, zumindest ihrer sekundären, nicht ausreichend nachgekommen, so dass die Kammer davon ausgeht, dass es sich im Rahmen der streitgegenständlichen Bewertung „Behandlungsbedarf an der Stirne lag vor. Wurde nicht empfohlen." um eine unwahre Tatsachenbehauptung und nicht nur um eine gemäß Art. 5 Abs. 1 GG geschützte Meinungsäußerung handelt. Eine unwahre Tatsachenbehauptung fällt nicht unter den grundrechtlichen Schutz. Ihre bewusste Äußerung bzw. Verbreitung stellt einen widerrechtlichen Eingriff in das allgemeine Persönlichkeitsrecht des Verletzten dar (vgl. BVerfG, NJW 1999, 1322, 1324; BVerfG, NJW 2000, 199, 200; BVerfG, NJW 2004, 354, 355; BGH, GRUR 2013, 751 Rn. 22 – „Autocomplete"-Funktion; BGH, GRUR 2012, 850 Rn. 37 – www.rainbow.at II).

Dem steht auch nicht entgegen, dass die Beklagte grundsätzlich nicht zur Auskunft über ihre Nutzer verpflichtet bzw. berechtigt ist. Der BGH hat zwar in seiner Entscheidung vom 01.07.2014, VI ZR 345/13, NJW 2014, 2651 – Ärztebewertungsportal, den Betreiber eines Internetportals mit Blick auf das in § 12 TMG formulierte Verbot, personenbezogene Daten der Nutzer eines Internetdienstes außerhalb bestimmter Erlaubnistatbestände zu verwenden, nicht als befugt erachtet, personenbezogene Daten des Nutzers zur Erfüllung eines wegen der Persönlichkeitsrechtsverletzung geltend gemachten Auskunftsanspruchs an den Betroffenen zu übermitteln. Damit wäre der Provider nicht verpflichtet, Namen und Anschrift des Verfassers eines Blog-Eintrags dem Betroffenen zu übermitteln. Dieses Auskunftsbegehren ist aber vorliegend nicht Streitgegenstand.

Denn der Betroffene kann von einem Provider jedenfalls die Löschung unwahrer Tatsachenbehauptungen verlangen. Die Möglichkeit eines Betroffenen, sich insbesondere gegen unwahre Tatsachenbehauptungen im Rahmen eines Ärztebewertungsportals dadurch wehren zu können, dass er sich unter Bezugnahme auf den jeweiligen Eintrag an die Beklagte wendet und dort dessen Beseitigung verlangt, wird ausdrücklich vom BGH in der Entscheidung vom 23.09.2014, GRUR 2014, 1228 Rn. 36 – Ärztebewertungsportal, bejaht.

Auch bei der vorzunehmenden Abwägung zwischen den kollidierenden Interessenlagen erscheint es angesichts des Vorliegens einer unwahren Tatsachenbehauptung eher der Beklagten zuzumuten, die kritisierende Bewertung zu löschen, als von der Klägerin, diese hinzunehmen. Durch die Aufnahme in das von der Beklagten betriebene Ärztebewertungsportal wird die Klägerin aufgrund der beschriebenen Fehlbehandlung beruflich erheblich belastet. Die schwerwiegende Persönlichkeitsrechtsverletzung wiegt insoweit gegenüber einer Beeinträchtigung der Kommunikationsfreiheit höher, auch unter Berücksichtigung des Umstands, dass die Klägerin (nur) in ihrer beruflichen Sozialsphäre betroffen ist, zumal hier eine unwahre Tatsachenbehauptung betroffen ist und nicht nur eine Meinungsäußerung.

Die Klägerin kann auch die Löschung der angegriffenen Bewertung insgesamt verlangen und nicht nur diejenige oben erörterten unwahren Tatsachenbehauptung: „Behandlungsbedarf an der Stirne lag vor. Wurde nicht empfohlen".

Bereits diese eine unwahre Tatsachenbehauptung in der Bewertung, die von der Beklagten verbreitet wird, rechtfertigt das hier titulierte vollständige Verbot einer Veröffentlichung des gesamten Textes in seiner konkret angegriffenen Form auf der Internetplattform der Beklagten, ohne dass es auf eine Prüfung etwaiger weiterer Äußerungen oder Bewertungen, wozu auch die Benotungen gehören, die sich sämtlichst als zulässige Meinungsäußerungen darstellen dürften, ankäme. Die insoweit vom BGH (WRP 2001, 400, 403 – TCM-Zentrum) im Wettbewerbsrecht entwickelten Grundsätze sind auch vorliegend anwendbar. Das hier auf das Verbot der konkreten Verletzungsform gerichtete Klagebegehren war damit schon deshalb in vollem Umfang begründet, da darin jedenfalls die oben bezeichnete falsche Tatsachenbehauptung enthalten ist. Ob darüber hinaus weitere persönlichkeitsrechtsverletzende Tatsachenbehauptungen oder sonst unzulässige Äußerungen enthalten sind, kann damit dahinstehen.

Die Entscheidung über die Androhung eines Ordnungsmittels beruht auf § 890 ZPO.

Der von der Klägerin mit dem Klageantrag zu 2) geltend gemachte Anspruch auf Ersatz vorgerichtlicher Abmahnkosten aus §§ 677, 683 S. 1, 670 BGB ist begründet. Sie hat mit der vorprozessualen Abmahnung ein Geschäft der Beklagten geführt (vgl. zu Ansprüchen aus Geschäftsführung ohne Auftrag (GoA): BGH GRUR 1992, 176, 177 – „Abmahnkostenverjährung"; BGH GRUR 1994, 311, 312 – „Finanzkaufpreis ohne Mehrkosten"; BGH GRUR 2001, 450, 453 – „Franzbranntwein-Gel"). Denn die bei Verletzung von Persönlichkeitsrechten, ähnlich den Wettbewerbsrechten vermutete Wiederholungsgefahr kann in der Regel nur durch Abgabe einer strafbewehrten Unterlassungserklärung beseitigt werden. Der Wille der Klägerin zur Fremdgeschäftsführung wird vermutet (vgl. BGHZ 98, 235; BGH NJW 2000, 72). Zu den gemäß §§ 683 S. 1, 670 BGB zu ersetzenden erforderlichen Aufwendungen zählen die Kosten der anwaltlichen Abmahnung und Aufforderung zur Abgabe einer strafbewehrten Unterlassungserklärung.

Im Hinblick auf die Privilegierung des § 10 TMG, auf die sich die Beklagte vorliegend berufen kann, gilt, dass Abmahnkosten erst verlangt werden können, wenn der Anspruchsgegner als Störer haftet. Dementsprechend ist auch der Ersatz von Abmahnkosten erst möglich, wenn der Provider Kenntnis von einer konkreten Rechtsverletzung erlangt hat (BGH GRUR 2011, 1038 Rn. 21 f. – Stiftparfüm; BGH, GRUR 2013, 751 – Autocomplete-Funktion). So lag der Fall hier. Die Klägerin hat die Beklagte unter dem 23.12.2013 auf die streitgegenständliche Bewertung hingewiesen. Erst nachdem die Beklagte sich weigerte, die Bewertung zu entfernen, ließ die Klägerin die Beklagte mit anwaltlichem Schreiben vom 04.02.2014 abmahnen.

Der nunmehr von der Klägerin ihrer Forderung auf Abmahnkostenerstattung im vorliegenden Rechtsstreit zugrunde gelegte Gegenstandswert von 10.000 EUR erscheint gemäß § 3 ZPO als angemessen. Der Ansatz einer 1,3fachen Geschäftsgebühr für die Abmahnung ist gerechtfertigt. Ansatzpunkte, hier eine geringere Gebühr anzusetzen, sind nicht ersichtlich.

Unter Zugrundelegung eines Gegenstandswerts von 10.000 EUR berechnet sich der klägerische Erstattungsanspruch in Höhe von 887,03 EUR wie folgt:

Geschäftsgebühr gem. Nr. 2300 VV, §§ 13, 14 RVG 725,40 EUR; Entgelt für Post- und Telekommunikations-Dienstleistungen gem. Nr. 7002 VV (pauschal) 20,00 EUR; 19 % Umsatzsteuer gem. Nr. 7008 VV 141,63 EUR.

Fotografieren von sich nicht ordnungsgemäß verhaltenden Hundebesitzern

(**Landgericht Bonn**, Urteil vom 7. Januar 2015 – 5 S 47/14 –)

1. **Ein durch das uneingewilligte Fotografieren vollzogener Eingriff in das Recht am eigenen Bild kann im Rahmen einer Güter- und Interessenabwägung gerechtfertigt sein, soweit es dem Handelnden um die Wahrung von Individualinteressen geht.**

2. **Die Wahrnehmung von Belangen der Allgemeinheit durch das Anzeigen von Ordnungswidrigkeiten (hier im Bereich des Naturschutzes) gibt einer Privatperson nicht das Recht, einen Hundebesitzer, der sein Tier frei laufen lässt, zwecks konkreter Beweisführung zu fotografieren.**

(Nicht amtliche Leitsätze)

Aus den Gründen:

Die zulässige Berufung des Beklagten ist unbegründet. Das Amtsgericht hat den Beklagten zu Recht dazu verurteilt, Fotoaufnahmen des Klägers beim Hundeausführen in der Siegaue ohne dessen Einwilligung zu unterlassen. Der entsprechende Anspruch des Klägers ergibt sich aus §§ 823 Abs. 1, 1004 Abs. 1 Satz 2 BGB analog.

Ein – ggf. unzulässiger – Eingriff in das Recht am eigenen Bild als Ausprägung des Allgemeinen Persönlichkeitsrechts liegt bereits dann vor, wenn – wie hier – ohne Einwilligung des Betroffenen Bildnisse hergestellt werden, wobei es nicht entscheidend darauf ankommt, ob Fotos mit der Absicht, sie der Öffentlichkeit zugänglich zu machen bzw. zu verbreiten, angefertigt werden (BGH NJW 1995, 1955 ff.).

Das Amtsgericht hat mit zutreffender Begründung ausgeführt, dass dieser Eingriff in das Recht am eigenen Bild hier auch rechtswidrig und damit unzulässig war. Nach der Rechtsprechung des Bundesgerichtshofs ist dies im Falle der Anfertigung von Bildern in Bereichen, die der Öffentlichkeit zugänglich sind, im Zuge einer Würdigung aller Umstände des Einzelfalls und durch Vornahme einer unter Berücksichtigung aller rechtlich, insbesondere auch verfassungsrechtlich geschützten Positionen der Beteiligten durchgeführten Güter- und Interessenabwägung zu ermitteln (BGH a.a.O.).

Ganz entscheidend ist bereits im Ausgangspunkt dieser Abwägung hier die Frage, welche (verfassungs-)rechtlichen Positionen in die Abwägung eingestellt werden können. Der Beklagte geht insoweit davon aus, dass er für sich die Einhaltung der Naturschutzvorschriften und deren Durchsetzung im Wege des Ordnungswidrigkeitsverfahrens ins Feld führen kann. Naturschutzvorschriften – grundgesetzlich verankert als Staatsziel in Art. 20a GG und nicht etwa als Grundrecht der Bürgerinnen und Bürger im Katalog der Art. 1 bis 19 GG – betreffen allerdings keine Individualrechtsgüter.

Der Bundesgerichtshof spricht in der zitierten Entscheidung aber davon, dass (verfassungs-)rechtliche Positionen der Beteiligten in die Erwägung einzubeziehen sind. Auch in der Rechtsprechung nach diesem Urteil geht es stets um Individualrechtsgüter, denen das Fertigen von Bildern oder Videos dienen sollte (vgl. insoweit: LG Bonn, Urteil vom 04.05.2012, Az.: 9 O 60/12; LG Köln, Beschluss vom 21.08.2013, Az.: 34 T 179/13; OLG München, Beschluss vom 04.01.2012, Az.: 20 U 464/11; LG München, Beschluss vom 18.10.2011, Az.: 1 S 12752/11 WEG; OLG Köln, Urteil vom 05.07.2005, Az.: 24 U 12/05; LG Berlin, Urteil vom 23.05.2005, Az.: 62 S 37/05; LG Darmstadt, Urteil vom 17.03.1999, Az.: 8 O 42/99; OLG Karlsruhe, Urteil vom 08.11.2001, Az.: 12 U 180/01 alle zitiert nach juris). Auch in der Kommentarliteratur zu dem Schutz des Allgemeinen Persönlichkeitsrechts im Rahmen des § 823 BGB und zur erforderlichen Abwägung heißt es, dass im Einzelfall das Allgemeine Persönlichkeitsrecht des Verletzten den schutzwürdigen Belangen des Schädigers, also insbesondere grundrechtlichen Positionen gegenüberzustellen ist (vgl. Münchener Kommentar-Wagner, BGB, § 823 Rn. 242; Palandt-Sprau, BGB, § 823 Rn. 95, 99).

Nichts anderes ergibt sich aus Entscheidungen des Oberlandesgerichts Düsseldorf (Urteil vom 05.05.1997, Az.: 5 U 82/96, zitiert nach juris) und des Oberlandesgerichts Karlsruhe (Urteil vom 08.11.2001, Az.: 12 U 180/01). Danach kann auch das verdeckte Anfertigen und Verwerten von Videomaterial zum Zwecke der Aufklärung einer Straftat rechtmäßig sein. In beiden Entscheidungen ging es allerdings um das Anfertigen und Verwenden von Bildern durch den Geschädigten selbst, der also ausschließlich seine eigenen Individualrechtsgüter im Blick hatte und nicht etwa Belange der Allgemeinheit. Ob im Falle erheblicher Straftaten auch ein nicht von dieser Straftat Betroffener dem Rechtsgedanken der Nothilfe folgend quasi für den Geschädigten Foto- oder Videomaterial anfertigen darf, kann hier dahinstehen, denn es geht zum einen nicht um eine (erhebliche) Straftat, zum anderen ist auch kein Individualrechtsgut eines Dritten betroffen, so dass auch der Rechtsgedanke der Nothilfe hier nicht bemüht werden kann.

Nach diesen Grundsätzen kann der Beklagte nicht auf die Belange des Naturschutzes abstellen, um seine Fotografien zu rechtfertigen. Auch soweit der Beklagte für sich das „Recht auf eine effektive Anzeige" unter Bezugnahme auf die Vorschriften der §§ 46 OWiG, 158 Abs. 1 StPO in Anspruch nimmt, ist dieses hier mangels eines betroffenen Individualrechtsguts gerade nicht tangiert. Schon aus der seitens des Beklagten zitierten Entscheidung des Bundesverfassungsgerichts (Beschluss vom 25.02.1987, Az.: 1 BvR 1086/85, zitiert nach juris) ergibt sich nämlich insoweit, dass aus dem Rechtsstaatsgebot folgt, dass der einzelne, der sein Recht nicht selbst in die Hand nehmen darf, zur Wahrnehmung seiner Rechte das Recht haben muss, Anzeige zu erstatten. Auch dieses verfassungsrechtlich verankerte Recht hängt damit davon ab, dass es um Individualrechtsgüter des Einzelnen geht. Selbst wenn dies nicht der Fall wäre, könnte der Beklagte aus dem „Recht auf eine effektive Anzeige" hier nichts herleiten. Denn es soll ihm ja nicht verboten werden, von ihm wahrgenommene Ordnungswidrigkeiten anzuzeigen. Vielmehr geht es um die Frage, ob er diese mit Beweismitteln in Form von Fotografien unterlegen darf.

Festzuhalten ist ferner, dass eine Bürgerin oder ein Bürger, die oder der eine Anzeige erstattet, keine eigenen subjektiven Rechte mit Blick auf die Verfolgung von Ordnungswidrigkeiten hat (vgl. insoweit OVG Lüneburg, Beschluss vom 23.09.2013, Az.: 13 LA 144/12, zitiert nach juris). Der Anzeigeerstatter kann sich die Entscheidung zur Verfolgungsintensität nicht in rechtlich billigenswerter Weise zu Eigen machen, dies auch mit Blick auf das staatliche Gewaltmonopol. Aus diesen Überlegungen folgt, dass es nicht die Sache des Beklagten ist, sich darüber zu sorgen, ob es im Zuge seiner Anzeigen zu Beweisproblemen kommt, die mittels Fotografien zu beseitigen wären. Generell hat das Oberverwal-

tungsgericht Lüneburg (a.a.O) zu „selbsternannten Hilfsermittlern“ ausgeführt, dass diese bei massenhaften Anzeigen von Verstößen (dort: Parkverstößen) kein eigenes schützenswertes Interesse haben, weil sich solche Personen lediglich zum Sachwalter öffentlicher Interessen machen. Dies hat der Beklagte selbst in seinem Schreiben vom 08.12.2014 ausdrücklich vorgetragen, soweit er dort angibt, im Zuge des Fotografierens von mutmaßlichen Ordnungswidrigkeiten in der Siegaue keine Eigeninteressen zu verfolgen.

Selbst wenn der Beklagte – entgegen vorstehender Ausführungen – für sich hier ein „Recht auf eine Anzeige“ ins Feld führen könnte, so müsste er jedenfalls auch die Wertung gelten lassen, die bezüglich Strafanzeigen nach § 158 Abs. 1 StPO gelten. Danach hat nämlich der Anzeigende im Zuge der Anzeigeerstattung das Allgemeine Persönlichkeitsrecht anderer zu achten (Karlsruher Kommentar zur Strafprozessordnung-Griesbaum, § 158 Rn. 4).

Mangels anderweitiger betroffener Individualrechtsgüter des Beklagten kann dieser sich lediglich auf die allgemeine Handlungsfreiheit gemäß Art. 2 Abs. 1 GG stützen. Und auch diese Rechtsposition ist hier nur schwach ausgeprägt mit Blick auf obige Ausführungen, wonach der Beklagte als Sachwalter öffentlicher Interessen an sich gar keine Eigeninteressen wahrnimmt.

Vor dem Hintergrund, dass sich der Beklagte nicht auf die Verfolgung von Ordnungswidrigkeiten und den Naturschutz berufen kann, kann dahinstehen, ob das Anfertigen der Fotografien zu diesen seitens des Beklagten verfolgten Zwecken geeignet und erforderlich ist.

Schließlich fehlt es an der Angemessenheit der streitgegenständlichen Fotografien. Das Allgemeine Persönlichkeitsrecht des Klägers in Gestalt des Rechts am eigenen Bild ist in der Sozialsphäre des Klägers recht deutlich betroffen, denn er wird ohne sein Wissen mehrfach bei einem Spaziergang und an seinem Auto gezielt fotografiert, ohne sich diesem – mangels Wissen – entziehen zu können. Die allgemeine Handlungsfreiheit des Beklagten, die aus genannten Gründen ohnedies hier stark eingeschränkt zu Tage tritt, hat in diesem Zusammenhang zurückzutreten. Daran ändert auch die Überlegung nichts, dass die Verwaltungsbehörde dieselben Beweismittel nach Vorschriften der Strafprozessordnung hätte anfertigen können. Denn diese Vorschriften ermächtigen gerade nur den Staat und nicht etwa den einzelnen Bürger. Dies ist ein maßgebliches Kennzeichen des staatlichen Gewaltmonopols.

Der Einwand des Beklagten mit Blick auf die Wiederholungsgefahr, es sei nicht zu erwarten, dass der Kläger weitere Ordnungswidrigkeiten in der Siegaue begehe, so dass auch keine weiteren Fotografien zu erwarten seien, verfängt nicht. Denn zum einen würde danach das zukünftige Vorliegen einer Wiederholungsgefahr wiederum von der Einschätzung des Beklagten abhängen, ob der Kläger gerade eine (ahndungswürdige) Ordnungswidrigkeit begeht. Bereits diese Einschätzung ist nach vorigen Ausführungen nicht seine Sache, sondern Sache der Ordnungsbehörde. Zum anderen hat der Beklagte klar erklärt, dass er seine Vorgehensweise nicht ändern wolle. Auch wenn der Kläger möglicherweise nicht regelmäßig das fragliche Naturschutzgebiet zum Spazierengehen (mit dem Hund) nutzt, so kann zwanglos davon ausgegangen werden, dass dies auch jederzeit wieder in Zukunft vorkommen kann. Im Ergebnis besteht damit eine hinreichende Wahrscheinlichkeit, dass der Kläger bei solchen Anlässen erneut von dem Beklagten fotografiert wird, wenn dieser meint, der Kläger beginge eine Ordnungswidrigkeit.

Fristversäumnis bei kurz vor Fristablauf erfolgtem Faxversand (Ls)

(**Landesarbeitsgericht Berlin-Brandenburg**, Beschluss vom 31. März 2015 – 15 Sa 11/15 –)

Ein vergeblicher Faxversuch um zehn Minuten vor zwölf ist jedenfalls dann nicht entschuldbar, wenn es zuvor schon zu zeitlichen Unregelmäßigkeiten bei der Faxversendung mittels Voice over IP (VoIP) kam.

Ausschluss eines Mitglieds aus dem Betriebsrat wegen Verstoß gegen Geheimhaltungspflicht (Ls)

(**Landesarbeitsgericht Düsseldorf**, Beschluss vom 23. Januar 2015 – 6 TaBV 48/14 –)

1. **Einem Antrag auf den Ausschluss eines Mitglieds aus dem Betriebsrat fehlt nicht deshalb das Rechtsschutzinteresse, weil er auf eine Pflichtverletzung aus einer vorangegangenen Amtsperiode gestützt wird. Ob der Antrag gemäß § 23 Abs.1 S.1 BetrVG auf eine frühere Pflichtverletzung gestützt werden kann, ist allein eine Frage der Begründetheit.**

2. **Wenn eine unmittelbar vor der Neuwahl des Betriebsrats begangene Pflichtverletzung konkrete Auswirkungen auf die vertrauensvolle Zusammenarbeit zwischen dem neugewählten Betriebsrat und dem Arbeitgeber hat, kann diese Pflichtverletzung zum Ausschluss aus dem Betriebsrat in der folgenden Amtsperiode führen. Dies ist jedenfalls möglich, wenn ein Betriebsratsmitglied nicht nur ein vom Arbeitgeber als geheimhaltungsbedürftig bezeichnetes Betriebs- oder Geschäftsgeheimnis öffentlich macht, sondern zugleich zum Ausdruck bringt, dies auch zukünftig so handhaben zu wollen.**

Initiativrecht des Betriebsrats im Bereich des § 87 Abs. 1 Nr. 6 BetrVG

(**Landesarbeitsgericht Berlin-Brandenburg**, Beschluss vom 22. Januar 2015 – 10 TaBV 1812/14 –)

Der Betriebsrat hat auch im Bereich des § 87 Abs. 1 Nr. 6 BetrVG ein Initiativrecht. Ob es im Einzelfall gerechtfertigt ist, in das Persönlichkeitsrecht der Arbeitnehmer einzugreifen, ist bei der Ausübung der Mitbestimmung zu beurteilen.

Sachverhalt:

Die Beteiligten streiten über die Einsetzung einer Einigungsstelle im Zusammenhang mit der elektronischen Zeiterfassung.

Bislang wird im Betrieb das elektronische System Personaleinsatzplanung (PEP) eingesetzt. Dieses wird zur Dienstplanung/Personalein-

satzplanung sowie zur Dienstplanabrechnung genutzt. Dabei ist bei einer Abweichung der Ist-Arbeitszeit von der in PEP enthaltenen Soll-Arbeitszeit ein Korrekturbogen manuell auszufüllen und von einer Zeitkorrekturbeauftragten in der PEP-Datenbank zu erfassen.

Spätestens seit Dezember 2011 wurde in der Unternehmensgruppe, der die Arbeitgeberin angehört, geplant, die elektronische Zeiterfassung von PEP auf eine sogenannte positive Zeitwirtschaft (PZW) umzustellen. Mit diesem System sollte die Ist-Arbeitszeit mittels Chipkarte an Terminals jeweils elektronisch erfasst und elektronisch an das PEP-System übermittelt werden. Entsprechendes plante die Arbeitgeberin im hiesigen Betrieb. Zur Einführung sollte eine Muster-Betriebsvereinbarung PZW eines Gesamtbetriebsrates aus der Unternehmensgruppe herangezogen werden. Mit diesem Regelungs-Muster war der hiesige Betriebsrat weitgehend einverstanden. Die Betriebsparteien konnten jedoch keine Einigung über die Standorte der Erfassungsterminals erzielen. Der Betriebsrat teilte mit Schreiben vom 15. Februar 2012 an den Geschäftsbereich Arbeitsrecht mit, dass sie sich mit dem Hausleiter und dem Vertriebsleiter bislang nicht über die Standorte der Terminals hätten einigen können.

Die Arbeitgeberin teilte sodann mit Schreiben vom 22. März 2012 an den Betriebsrat mit, dass sie sich aufgrund des derzeitigen Verhandlungsstandes im Hinblick auf die Aufstellungsorte für die Zeiterfassungsterminals dazu entschieden habe, von einer Einführung der PZW im hiesigen Betrieb Abstand zu nehmen.

Nach weiterem Schriftverkehr im Juli und August 2012 und sachverständiger Prüfung für den Betriebsrat forderte der Betriebsrat die Arbeitgeberin mit Schreiben vom 23. November 2012 erneut zur Fortsetzung der Verhandlungen auf. Unter dem 8. Oktober 2013 beschloss der Betriebsrat, die hiesigen Verfahrensbevollmächtigten, das Mitbestimmungsrecht aus § 87 Abs. 1 Nr. 6 BetrVG im Hinblick auf die Verhandlung einer Betriebsvereinbarung „Positive Zeitwirtschaft" (BV PZW) sowohl außergerichtlich als auch gerichtlich gegenüber der Arbeitgeberin durchzusetzen.

Im Rahmen weiteren Schriftverkehrs lehnte die Arbeitgeberin unter dem 1. November 2013 unter Hinweis auf den Beschluss des Bundesarbeitsgerichts vom 28. November 1989 – 1 ABR 97/88 und das dort postulierte fehlende Initiativrecht des Betriebsrates bei der Mitbestimmung nach § 87 Abs. 1 Nr. 6 BetrVG weitere Gespräche und Verhandlungen ab.

Aus den Gründen:

3. Eine Einigungsstelle im Sinne des § 76 BetrVG kann gemäß § 99 Abs. 1 ArbGG durch das Arbeitsgericht nur eingerichtet werden, wenn sie im Sinne des § 99 Abs. 1 Satz 2 ArbGG nicht offensichtlich unzuständig ist. Offensichtlich unzuständig ist eine Einigungsstelle nur dann, wenn bei fachkundiger Beurteilung durch das Gericht sofort erkennbar ist, dass ein Mitbestimmungsrecht des Betriebsrates in der fraglichen Angelegenheit unter keinem rechtlichen Gesichtspunkt in Frage kommt, sich also die Streitigkeit zwischen Arbeitgeber und Betriebsrat erkennbar nicht unter einem mitbestimmungspflichtigen Tatbestand subsumieren lässt (vgl. nur LAG Hamm, Beschluss vom 16. Dezember 2014, 7 TaBV 73/14; LAG Düsseldorf, Beschluss vom 25. August 2014 – 9 TaBV 39/14; LAG Berlin-Brandenburg, Beschluss vom 9. April 2014 – 4 TaBV 638/14; LAG Hamburg, Beschluss vom 26. März 2014 – 5 TaBV 3/14; LAG Köln, Beschluss vom 19. Februar 2014 – 11 TaBV 90/13 jeweils mit weiteren Nachweisen zur Rechtsprechung und Literatur). Die Frage der offensichtlichen Unzuständigkeit entbindet nach alledem das Gericht im Verfahren nach § 99 ArbGG nicht davon, überhaupt einen mitbestimmungspflichtigen Tatbestand festzustellen.

3.1 Nach § 87 Abs. 1 Nr. 6 BetrVG hat der Betriebsrat ein Mitbestimmungsrecht bei der Einführung und Anwendung von technischen Einrichtungen, die dazu geeignet sind, Leistung und/oder Verhalten von Arbeitnehmern zu überwachen. Zu diesen technischen Einrichtungen zählt auch ein Zeiterfassungssystem. Denn in einem Zeiterfassungssystem werden typischerweise zumindest die Komm- und Gehzeiten von Arbeitnehmern sowie vielfach auch die Pausenzeiten technisch erhoben und verarbeitet. Dass die positive Zeitwirtschaft ein solches zur Überwachung geeignetes System ist, ist zwischen den Beteiligten auch nicht streitig. Streitig ist allerdings, ob der Betriebsrat ein Initiativrecht zur Einführung oder Intensivierung der Überwachung von Arbeitnehmern hat.

3.2 Der Gesetzgeber hat bei der Einführung des § 87 BetrVG im Jahre 1972 ganz bewusst nicht zwischen Mitbestimmungsrechten mit Initiativrecht des Betriebsrates und solchen ohne Initiativrecht des Betriebsrates unterschieden. Der „Entwurf eines Gesetzes über die Mitbestimmung der Arbeitnehmer in Betrieb und Unternehmen" der Bundestagsfraktion der CDU/CSU (BT-Drs. VI/1806) beinhaltete im § 29 Abs. 1 unter der Überschrift „Mitbestimmungsrecht" einerseits die Regelung

„Folgende Angelegenheiten können vom Arbeitgeber und Betriebsrat nur gemeinsam geregelt werden"

und andererseits im § 30 unter der Überschrift „Zustimmungsrecht" die Regelung

„Folgende Angelegenheiten können vom Arbeitgeber nur mit vorheriger Zustimmung des Betriebsrats durchgeführt werden".

Im Falle des § 29 beinhaltete Abs. 2

„Ist eine Übereinstimmung über die vorstehenden Angelegenheiten nicht zu erzielen, so entscheidet die Einigungsstelle verbindlich",

Im Falle des § 30 demgegenüber beinhaltete der dortige Abs. 2

„Ist eine Verständigung nicht zu erzielen, so kann der Arbeitgeber bei der Einigungsstelle die verbindliche Entscheidung über die Ersetzung der Zustimmung des Betriebsrats beantragen".

Nach dem Schriftlichen Bericht des Ausschusses für Arbeits- und Sozialordnung (vgl. zu BT-Drs. VI/2729) wurde dieser Vorschlag nach Beratung im Ausschuss abgelehnt und nicht weiter verfolgt.

Der Ausschuss für Arbeit und Sozialordnung war in seiner Gesamtheit der Ansicht, dass die Beteiligung des Betriebsrates in sozialen Angelegenheiten gegenüber dem geltenden Recht auszuweiten sei. Allerdings sprach sich die Mehrheit gegen die im CDU/CSU-Entwurf vorgesehene Aufteilung der sozialen Angelegenheiten aus, die zwischen solchen, in denen der Betriebsrat ein echtes Mitbestimmungsrecht, d.h. auch ein eigenes Initiativrecht hat, und solchen, die ausschließlich von der Initiative des Arbeitgebers abhängen und lediglich der Zustimmung des Betriebsrates bedürfen, unterscheidet. Die Mehrheit des Ausschusses erkannte an, dass nach der CDU/CSU-Vorlage der Kreis der beteiligungsbedürftigen Angelegenheiten ebenfalls erweitert werden sollte. Sie sah jedoch in dieser Aufspaltung eine sachlich nicht gebotene Einschränkung des Mitbestimmungsrechts des Betriebsrates (zu BT-Drs. VI/2729, S. 4).

3.3 Dennoch hatte das Bundesarbeitsgericht mit einer vereinzelten Entscheidung vom 28. November 1989 – 1 ABR 97/88 – entschieden, dass § 87 Abs. 1 Nr. 6 BetrVG den Betriebsrat nicht berechtige, die Einführung einer technischen Kontrolleinrichtung zu verlangen und gegebenenfalls über den Spruch einer Einigungsstelle zu erzwingen. Dieser Satz jener Entscheidung, den das Bun-

desarbeitsgericht zu keinem Zeitpunkt so wiederholt hat, hat seither die meisten Instanzgerichte veranlasst, ein Initiativrecht des Betriebsrates zur Einführung einer technischen Kontrolleinrichtung abzulehnen und dieses sogar als offensichtlich nicht bestehend anzunehmen. Die Voraussetzungen für eine solche richterliche Rechtsfortbildung sind jedoch nicht gegeben (vgl. zur richterlichen Rechtsfortbildung allgemein LArbG Berlin-Brandenburg, Beschluss vom 5. Juni 2014 – 10 TaBVGa 146/14).

Richterliche Rechtsfortbildung darf nicht dazu führen, dass ein Gericht seine eigene materielle Gerechtigkeitsvorstellung an die Stelle derjenigen des Gesetzgebers setzt (BAG, Urteil vom 10. Dezember 2013 – 9 AZR 51/13). Nach Art. 20 Abs. 2 Satz 2 GG wird die Staatsgewalt vom Volke in Wahlen und Abstimmungen und durch besondere Organe der Gesetzgebung, der vollziehenden Gewalt und der Rechtsprechung ausgeübt. Die Aufgabe der Rechtsprechung beschränkt sich darauf, den vom Gesetzgeber festgelegten Sinn und Zweck eines Gesetzes auch unter gewandelten Bedingungen möglichst zuverlässig zur Geltung zu bringen oder eine planwidrige Regelungslücke mit den anerkannten Auslegungsmethoden zu füllen. Eine Interpretation, die als richterliche Rechtsfortbildung den Wortlaut des Gesetzes hintanstellt und sich über den klar erkennbaren Willen des Gesetzgebers hinwegsetzt, greift unzulässig in die Kompetenzen des demokratisch legitimierten Gesetzgebers ein (BVerfG, Urteile vom 11. Juli 2012 – 1 BvR 3142/07, 1 BvR 1569/08).

3.4 Bereits in der Entscheidung vom 28. November 1989 hatte das Bundesarbeitsgericht selbst erste Zweifel an der zuvor geäußerten Rechtsauffassung formuliert. Denn dort wurde zugleich angemerkt:

> *„Ob ein aus anderen Gründen gegebenes Interesse des Betriebsrats an der Einführung einer technischen Kontrolleinrichtung auch ein entsprechendes Initiativrecht des Betriebsrats begründet, kann sich allenfalls aus anderen Vorschriften des Betriebsverfassungsgesetzes, nicht aber aus § 87 Abs. 1 Nr. 6 BetrVG ergeben."*

In jenem Verfahren meinte der Betriebsrat, dass er die technische Zeiterfassung im Zusammenhang mit seinem Mitbestimmungsrecht aus § 87 Abs. 1 Nr. 1 und Nr. 10 BetrVG benötige, da die maschinelle Arbeitszeiterfassung eine Frage der betrieblichen Ordnung sei und darüber hinaus der Lohngestaltung diene. Die Arbeitnehmer würden in erheblichem Umfange Überstunden leisten, deren leistungsgerechte Vergütung der Arbeitgeber ablehne. Nur eine maschinelle Arbeitszeiterfassung setze ihn, den Betriebsrat, in die Lage, auf die Einhaltung der Arbeitszeit und der Arbeitszeitvorschriften hinzuwirken und darüber zu wachen, dass geleistete Überstunden vergütet würden. Dieses hielt das Bundesarbeitsgericht zur Begründung eines Initiativrechtes nicht für ausreichend, da der Arbeitgeber dem Betriebsrat nur diejenigen Unterlagen zur Verfügung zu stellen habe, die er selbst besitze. Der Betriebsrat könne nicht verlangen, dass der Arbeitgeber nur für ihn Unterlagen erstelle und zu deren Erstellung erforderliche Einrichtungen anschaffe.

Diese Rechtsprechung hat das Bundesarbeitsgericht bereits mit dem Beschluss vom 6. Mai 2003 im Verfahren 1 ABR 13/02 geändert. Eine Pflicht des Arbeitgebers zur Erteilung solcher Auskünfte zur Arbeitszeit bestehe auch dann, wenn der Arbeitgeber über die entsprechenden Kenntnisse selbst bislang nicht verfüge. Die gegenteilige Auffassung überzeuge nicht.

Daten zur Arbeitszeit der Arbeitnehmer, über die der Betriebsrat Auskunft begehre und deren Kenntnis er zur Wahrnehmung seiner Überwachungsaufgabe benötige, würden im Betrieb ohne weiteres und ständig anfallen. Der Arbeitgeber, der über die tatsächlichen Arbeitszeiten seiner Mitarbeiter Auskunft geben solle, müsse sich diese Daten nicht etwa von dritter Seite erst beschaffen. Er müsse lediglich auf geeignete Weise dafür sorgen, dass die objektiv vorhandenen Daten im Betrieb zur Kenntnis genommen und mitteilbar gemacht würden. Anders als im Fall nicht existierender Unterlagen brauche er dazu nichts herzustellen, sondern nur etwas Gegebenes wahrzunehmen.

Zu einer solchen Wahrnehmung der anfallenden Daten sei der Arbeitgeber schon unabhängig von der Überwachungsaufgabe des Betriebsrats verpflichtet. Darauf, ob er die Daten erheben wolle, komme es nicht an. Ein Verzicht auf die Erhebung von Arbeitszeitdaten der Arbeitnehmer sei keine zu respektierende Ausübung der betrieblichen Organisations- und Leitungsmacht des Arbeitgebers (BAG, Beschluss vom 06. Mai 2003 – 1 ABR 13/02).

3.5 Sicherlich ist der Grundansatz des Bundesarbeitsgerichts in der Entscheidung vom 28. November 1989 zutreffend, dass der Betriebsrat in der Regel einen Eingriff in das Persönlichkeitsrecht der Arbeitnehmer eher verhindern als ermöglichen will, aber es ist nicht von vornherein ausgeschlossen, dass es andere schützenswerte Rechte gibt, die den Persönlichkeitsschutz überwiegen (vgl. Gola/Wronka Handbuch Arbeitnehmerschutz, 6. Aufl. 2013, RN 1891; Beispiele dazu finden sich auch schon bei Schwarz, Arbeitnehmerüberwachung und Mitbestimmung, 1982 S. 37 f.). Deshalb gibt es neben dem Willen des Gesetzgebers auch ansonsten keinen Grund, den Betriebsrat von jeder Initiative zur einschlägigen technischen Ausrüstung auszuschließen. Soweit sich aus den Resultaten solcher Initiativen Unvereinbarkeiten mit geschützten Persönlichkeitsrechten betroffener Arbeitnehmer ergeben sollten, erfolgt die Abgrenzung nicht beim Initiativrecht, sondern durch die „Binnenschranken der Betriebsautonomie", also hier durch die Ermessensausübung der Einigungsstelle (vgl. ArbG Berlin, Beschluss vom 20. März 2013 – 28 BV 2178/13 m.w.N.).

Damit kann sich allein aus dem vom Betriebsrat geltend gemachten Regelungsgegenstand keine offensichtliche Unzuständigkeit der Einigungsstelle ergeben. Der Betriebsrat hat auch im Rahmen des § 87 Abs. 1 Nr. 6 BetrVG ein Initiativrecht (so auch Fitting, Betriebsverfassungsgesetz 27. Aufl. § 87 RN 251; HaKo-BetrVG/Kohte, 4. Aufl. § 87 RN 20; Däubler/Kittner/Klebe/Wedde BetrVG 13. Aufl. § 87 RN 166; Däubler, Gläserne Belegschaften 6. Aufl. § 14 RN 815). Ob es hinreichende Gründe gibt, mit einer Betriebsvereinbarung zur positiven Zeitwirtschaft das Persönlichkeitsrecht der Arbeitnehmer im Betrieb zu berühren, muss die Einigungsstelle im Rahmen des von ihr nach § 76 Abs. 5 Satz 3 BetrVG auszuübenden Ermessens im Lichte des § 75 Abs. 2 BetrVG selbst entscheiden.

Beleidigung des Chefs in vertraulicher SMS an Kollegen

(**Landesarbeitsgericht Rheinland-Pfalz**, Urteil vom 22. Januar 2015 – 3 Sa 571/14 –)

Beleidigende Äußerungen über Vorgesetzte innerhalb vertraulichen Kollegenkontakts rechtfertigen regelmäßig keine Kündigung. Regelmäßig darf der Arbeitnehmer auf die Vertraulichkeit des Gesprächs vertrauen.

(Nicht amtlicher Leitsatz)

Sachverhalt:

Die Parteien des vorliegenden Rechtsstreits streiten darüber, ob das zwischen ihnen bestehende Arbeitsverhältnis aufgrund einer ordentlichen Arbeitgeberkündigung sein Ende gefunden hat.

Der Kläger ist bei der Beklagten seit dem 01.05.2010 als Oberarzt beschäftigt. In den letzten Jahren war er bei der Beklagten ausschließlich als Herzchirurg eingesetzt.

Am 19.05.2014 erklärte er sich in einer Teambesprechung angesichts eines bei der Beklagten bestehenden Personalengpasses bereit, die medizinisch-technische Operationsassistentin Frau N. zu fragen, ob sie bereit sei, Rufbereitschaft zu leisten. Auf die Anfrage antwortete Frau N. wie folgt:

N. (16.28 Uhr): „Hallo, es ist schon alles mit dem Chef besprochen"

Kläger (16.56 Uhr): „Dann ist ja gut. Heute morgen hat er nichts davon gesagt. Er ist u bleibt ein autistisches krankes Arschl… l G m"

Nachdem Frau N. daraufhin den besagten „Chef", den Chefarzt Prof. Dr. N., über diesen Vorgang in Kenntnis gesetzt hatte, kündigte die Beklagte das Arbeitsverhältnis mit Schreiben vom 18.06.2014 ordentlich zum 30.09.2014.

Hierzu hat der Kläger u.a. vorgetragen:

Zum einen fehle es an einer Abmahnung. Zum anderen habe er darauf vertrauen dürfen, dass Frau N. seine Äußerung nicht an Prof. Dr. N. bzw. an die Beklagte weiterleiten werde, zumal Frau N. – mit der der Kläger von 2010 bis Herbst 2012 eine eheähnliche Beziehung geführt habe – ihm noch im Frühjahr 2014 angesichts von Meinungsverschiedenheiten in der Abteilung erklärt habe, sie werde nichts tun, um ihm zu schaden. Im Übrigen habe die Beklagte ihm eine Weiterbeschäftigung auf einem anderen Arbeitsplatz anbieten müssen, da er auch als „normaler" Chirurg in einer anderen Abteilung arbeiten könne. Negative Auswirkungen auf die Patienten der Herzchirurgie stünden nicht zu befürchten, da er mit Prof. Dr. N. ohnehin nur ein- bis zweimal pro Monat gemeinsam operiere.

Aus den Gründen:

Das Arbeitsgericht ist sowohl im Ergebnis als auch in der Begründung zu Recht davon ausgegangen, dass die streitgegenständliche ordentliche Kündigung das zwischen den Parteien bestehende Arbeitsverhältnis nicht beendet hat mit der Folge, dass dem Kläger ein Anspruch auf ein qualifiziertes wohlwollendes Zwischenzeugnis zusteht und er seine einstweilige Weiterbeschäftigung bis zum rechtskräftigen Abschluss dieses Verfahrens verlangen kann.

Mit dem Arbeitsgericht ist zunächst davon auszugehen, dass vorliegend die Voraussetzungen für die soziale Rechtfertigung einer ordentlichen verhaltensbedingten Kündigung gemäß § 1 Abs. 1 Satz 2 KSchG nicht gegeben sind.

…

Beleidigt ein Arbeitnehmer seinen Arbeitgeber, seinen Vertreter und Repräsentanten, einen Vorgesetzten oder seine Arbeitskollegen grob, d.h. wenn die Beleidigungen nach Form und Inhalt eine erhebliche Ehrverletzung für den Betroffenen bedeutet, stellt dies einen erheblichen Verstoß gegen seine vertragliche Pflicht zur Rücksichtnahme gem. § 241 BGB aus dem Arbeitsverhältnis dar und kann folglich ebenso einen wichtigen Grund für eine außerordentliche Kündigung an sich bilden, wie auch einen solchen für eine ordentliche verhaltensbedingte Kündigung (vgl. BAG 27.09.2012 – 2 AZR 646/11, EzA-SD 9/2013 S. 6 Leitsatz; 17.07.2011 EzA § 626 BGB 2002 Nr. 38; 10.12.2009 EzA § 626 BGB 2002 Nr. 29; 10.10.2002 EzA § 626 BGB 2002 Unkündbarkeit Nr. 1, 06.11.2003 EzA § 1 KSchG Verhaltensbedingte Kündigung Nr. 60; LAG R.-P. 18.08.2011 NZA RR 2012, 16; vgl. Dörner/Luczak/Wildschütz/Baeck/Hoß, Handbuch des Fachanwalts Arbeitsrecht, 12. Aufl., 2015, Kapitel 4 Rn. 1313 ff. = S. 1658 ff.).

Bei der rechtlichen Würdigung sind allerdings die Umstände zu berücksichtigen, unter denen die betreffenden Äußerungen gefallen sind. Geschah dies im Rahmen einer emotional geprägten Auseinandersetzung, vermögen sie eine Kündigung des Arbeitsverhältnisses nicht ohne weiteres zu begründen (LAG R.-P. 18.08.2011 a.a.O.). Hat der Arbeitgeber Beleidigungen ausgesprochen, so kann auch eine Reaktion des Arbeitnehmers zulässig und nicht zu beanstanden sein; auch in einer zugespitzten innerbetrieblichen Situation ist es dem Arbeitnehmer erlaubt, für den eigenen Sachstandpunkt mit scharfer Polemik zu werben, soweit dabei nicht andere Personen beleidigt oder in vergleichbar schwerer Weise unsachlich angegriffen werden (LAG Mecklenburg-Vorpommern 14.08.2012 NZA-RR 2013, 20).

Die Grenze zwischen einer lediglich überspitzten und polemischen Kritik und einer nicht mehr vom Grundrecht auf freie Meinungsäußerung gem. Art. 5 Abs. 1 GG gedeckten Schmähung ist dann überschritten, wenn bei der Äußerung nicht mehr die Auseinandersetzung in der Sache, sondern die Diffamierung der Person im Vordergrund steht (BAG 07.07.2011, EzA § 626 BGB 2002 Nr. 38).

Vorliegend ist mit dem Arbeitsgericht davon auszugehen, dass mit der Formulierung „autistisches krankes Arschl…" eine grobe Beleidigung gegeben ist, ohne dass dies weiter erörtert werden müsste.

Allerdings sind bei der rechtlichen Beurteilung in der Wirksamkeit einer darauf gestützten Kündigung die Umstände zu berücksichtigen, unter denen die diffamierende und/oder ehrverletzende Äußerung gefallen ist.

Nach Maßgabe der besonderen Umstände des hier zu entscheidenden Einzelfalles dürfe der Kläger darauf vertrauen, dass Frau N. als Adressatin der SMS diese nicht an Prof. Dr. N. bzw. den Beklagten weiterleiten würde.

Werden diffamierende und ehrverletzende Äußerungen über Vorgesetzte oder Kollegen nur in vertraulichen Gesprächen unter Arbeitskollegen abgegeben, so kann unter Umständen die außerordentliche Kündigung des Arbeitsverhältnisses ebenso wie die ordentliche Kündigung nicht gerechtfertigt sein. Denn vertrauliche Äußerungen unterfallen dem Schutzbereich des allgemeinen Persönlichkeitsrechts. Die vertrauliche Kommunikation in der Privatsphäre ist Ausdruck der Persönlichkeit und grundrechtlich gewährleistet (BAG 10.12.2009 EzA § 626 BGB 2002 Nr. 29). Der Arbeitnehmer darf regelmäßig darauf vertrauen, seine Äußerungen werden nicht nach außen getragen und der Betriebsfrieden nicht gestört bzw. das Vertrauensverhältnis nicht zerstört. Hebt der Gesprächspartner später die Vertraulichkeit auf, geht dies rechtlich nicht zu Lasten des Arbeitnehmers (BAG 10.12.2009 a.a.O.). Diesen Schutz der Privatsphäre und der Meinungsfreiheit kann der Arbeitnehmer lediglich dann nicht in Anspruch nehmen, der selbst die Vertraulichkeit aufhebt, so dass die Gelegenheit für Dritte, seine Äußerung zur Kenntnis zu nehmen, ihm zurechenbar wird. Das gilt beispielsweise in dem Fall, in dem er eine Mitteilung an eine – vermeintliche – Vertrauensperson richtet, um einen Dritten „zu treffen" (BAG 10.10.2002 EzA § 626 BGB 2002 Unkündbarkeit Nr. 1; 10.12.2009 EzA § 626 BGB 2002 Nr. 29; vgl. Dörner/Luczak/Wildschütz/Baeck/Hoß, a.a.O., Kap. 4 Nr. 1328 = S. 1662 f.).

Insoweit ist das Arbeitsgericht zutreffend davon ausgegangen, dass dem ein entsprechender „Erfahrungssatz" des Inhalts zugrunde liegt, „dass anfechtbare Äußerungen über Vorgesetzte, sofern sie im Kollegenkreis folgen, in der sicheren Erwartung geschehen, dass sie nicht über den Kreis der Gesprächsteilnehmer hinaus

dringen werden" (BAG 21.10.1965 AP Nr. 5 zu § 1 KSchG Verhaltensbedingte Kündigung; 30.11.1972 AP Nr. 66 zu § 626 BGB; 10.12.2009 a.a.O.). Diesen Grundsätzen folgt auch das Landesarbeitsgericht Rheinland-Pfalz (LAG R.-P. 19.02.2004 – 6 Sa 1120/03; 08.09.2009 NZA RR 2010, 212; 24.07.2014 – 5 Sa 25/14). Vor diesem Hintergrund gehört es zu den vom Arbeitgeber nach den zuvor dargestellten Grundsätzen darzulegende Kündigungstatsachen, dass Umstände vorliegen, die eine mögliche Rechtfertigung des Verhaltens des Arbeitnehmers gleichwohl ausschließen (BAG 10.12.2009, a.a.O.).

Vorliegend hat das Arbeitsgericht insoweit aber zutreffend angenommen, dass der Kläger darauf vertrauen durfte, dass Frau N. den Inhalt seiner SMS nicht an Prof. Dr. N. oder die Beklagte weiterleiten würde. Dies hat das Arbeitsgericht ausführlich und in jeder Hinsicht zutreffend begründet; deshalb wird zur Vermeidung von Wiederholungen auf S. 8–10 der angefochtenen Entscheidung (= Bl. 69–71 d. A.) Bezug genommen.

Folglich ist dem Kläger aufgrund der Besonderheit des hier zu beurteilenden Einzelfalles keine Pflichtverletzung anzulasten. Eine durch die Weiterleitung der negativen Äußerung eingetretene Störung des Vertrauensverhältnisses oder des Betriebsfriedens ist hier nicht durch die Herabsetzung des Vorgesetzten an sich eingetreten, sondern erst dadurch, dass der Gesprächspartner die Vertraulichkeit missachtet und sich in einer für den Arbeitnehmer unerwarteten Weise indiskret verhalten hat.

Würde man insoweit eine andere Auffassung vertreten, hätte es vorliegend nach dem Grundsatz der Verhältnismäßigkeit jedenfalls einer vorherigen – nicht gegebenen Abmahnung – bedurft.

…

Mitbestimmung bei Einrichtung einer Facebook-Seite des Arbeitgebers (Ls)

(**Landesarbeitsgericht Düsseldorf**, Beschluss vom 12. Januar 2015 – 9 TaBV 51/14 –)

1. **Für einen Antrag gerichtet auf die Unterlassung des Betriebes einer Facebook-Seite des Arbeitgebers ist der Konzernbetriebsrat nach § 58 Abs. 1 BetrVG zuständig. Der Konzernbetriebsrat ist originär zuständig, wenn die Angelegenheit den Konzern oder mehrere Konzernunternehmen betrifft und das Regelungsziel nur durch eine einheitliche Regelung auf Konzernebene erreicht werden kann. Ein entsprechendes zwingendes Erfordernis für die konzerneinheitliche Regelung kann sich aus technischen oder rechtlichen Gründen ergeben. Auf dieser Grundlage besteht bei dem Betrieb einer unternehmenseinheitlichen facebook-Seite durch den Arbeitgeber schon technisch ein zwingendes Erfordernis für eine unternehmenseinheitliche Regelung.**

2. **Der Mitbestimmungstatbestand nach § 87 Abs. 1 Nr. 6 BetrVG ist nicht verletzt. Auch wenn der Arbeitgeber mit Suchmaschinen nach Kommentaren Mitarbeiter betreffend suchen kann, fehlt es an einer Aufzeichnung durch eine technische Einrichtung. Denn die Überwachung muss durch die technische Einrichtung selbst bewirkt werden. Dazu muss diese aufgrund ihrer technischen Natur unmittelbar, d.h. wenigstens in ihrem Kern die Überwachung vornehmen, indem sie das Verhalten oder die Leistung der Arbeitnehmer kontrolliert. Allein dass Mitarbeiter auf der Facebook-Seite von Dritten negativ bewertet werden und dass der Arbeitgeber mit den Facebook-eigenen Möglichkeiten gezielt nach negativen Einträgen suchen könnte, führt nicht dazu, dass er eine technische Einrichtung betreibt.**

3. **Nichts anderes ergibt sich aus den von Facebook angebotenen statistischen Auswertungen. Denn diese betreffen nicht die Mitarbeiter. Es geht bei der Funktionalität „Messungen und Statistiken" um die Auswertung der Kundenbelange. Auch hinsichtlich der Administratoren liegt kein Tatbestand des § 87 Abs. 1 Nr. 6 BetrVG vor. Denn der Arbeitgeber hat eine globale „Administratoren-Kennung" vergeben, die von allen Personen genutzt werden kann, die mit der Pflege der Seite beauftragt sind.**

Kontoauszüge in Leistungsakten des Jobcenters

(**Landessozialgericht Berlin-Brandenburg**, Beschluss vom 10. März 2015 – L 31 AS 2974/14 –)

1. **Die Aufbewahrung von Kontoauszügen in Leistungsakten des Jobcenters ist eine rechtmäßige Datenspeicherung.**

2. **Handlungsempfehlung des Landesbeauftragten für den Datenschutz entbehren der Verbindlichkeit für die Behörde und begründen damit keine rechtliche Handhabe zur Durchsetzung.**

(Nicht amtliche Leitsätze)

Aus den Gründen:

Das Urteil des Sozialgerichts Cottbus vom 13. Oktober 2014 sowie der Bescheid des Beklagten vom 24. Oktober 2013 in der Gestalt des Widerspruchsbescheides vom 28. November 2013 sind rechtmäßig und verletzen den Kläger nicht in seinen Rechten. Das Sozialgericht Cottbus hat es zu Recht abgelehnt, die angefochtenen Bescheide aufzuheben. Die grundsätzliche Weigerung des Beklagten, Kontoauszüge aus den Verwaltungsakten zu entfernen, ist rechtens.

Der Kläger hat keinen Anspruch auf Entfernung sämtlicher Kontoauszüge aus der Verwaltungsakte. Bei der Aufbewahrung der Kontoauszüge im Original oder in Kopie in der Verwaltungsakte handelt es sich um eine rechtmäßige Speicherung von Daten nach § 67 c SGB X. Dies hat auch das Bayerische Landessozialgericht (LSG) mit Beschluss vom 21. Mai 2014 – Az. L 7 AS 347/14 B ER – so ausgeführt. Danach sei die Aufbewahrung der Kontoauszüge zunächst erforderlich, um die Hilfebedürftigkeit des Klägers bzw. Antragstellers zu überprüfen. Die Kontoauszüge seien sorgfältig auf Einkommen, Vermögen und Bedarf zu prüfen. Eine kurze Einsichtnahme genüge dafür nicht. Die Kontoauszüge der letzten Monate könnten Anlass für eine Direktüberweisung der Unterkunftskosten an den Vermieter nach § 22 Abs. 7 Satz 2 SGB II

geben. Aus Kontoauszügen ablesbares unwirtschaftliches Verhalten könne zu einer Sanktion nach § 31 Abs. 2 Nr. 2 SGB II führen. Kontoauszüge seien somit eine wesentliche Entscheidungsgrundlage für die Gewährung von Leistungen nach dem SGB II und als solche zu der Verwaltungsakte zu nehmen. Die Kontoauszüge seien nicht nur für die aktuelle Verbescheidung des nächsten Bewilligungsabschnitts erforderlich, sondern auch für sich eventuell anschließende Widerspruchs- und Gerichtsverfahren. Hinzu komme die Möglichkeit einer Korrektur von Bescheiden im Überprüfungsverfahren nach § 44 SGB X. Aktenordnungen mit ihren pauschalen Regelungen zu Aufbewahrungsfristen seien als verwaltungsinterne Richtlinien nicht geeignet, gesetzliche Vorgaben wie die Grenzen des § 67c SGB X zu beseitigen.

Schließlich stellen die von dem Kläger in Bezug genommenen Hinweise der Landesbeauftragten für den Datenschutz zur datenschutzgerechten Ausgestaltung der Anforderung von Kontoauszügen bei der Beantragung von Sozialleistungen nicht justiziable Handlungsempfehlungen im Sinne des § 23 Abs. 2 Satz 1 des Gesetzes zum Schutz personenbezogener Daten im Land Brandenburg dar. Die fehlende Verbindlichkeit ergibt sich bereits aus dem Wortlaut der Hinweise selbst („sollten die folgenden Hinweise für eine datenschutzgerechte Verfahrensweise bei der Anforderung von Kontoauszügen beachtet werden"). Der fehlenden Verbindlichkeit korrespondiert die nicht bestehende rechtliche Handhabe zur Durchsetzung der Handlungsempfehlungen. Die Behörde, an die sich die Handlungsempfehlung richtet, muss die Empfehlungen des Datenschutzbeauftragten auch nicht befolgen. Der Senat sieht sich veranlasst darauf hinzuweisen, dass aus seiner Sicht die Empfehlungen der Datenschutzbeauftragten einer Überprüfung am Maßstab der Lebenswirklichkeit jedenfalls im Bereich der Grundsicherung für Arbeitsuchende nicht standhalten können. Der Verbleib der Kontoauszüge in den Verwaltungsakten ist wegen ihrer Relevanz für Folgeverfahren jedenfalls in all denjenigen Fällen, in denen der Bevollmächtigte des Klägers in Erscheinung tritt, nicht nur hinzunehmen, sondern geradezu geboten.

Verwertbarkeit von Dashcam-Aufnahmen in einem Strafverfahren

(**Amtsgericht Nienburg**, Urteil vom 20. Januar 2015 – 4 Ds 155/14, 4 Ds 520 Js 39473/14 (155/14) –)

1. **Im Strafverfahren besteht kein generelles Beweisverwertungsverbot für Dashcam-Aufzeichnungen.**
2. **Ob eine Dashcam-Aufzeichnung im Strafverfahren verwertet werden darf, ist eine Frage des Einzelfalls.**

Sachverhalt:

II. Am Sonntag, den 13.07.2014, befuhr der Zeuge H. gegen 20.00 Uhr mit dem PKW Alfa Mito, amtliches Kennzeichen …, in M. die vierspurige B … in Fahrtrichtung N. Der Zeuge fuhr mit einer Geschwindigkeit von ungefähr Km/h 100. Auf Höhe der touristischen Unterrichtungstafel überholte der Angeklagte mit dem PKW VW T5, amtliches Kennzeichen …, auf der linken Fahrspur den auf der rechten Fahrspur fahrenden Zeugen H. Die Geschwindigkeit des Angeklagten war im Verhältnis zum Zeugen leicht erhöht.

1. Als sich das Fahrzeug des Angeklagten etwas mehr als eine Fahrzeuglänge (gemessen am Fahrzeug PKW VW T5) vor das Fahrzeug des Zeugen geschoben hatte, wechselte der Angeklagte bei freier Bahn und ohne Anzeige der Fahrtrichtung von der linken auf die rechte Spur. Dort angelangt verlangsamte er seine Geschwindigkeit, so dass sich der Abstand der beiden Fahrzeuge sofort auf weniger als eine Fahrzeuglänge (wiederum gemessen an der Größe des PKW VW T5) verringerte. Mit diesem Fahrmanöver wollte der Angeklagte den Zeugen H. zum Abbremsen oder Ausweichen verleiten und so für ein vorausgehendes, vermeintlich verkehrswidriges Verhalten maßregeln.

Um einen Auffahrunfall zu verhindern, wechselte der Zeuge H. auf den linken Fahrstreifen und überholte das Fahrzeug des Angeklagten. Während der Zeuge H. noch sein Fahrzeug beschleunigte, driftete das Fahrzeug des Angeklagten über die Mittelmarkierung, so dass sich die linken Räder des VW T5 auf der linken Fahrspur befanden und der Zeuge H. seinerseits weiter nach links zur Leitplanke ausweichen musste. Als sich die beiden Fahrzeuge auf gleicher Höhe befanden, betrug der Seitenabstand zwischen den Fahrzeugen bei einer Geschwindigkeit von rund Km/h 100 nur noch ungefähr 5 cm. Es ist unerklärlich, warum der Seitenabstand von wenigen Zentimetern nicht weiter unterschritten wurde und warum es nicht zu einem schweren Verkehrsunfall gekommen ist.

2. Der Zeuge H. fuhr sodann zum „… Döner". Der Angeklagte folgte dem Zeugen mit seinem Fahrzeug und hielt ebenfalls auf dem Parkplatz an. Auf dem Parkplatz überzog der Angeklagte den Zeugen H. mit einer Schimpftirade und betitelte den Zeugen als „dummen Wichser" und „Arschloch".

3. Der Zeuge H. ist ausgebildeter IT-Administrator. Er ist im Datenschutzrecht geschult. Kurz vor dem unter Ziffer 1. geschilderten Fahrverlauf fiel dem Zeugen H. das hinter ihm befindliche Fahrzeug des Angeklagten durch sehr dichtes Auffahren auf. Daher aktivierte der Zeuge H. zum Zwecke der Beweissicherung für den etwaigen Fall eines Zusammenstoßes eine neben seinem Innenspiegel angebrachte Kamera (sogenannte Dashcam). Diese Kamera filmte sodann den Straßenbereich vor der Kühlerhaube des Fahrzeugs des Zeugen und speicherte die Aufnahmen digital auf einer SD-Speicherkarte. In die Bildfolge wird das jeweilige Datum samt Uhrzeit eingeblendet. Die Bildfolge hat eine Gesamtlänge von fünfeinhalb Minuten und endet auf dem Parkplatz des „… Döner". Wegen der abgebildeten Einzelheiten wird gemäß § 267 Abs. 1 Satz 3 StGB Bezug auf die zu den Akten genommenen neun Einzelbildausdrucke mit den Zeitstempeln 19:06:27 bis 19:10:30 genommen (Anlagen 1 bis 9 des Protokolls der Hauptverhandlung).

Aus den Gründen:

1. Der Angeklagte räumt das festgestellte Geschehen im Wesentlichen ein. Er hat in der Hauptverhandlung jedoch betont, er habe den Zeugen H. nicht seitlich nach links abdrängen wollen. Der Angeklagte hat sich dahingehend eingelassen, seine Tochter habe just zu weinen begonnen, als der Zeuge H. an ihm links vorbeigefahren sei. Er habe sich in diesem Augenblick nach rechts hinten zu seiner Tochter umgedreht. Dabei habe er das Steuer aus Unachtsamkeit verzogen, so dass das Fahrzeug unbeabsichtigt nach links gedriftet sei.

2. Die Einlassung des Angeklagten wird in weiten Teilen durch die Aussagen der vernommenen Zeugen und die in Augenschein genommenen Filmaufzeichnungen der Dashcam bestätigt. Hierbei sind die Behauptungen des Angeklagten, er habe Rückschau gehalten und sei nur aus Unachtsamkeit auf die linke Spur gedriftet, nicht zu widerlegen. Weder die Aussagen der Zeugen noch die sonstigen Beweismittel lassen zweifelsfrei den Schluss zu, dass der Angeklagte den Zeugen H. abdrängen wollte.

a) Der Zeuge H. und seine Beifahrerin, die Zeugin S., haben ausgesagt, dass sie während des eigenen Überholmanövers die im

Fahrzeug VW T5 befindlichen Personen nicht haben sehen können. Der Höhenunterschied zwischen den beiden Fahrzeugen habe dies auf die kurze Entfernung nicht zugelassen. Sie haben daher keine Kenntnis, ob der Angeklagte beim Überfahren der Mittelmarkierung nach hinten rechts oder aber zur Seite nach links, also in Richtung des Fahrzeugs der Zeugen, gesehen habe.

b) Die Aufzeichnung der Dashcam ist verwertbar. Aus der Bildfolge und den dazugehörigen Einzelbildausdrucken ist der objektive Fahrverlauf im Einzelnen klar ersichtlich. Im Hinblick auf den Nachweis einer Vorsatztat ist die Aufzeichnung aber unergiebig.

aa) Ob und gegebenenfalls unter welchen Voraussetzungen Dashcam-Aufzeichnungen in gerichtliche Verfahren zulässig eingeführt und verwertet werden dürfen, ist derzeit Gegenstand einer breiten Diskussion in der juristischen Fachwelt und der allgemeinen Öffentlichkeit (vgl. bspw. Bachmeier, in: DAR 2014, 15 f.; Klann, in: DAR 2014, 451 f.; Brenner, in: DAR 2014, 619, 624 f.; Balzer/Nugel, in: NJW 2014, 1622 f.; Stellungnahme des Düsseldorfer Kreises vom 20.03.2014, ZD-Aktuell 2014, 03978, – zitiert nach juris – ; Heckmann, in: jurisPR-ITR 18/2014 Anm. 1 f., – zitiert nach Juris – ; Nugel, in: jurisPR-VerkR 17/2014 Anm. 2, – zitiert nach juris – ; s.a. Zeit-Online: „Verbotene Filmerei kann teuer werden", abgerufen im weltweiten Netz am 17.02.2015 unter www.zeit.de/mobilitaet/2014-10/dashcam-bussgeld). Aus dem Bereich der Zivil- und Verwaltungsgerichtsbarkeit liegen die ersten Entscheidungen der Eingangsinstanzen vor (vgl. bspw. AG München, Urteil vom 06.06.2013, 343 C 4445/13; AG München, Beschluss vom 13.08.2014, 345 C 5551/14; VG Ansbach, Urteil vom 12.08.2014, AN 4 K 13.01634, – alle zitiert nach juris –). Strafgerichtliche Entscheidungen sind noch nicht ersichtlich.

bb) Die vorliegende Dashcam-Aufzeichung ist in vollem Umfang verwertbar. Ihr steht weder ein Beweiserhebungs- noch ein Beweisverwertungsverbot entgegen.

(1) Die Anfertigung der Kameraaufzeichnung durch den Zeugen H. ist gemäß § 4 Abs. 1 BDSG in Verbindung mit einer entsprechenden Anwendung des § 28 Abs. 1 Nr. 1 BDSG zulässig.

(a) Die Digitalaufzeichnung unterfällt gemäß § 3 Abs. 2 Satz 2 BDSG dem Anwendungsbereich des BDSG. Da dem Videobild in der gewählten Betriebsform automatisch das Datum und die Uhrzeit der Aufzeichnung zugeordnet werden, handelt es sich bei der Aufzeichnung um eine sogenannte nicht automatisierte Verarbeitung personenbezogener Daten (vgl. sehr ausführlich hierzu: VG Ansbach, Urteil vom 12.08.2014, AN 4 K 13.01634, RdnRn. 38, 40 f., – zitiert nach juris –).

(b) Die spezialgesetzliche Ermächtigung des Zeugen H. folgt nicht aus § 6b BDSG, sondern aus einer entsprechenden Anwendung des § 28 Abs. 1 Nr. 1 BDSG.

(aa) § 6b BDSG ist nicht anwendbar, da die Norm nur für den ortfesten Betrieb einer Kamera gilt. Dieser Schluss ergibt sich bereits aus der Hinweispflicht des § 6b Abs. 2 BDSG (Klann, in: DAR, 2014, 451, 452). Denn beim Betrieb einer beweglichen Kamera ist es schlicht unmöglich, die betroffenen Personen auf die bevorstehende Aufzeichnung hinzuweisen.

(bb) § 28 Abs. 1 Nr. 1 BDSG ist seinerseits nicht unmittelbar, sondern nur entsprechend anzuwenden, da der vom Zeugen verfolgte Geschäftszweck – Beweissicherung für den Fall des Unfalls – in der Norm planwidrig fehlt (vgl. Klann, in: DAR, 2014, 451, 453 f.).

§ 28 Abs. 1 Nr. 1 BDSG wäre nur dann direkt anwendbar, wenn der Zeuge im Verhältnis zu seinem Kraftfahrzeugversicherer verpflichtet wäre, im Vorfeld eines Unfalls nach besten Kräften Beweise zu sichern (vgl. Klann, in: DAR, 2014, 451, 453 f.).

Für die strafrechtliche Verwertbarkeit von Beweismitteln und die Suche nach materieller Wahrheit und Gerechtigkeit kann es jedoch nicht darauf ankommen, ob der jeweilige Zeuge durch Zufall im Verhältnis zum Kraftfahrzeugversicherer derart verpflichtet ist. Entscheidend ist nicht die Reichweite versicherungsvertraglicher Rechte und Pflichten, sondern das vom Zeugen verfolgte Ziel.

Fertigt der Zeuge – wie hier – aus aktuellem und konkreten Anlass vorausschauend Beweismittel zum Nachweis der Begründung, Reichweite und Ausschluss einer gesetzlichen Haftung aus einem Unfallereignis und damit im Hinblick auf ein konkret bestimmbares gesetzliches Schuldverhältnis an, so ist dies in jeder Hinsicht mit den im Gesetz genannten Fällen der Erfüllung konkret bestimmter rechtsgeschäftlicher oder rechtsgeschäftsähnlicher Zwecke vergleichbar. Es ist kein Grund ersichtlich, warum in diesem Zusammenhang zwischen rechtsgeschäftlichen bzw. rechtsgeschäftsähnlichen und gesetzlichen Schuldverhältnissen unterschieden werden sollte (ähnlich Klann, in: DAR, 2014, 451, 453 f.). Der Betroffene verfolgt jeweils konkret abgegrenzte und bestimmbare vermögensbezogene Rechtsangelegenheiten im Zusammenhang mit dem Betrieb seines Kraftfahrzeugs im öffentlichen Straßenverkehr.

(c) Die Voraussetzungen der Ermächtigungsnorm entsprechend § 28 Abs. 1 Nr. 1 BDSG sind erfüllt. Im Rahmen der gebotenen Interessenabwägung zwischen dem Interesse des Zeugen an der Anfertigung der Aufzeichnung zum Zwecke der Beweissicherung und dem Interesse des Angeklagten an der Unverletzlichkeit des Rechts auf informationelle Selbstbestimmung überwiegt das Interesse des Zeugen (a.A. AG München, Beschluss vom 13.08.2014, 345 C 5551/14; VG Ansbach, Urteil vom 12.08.2014, AN 4 K 13.01634, – beide zitiert nach juris –). Maßgeblich ist insoweit, dass die kurze, anlassbezogene Aufzeichnung nur die Fahrzeuge, aber nicht die Insassen der Fahrzeuge abbildet und nur Vorgänge erfasst, die sich im öffentlichen Straßenverkehr ereignen. Der Eingriff in das Recht des Angeklagten ist daher denkbar gering, während das Interesse des Zeugen an einem effektiven Rechtsschutz besonders hoch ist. Denn gerade die gerichtliche Aufklärung von Verkehrsunfallereignissen leidet fast ausnahmslos unter dem Mangel an verlässlichen, objektiven Beweismitteln. Zeugenaussagen sind vielfach ungenau und subjektiv geprägt, Sachverständigengutachten kostspielig und häufig unergiebig. Der anlassbezogene Einsatz der Dashcam ist deshalb in dieser konkreten Fallgestaltung für den vom Zeugen verfolgten Zweck der Beweissicherung geeignet, erforderlich und verhältnismäßig.

Dem kann nicht entgegengehalten werden, dass die Aufzeichnung möglicher Weise später unzulässig im Internet veröffentlicht oder zu anderweiten Zwecken missbraucht werden könnte (so aber wohl zu verstehen: AG München, Urteil vom 14.08.2014, 345 C 5551/14, und VG Ansbach, Urteil vom 12.08.2014, AN 4 K 13.01634, – beide zitiert nach juris –). Die Gefahr des späteren Missbrauchs von ursprünglich zulässig gefertigten Beweismitteln besteht immer. Die dem Einwand zugrundeliegende abstrakte Furcht vor allgegenwärtiger Datenerhebung und dem Übergang zum Orwell'schen Überwachungsstaat darf nicht dazu führen, dass den Bürgern sachgerechte technische Hilfsmittel zur effektiven Rechtsverfolgung und Rechtsverteidigung kategorisch vorenthalten werden (ähnlich, aber mit anderer Begründung: Klann, in: DAR 2014, 451, 456).

(2) Die zulässig angefertigte Kameraaufzeichnung darf im Strafverfahren auch verwertet werden. Es sind keine Gründe ersichtlich,

die einer Verwertung entgegenstünden. Hierbei kann ohne weiteres auf die allgemeinen Grundsätze zur Verwertbarkeit von Beweismitteln mit Spannungsbezug zum allgemeinen Persönlichkeitsrecht Dritter zurückgegriffen werden (sogenannte Sphärentheorie des Bundesverfassungsgerichts, vgl. bspw. BVerfG NJW 1990, 563, 564 – „Tagebuch"; BGH NJW 1996, 2940 = BGH, Beschluss vom 13.05.1996, GSSt 1/96 – „Hörfalle"; BGH NStZ 1998, 635; s.a. BAG, Beschluss vom 29.06.2004, 1 ABR 21/03 – „Videoüberwachung am Arbeitsplatz").

Da die Aufnahme Vorgänge aus dem öffentlichen Straßenverkehr abbildet, ist der absolute Kernbereich der persönlichen Lebensführung des Angeklagten nicht betroffen. Das Gericht hat daher abzuwägen, ob im konkreten Fall das öffentliche Interesse an der effektiven Strafverfolgung oder das aus dem allgemeinen Persönlichkeitsrecht erwachsende Geheimschutzinteresse des Angeklagten überwiegt. Hierbei sind unter anderem die Schwere der angeklagten Tat, das Sicherheitsbedürfnis der Allgemeinheit, die Verfügbarkeit sonstiger Beweismittel und die Intensität und Reichweite des Eingriffs in das Recht auf informationelle Selbstbestimmung zu berücksichtigen.

Im Rahmen einer Gesamtschau überwiegt bei wertender Betrachtung unter Berücksichtigung der schutzwürdigen Belange des Angeklagten das allgemeine Interesse an der Effektivität der Strafverfolgung. Die Verwertung der Aufzeichnung ist erforderlich, da aufgrund der Unergiebigkeit der Zeugenaussagen keine anderen Beweismittel zur Verfügung stehen. Die Verwertung ist auch verhältnismäßig. Denn zum einen ist nicht der Angeklagte selbst, sondern nur sein Fahrzeug abgebildet. Ein zu berücksichtigender Verstoß gegen das KUG kommt also von Anfang an nicht in Betracht. Zum anderen bestand zum Zeitpunkt der Verwertung nach dem bisherigen Gang der Hauptverhandlung der dringende Verdacht, dass der Angeklagten im Falle eines Schuldspruchs zu einer empfindlichen Freiheitsstrafe verurteilt und ihm wegen fehlender Eignung die Fahrerlaubnis entzogen wird. Da diese Maßnahmen im konkreten Fall vor allem das Interesse aller Bürger an der zukünftigen Sicherheit des Straßenverkehrs schützen sollen, tritt das Recht des Angeklagten auf informationelle Selbstbestimmung hier hinter dem Interesse der Allgemeinheit an einer effektiven Strafverfolgung zurück.

Dieser Wertung kann man nicht entgegenhalten, dass der vom Zeuge verfolgte Zweck der Aufzeichnung – Beschaffung eines Beweismittels für den Fall der gesetzlicher Haftung – nicht mit dem vom Gericht verfolgten Zweck der Verwertung – Erkenntnisquelle im Strafverfahren – übereinstimmt. Denn das Geheimschutzinteresse des Angeklagten würde nur dann überwiegen, sofern sich der Angeklagte gegen eine dem Grunde nach unzulässige Überwachung durch Dritte zur Wehr setzen würde.

Das wäre gegebenenfalls dann der Fall, wenn Personen aus eigener Machtvollkommenheit zielgerichtet mittels Dashcam-Aufzeichnungen Daten für staatliche Strafverfahren erheben und sich so zu selbsternannten „Hilfssheriffs" aufschwingen. So liegt der Fall aber nicht. Verfolgt der Betreiber der Dashcam wie hier den zulässigen Zweck der Beweissicherung für den konkreten Haftungsfall, so bestehen gegen die Verwertung im Strafverfahren zumindest dann keine durchgreifenden Bedenken, wenn der Betreiber der Dashcam auch Verletzter einer vom Betroffenen verwirklichten Straftat sein könnte. Da im Bereich des Straßenverkehrsstrafrechts vielfach Rechtsgüter der Allgemeinheit betroffen sind, ist der Begriff des Verletzten im Sinne des § 172 StPO auszulegen. Da dem Angeklagte nicht nur eine Verletzung des allgemeinen Rechtsguts der Sicherheit des Straßenverkehrs, sondern auch eine Beeinträchtigung von Individualrechtsgütern und Rechten – nämlich Leben, Leib und Willensfreiheit des Zeugen H. sowie dessen Eigentums – vorgeworfen wird, wäre der Zeuge H. befugt gewesen, gegen eine Verfahrenseinstellung gemäß § 172 Abs. 1 StPO die Vorschaltbeschwerde zu erheben. Diese Übereinstimmung von prozessualer und materiell-rechtlicher Stellung des Zeugen H. rechtfertigt die Verwertung der Dashcam-Aufzeichnung auch unter dem Gesichtspunkt einer ursprünglich abweichenden Zielsetzung bei Anfertigung der Aufzeichnung.

cc) Die Verwertung der Aufzeichnung ist im Ergebnis aber nur teilweise ergiebig.

(1) Aus der Aufzeichnung ergeben sich keine Anknüpfungstatsachen, die den zweifelsfreien Schluss zuließen, dass der Angeklagte den Zeugen H. vorsätzlich abdrängen wollte. Die Einlassung des Angeklagten, seine Drift auf den linken Fahrstreifen beruhe auf Unachtsamkeit und Ungeschicklichkeit, ist auch anhand der Aufzeichnung nicht zu widerlegen. Mit dem Rechtsgrundsatz „Im Zweifel für den Angeklagten" ist daher davon auszugehen, dass die Einlassung des Angeklagten insoweit zutreffend ist.

(2) Gleichwohl ist die Aufzeichnung der Dashcam von herausragender Bedeutung für die gerichtlichen Feststellungen. Die Aufzeichnung versetzt das Gericht in die Lage, die Einlassung des Angeklagten und die Aussagen der Zeugen im unmittelbaren Zusammenhang des Gesamtgeschehens zu werten. Erst aus der Gesamtschau aller subjektiven und objektiven Beweismittel lässt sich der Vorgang im rechten Lichte würdigen. Dies gilt insbesondere für die konkreten Umstände des Eintritts des tatbestandsmäßigen Nötigungserfolgs, aber auch für die Umstände des Eintritts der fahrlässig verursachten Gefährdung des Straßenverkehrs. Die Einlassung des Angeklagten und die Zeugenaussagen werden durch die Aufzeichnung nicht nur im Wesentlichen bestätigt, sondern um eine Vielzahl von Einzelheiten ergänzt. Erst die Inaugenscheinnahme der abgebildeten, messbaren Geschwindigkeits- und Entfernungsunterschiede ermöglicht es dem Gericht, das strafrechtlich relevante, komplexe Geschehen zweifelsfrei festzustellen und in seiner gesamten Tragweite zu erfassen.

...

Berichte, Informationen, Sonstiges

Jedes zweite Unternehmen überprüft Bewerber in sozialen Netzwerken

Fachliche Qualifikationen und Äußerungen stehen im Mittelpunkt.

Jeder siebte Personaler hat nach dem Online-Check bereits Bewerber aussortiert.

Wer sich auf eine Stelle bewirbt, muss damit rechnen, dass neben seinen Bewerbungsunterlagen auch seine Profile in Sozialen Netzwerken gründlich geprüft werden. In rund jedem zweiten Unternehmen (46 Prozent) werden die entsprechenden Seiten im Netz unter die Lupe genommen. Dabei werden Einträge in beruflichen Netzwerke wie Xing oder LinkedIn häufiger ausgewertet (39 Prozent) als die eher privat ausgerichteten wie Facebook oder Twitter (24 Prozent). Das ist das Ergebnis einer repräsentativen Befragung im Auftrag des Digitalverbands BITKOM unter 408 Personalverantwortlichen in Unternehmen ab 50 Mitarbeitern.

Mehr als jeder siebte Personalchef (15 Prozent), der sich Profile von Bewerbern in Soziale Netzwerken anschaut, hat sich bereits aufgrund eines Online-Checks entschieden, Bewerber nicht zum Gespräch einzuladen oder einen Job doch nicht anzubieten. 90 Prozent dieser Personalentscheider geben Widersprüche zu den Bewerbungsunterlagen als Grund für die Entscheidung an. Jeder Dritte (32 Prozent) berichtet von inkompetenten fachlichen Äußerungen der Kandidaten, 6 Prozent sind auf beleidigende Äußerungen gestoßen. Keine Rolle spielen dagegen die politische Weltanschauung des Kandidaten oder Fotos von ausgelassenen Partys.

Im Mittelpunkt des Interesses stehen bei der Prüfung von Social-Media-Profilen die fachliche Qualifikation (89 Prozent), öffentliche Äußerungen zu Fachthemen (72 Prozent) sowie über das Unternehmen oder seine Wettbewerber (56 Prozent). Knapp jeder Zweite (44 Prozent) achtet auch auf Hobbys oder private Aktivitäten der Kandidaten, 34 Prozent betrachten veröffentlichte Fotos sehr genau. Weniger von Interesse sind die Anzahl der Kontakte in den Netzwerken (5 Prozent) oder politische Ansichten (4 Prozent).

Wann die Einträge in den Sozialen Netzwerken überprüft werden, variiert dabei. Fast zwei Drittel der Unternehmen (62 Prozent) informieren sich im Netz vor der Entscheidung, ob ein Bewerber zum Gespräch eingeladen wird, 39 Prozent überprüfen die Angaben nach dem Gespräch, 30 Prozent bereits bei der ersten Sichtung der Unterlagen. Und 12 Prozent gleichen ihr Bild vom Kandidaten kurz vor der Entscheidung, ob ein Vertrag unterschrieben wird, noch einmal mit den Social-Media-Profilen ab.

(BITKOM-Pressemitteilung vom 02.06.2015: Personaler nutzen Soziale Medien)

Dashcams: 6 von 10 Deutschen erwarten mehr Verkehrssicherheit durch Autokameras

Jeder Dritte fordert Dashcam-Pflicht in Deutschland

Sie werden auf dem Armaturenbrett oder an der Windschutzscheibe des Autos angebracht und zeichnen das Verkehrsgeschehen vor dem Fahrzeug auf – sogenannte Dashcams sind im Kommen. Drei von vier Deutschen (74 Prozent) gehen davon aus, dass die Videokameras im Auto in den kommenden Jahren in Deutschland zum Alltag gehören werden. Fast sechs von zehn Befragten (58 Prozent) sind zudem der Ansicht, dass die Kameras zur Verkehrssicherheit beitragen. Das hat eine repräsentative Umfrage im Auftrag des Digitalverbands BITKOM ergeben.

„Schon jetzt sind zahlreiche Dashcam-Modelle in unterschiedlichen Preiskategorien erhältlich, und der Markt wird mittelfristig stark wachsen“. Mithilfe einer Dashcam können z.B. Unfälle aufgezeichnet werden. Aber auch Landschaftsaufnahmen auf dem Weg in den Urlaub sind möglich. Einige Modelle haben außerdem Spezialfunktionen wie einen Abstandswarner oder Spurhalteassistenten.

Dashcams sind derzeit vor allem in Russland weit verbreitet. Dort nutzen viele Autofahrer die Kameras, um bei einem Unfall Beweismaterial in der Hand zu haben. In Deutschland ist die Rechtslage rund um die Verwendung von Dashcams und die Zulässigkeit der Aufnahmen vor Gericht noch strittig. Zwei Drittel (67 Prozent) der Deutschen wünschen sich, dass Dashcam-Videos als juristische Beweismittel zugelassen werden, wie die BITKOM-Umfrage zeigt. Gut die Hälfte (54 Prozent) denkt, dass Dashcams den Fahrer zu einer vorsichtigeren Fahrweise zwingen. Ein Drittel (33 Prozent) findet, die Nutzung von Dashcams sollte sogar gesetzlich vorgeschrieben werden. Ebenso viele (32 Prozent) wünschen sich, dass Dashcams standardmäßig in alle Neuwagen eingebaut werden.

Gut die Hälfte der Befragten (54 Prozent) findet indes, dass Dashcams eine Atmosphäre der Überwachung erzeugen. Knapp 45 Prozent fürchten, die Kameras könnten den Fahrer vom Verkehr ablenken. 38 Prozent sagen, Dashcam-Nutzer seien ihnen suspekt. Und rund ein Viertel (26 Prozent) findet, die Autokameras stellen einen Eingriff in die Privatsphäre anderer Verkehrsteilnehmer dar und sollten verboten werden.

(BITKOM-Pressemitteilung vom 01.06.2015)

EU-DS-GVO nun doch noch in diesem Jahr

Am 16. Juni hat auch der Rat seine Beratung zur EU-DS-GVO abgeschlossen und sich auf ein gemeinsames Papier geeinigt. Die nachfolgenden Verhandlungen im sog. Trilog zwischen Kommission, dem Parlament und dem Rat sollen nach dem politisch erklärten Ziel der europäischen Staats- und Regierungschefs Ende 2015 abgeschlossen werden.

Diese sog. Trilog-Verhandlungen finden nicht öffentlich statt. Bei diesen Treffen versuchen sich Vertreter der drei involvierten Organe der europäischen Gesetzgebung auf einen gemeinsamen Gesetzestext zu einigen.

Nach einem von der EVP-Fraktion im Europäischen Parlament veröffentlichten vorläufigen, d.h. bislang noch nicht mit Kommission und Rat abgestimmten Zeitplan könnte der Ablauf die erste Verhandlungsrunde bereits am 24. Juni stattfinden.

Literaturhinweise

Peter Gola/Rudolf Schomerus, **BDSG Bundesdatenschutzgesetz**, Verlag C.H. Beck, 12. Auflage, 2015, bearbeitet von Peter Gola, Christoph Klug, Barbara Körffer, XVII, 677 S., 65,00 €

Es ist einigermaßen schwierig, eine Neuauflage eines allseits bekannten und bestens eingeführten BDSG-Kommentars angemessen zu besprechen. Im Grund ist in den zahlreichen Rezensionen der Vorauflagen alles schon gesagt, so dass man sich darauf beschränken könnte, lediglich auf die Änderungen und Ergänzungen einzugehen. Wenn allerdings ein Standardwerk – und das ist der Gola/Schomerus ohne jeden Zweifel – sich immer wieder aufs Neue bewährt und seine Qualität, namentlich die gelungene Verbindung von Praxishilfe und wissenschaftlicher Auseinandersetzung, unter Beweis stellt, dann darf die ihm entgegengebrachte Wertschätzung sicherlich auch noch einmal wiederholt werden. Vor allem scheint dies auch deswegen gerechtfertigt, weil völlig offen ist, ob es noch einmal zu einer Neubearbeitung kommen wird. Das Schicksal des BDSG ist mehr als ungewiss, wenn die EU-Datenschutz-Grundverordnung verabschiedet ist und nach ihrem Inkrafttreten einen großen Teil der BDSG-Bestimmungen verdrängen dürfte.

Die 12. Auflage aktualisiert u.a. die Kommentierungen zur Auftragsdatenver-

arbeitung, zum Scoring und Beschäftigtendatenschutz. Soweit das in der Praxis zunehmend an Bedeutung gewinnende Thema „Cloud Computing" behandelt wird, beschränken sich die Ausführungen leider im Wesentlichen auf weiterführende Literaturhinweise (vgl. § 11 Rdn. 8) - allerdings verständlich, wenn das kompakte Format des Kommentars nicht gesprengt werden soll.

Handlich, übersichtlich in der Gliederung und gut lesbar auf Grund der klaren Sprache bietet die jüngste Bearbeitung des Kommentar einmal mehr Soforthilfe in allen „datenschutzrechtlichen Lebenslagen". Fast unnötig zu betonen: Er ist unverzichtbar für alle, die sich mit den BDSG-Normen auseinandersetzen müssen oder wollen – und dazu bemerkenswert preisgünstig.

(RA Dr. Georg Wronka, Bonn)

Ansgar Goreng/Matthias Lachenmann, **Formularhandbuch Datenschutzrecht**, Verlag C.H.Beck, 2015, XXII, 593 S., 99,00 €

Das Buch beleuchtet ein breit gefächertes Spektrum datenschutzrechtlicher Fragestellungen, die in der Praxis von besonderer Relevanz sind. Es geht aber über ihre juristische Einordnung weit hinaus. Die eigentliche Zielrichtung liegt vielmehr darin, dem Ratsuchenden praktische Hilfestellung bei der Umsetzung der rechtlichen Anforderungen an bestimmte betriebliche Prozesse zu bieten. Diese Aufgabe erledigen die 9 Autoren ganz überwiegend in ausgezeichneter Weise. Mit zahlreichen Textmustern und Formulierungsvorschlägen für Verträge und Richtlinien sowie mit Checklisten, Prüflisten und Merkblättern erleichtern sie demjenigen, auf den diese Aufgabe zukömmt, die Ausarbeitung unternehmensspezifischer Lösungen erheblich.

Zu den in 5 Kapiteln abgehandelten Themen gehören – dies nur ein kurzer und willkürlicher Auszug –

- Auftragsdatenverarbeitung
- Fernwartung
- Videoüberwachung
- Webtracking
- Einsatz von Social Media Plug-ins
- Telearbeit
- BYOD
- Cloud Computing
- Whistleblower-Hotlines

Dabei widmet sich das erste Kapitel über 60 Seiten dem betrieblichen Datenschutzbeauftragten (Bestellung, Tätigkeitsbereich usw.) – wohl ein Indiz, dass das Werk diesen Funktionsträger besonders ansprechen will. Es wendet sich aber erklärtermaßen auch an juristische Berater (Anwälte, Rechtsabteilungen), die häufig – vor allem, wenn sie mit der Materie nicht so vertraut sind – für eine Wegweisung dankbar sein werden.

Kurzum: Eine überaus verdienstvolle und empfehlenswerte Veröffentlichung.

(RA Dr. Georg Wronka, Bonn)

Dirk Zitzen, **Kommunale Videoüberwachung.** Das Recht der inneren und äußeren Sicherheit, Bd. 3, Duncker Humblot, Berlin, 2015, 253 S. Print 79,90 €; E-Book 71,90 €

Das Buch befasst sich mit dem Einsatz der Videoüberwachungstechnik durch Kommunen in Nordrhein-Westfalen. Wenngleich damit, soweit nicht Bundesrecht greift, Normen des Landes NRW herangezogen werden, sind die Ausführungen für Kommunen insgesamt von Belang, da gravierende Unterschiede in den Rechtsregeln der Bundesländer insoweit nicht bestehen.

Während sich die rechtswissenschaftliche Diskussion in den letzten Jahren intensiv mit der polizeilichen Videoüberwachung befasste, wurden die Befugnisse der Kommunen zur Videoüberwachung in einem eher geringen Umfang betrachtet. Insofern hilft das Buch eine Lücke zu füllen. Der Autor arbeitet zunächst die verfassungsrechtlichen Vorgaben heraus, und die – je nach der Eingriffsqualität – erforderlichen Anforderungen für den Eingriff in das Recht des Bürgers am eigenen Bild. Sodann werden die Normen dargestellt, die die Kommunen zu präventiven bzw. repressiven Überwachungsmaßnahmen ermächtigen. Eingegangen wird auf Befugnisse aus dem Polizei- und Ordnungsrecht, dem Landesdaten- und dem Bundesdatenschutzgesetz, der Strafprozessordnung und aus dem Zivilrecht. Aufgezeigt werden auch die diesbezüglichen für den behördlichen DSB relevanten Aspekte der Vorabkontrolle, des Verfahrensverzeichnisses und der Einschaltung von Auftragsdatenverarbeitern.

Der Autor kommt zu dem Ergebnis, dass die geltende Rechtslage in verschiedenen Bereichen Regelungsdefizite aufweist. Er erarbeitet unter Berücksichtigung datenschutzfördernder Technik Regelungsvorschläge für bereichsspezifische Erweiterungen der Befugnisse der Kommunen zur Videoüberwachung. Darüber hinaus entwickelt er eine Regelung für ein Verbot von Kameraattrappen.

(Prof. Peter Gola, Königswinter)

Xenia Lang, **Geheimdienstinformationen im deutschen und amerikanischen Strafprozess.** Schriftenreihe des Max-Planck-Instituts für ausländisches und internationales Strafrecht, Strafrechtliche Forschungsberichte, Band S 145, Duncker & Humblot, Berlin, 2015, 400 S., 41,00 €

Der Kampf gegen den Terrorismus beschränkt sich nicht allein auf die Verhinderung gefährlicher Terroranschläge, sondern erfasst auch deren strafrechtliche Bewertung und Verfolgung. Undurchsichtige Kriminalitätsstrukturen erschweren jedoch die Arbeit der Strafverfolgungsbehörden, sodass diese vermehrt auf eine Zusammenarbeit mit anderen Sicherheitsbehörden setzen. Allerdings wird besonders die Kooperation mit den Nachrichtendiensten in Deutschland sehr kritisch gesehen. So wies das Bundesverfassungsgericht 2013 in seinem Urteil zur Antiterrordatei unter anderem auf die Gefahren für die Grundrechte hin, die ein Informationsaustausch zwischen den Behörden mit sich bringt.

Der in diesem Bereich bestehenden Forschungslücke begegnet die Autorin mit einer rechtsvergleichenden Analyse der deutschen und der amerikanischen Rechtsordnung.

(Schriftleitung)

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.

Carola Elbrecht /Michaela Schröder, **Verbandsklagebefugnisse bei Datenschutzverstößen für Verbraucherverbände**, K&R 2015, S. 361 ff.
Im Zuge der zunehmenden Digitalisierung des Verbraucheralltags weisen auch die meisten Nutzungs- und Vertragsverhältnisse zwischen Verbraucher und Internetanbieter einen datenschutzrechtlichen Bezug auf. Folgerichtig habe sich nach Auffassung der Autorinnen die Bundesregierung entschieden, in Zeiten der massenhaften Datenverarbeitung durch Unternehmen für eine effektive Durchsetzung des Datenschutzrechts neben den behördlichen Instrumenten der Kontrolle und Sanktionen durch Datenschutzaufsichtsbehörden auch die Befugnisse der Verbraucherschutzorganisation durch Novellierung des UKlAG zu erweitern.

Johannes Gräbig, **Haftung von Suchmaschinen – Verletzung des Rechts am eigenen Bild durch die Bildersuche**, MMR 2015, S. 365 ff.
Erörtert werden nach Erläuterung des technischen Hintergrunds u.a. Fragen des Urheberrechts und des Rechts am eigenen Bild. Kritisiert wird eine Haftungspivilegierung trotz Täterschaft.

Gerit Hornung, **Verfügungsrahmen an fahrzeugbezogenen Daten – Das vernetzte Auto zwischen innovativer Wertschöpfung und Persönlichkeitsrecht**, DuD 2015, S. 359 ff.
Die in modernen Kfz verbaute IT und der Zugang zum Internet dienen zunehmend nicht nur der Fahrsicherheit und dem Fahrkomfort, sondern allen möglichen weiteren Zwecken. Viele der durch die heute schon über 100 Sensoren erhobenen Daten haben einen wirtschaftlichen Wert. Eine der drängendsten Fragen für Automobilhersteller, Internetanbieter und Fahrzeuginsassen ist deshalb, wer über die fahrzeugbezogenen Daten verfügen und diese ökonomisch ausbeuten darf.

Michael Kort, **Informationsrechte des Betriebsrats nach § 80 II BetrVG bei Mitarbeitergesprächen, Zielvereinbarungen und Talent Management**, NZA 2015, S. 520 ff.
Mitarbeiter-Zielvereinbarungen und Maßnahmen des Talent-Managements sind der Praxis zunehmend von Bedeutung. Im Vorfeld einer möglichen Mitbestimmungspflichtigkeit stellt sich die Frage, inwiefern der Betriebsrat Informationsrechte gem. § 80 ll BetrVG in Hinblick auf Mitarbeitergespräche, Zielvereinbarungen und Maßnahmen des Talent-Managements hat.

Markus Lang/Matthias Lachenmann, **Kein Mitbestimmungsrecht bei Videokamera-Attrappen**, NZA 2015, S. 591 ff.
Der Beitrag bewertet das Urteil des LAG Mecklenburg-Vorpommern (RDV 2015, 155), das ein Mitbestimmungsrecht des Betriebsrats bei Videokamera-Attrappen ablehnte. Davon ausgehend wird das Kollektivarbeitsrecht bei Kamera-Attrappen ebenso dargestellt wie die Grundsätze der Videoüberwachung im Betrieb.

Thomas Petri, **Auftragsdatenverarbeitung – heute und morgen – Reformüberlegungen zur Neuordnung des Europäischen Datenschutzrechts**, ZD 2015, S. 305 ff.
Der Beitrag erörtert die typischen Probleme der Auftragsdatenverarbeitung. Ein Ausblick auf die anstehende EU-DS-GVO lässt keine grundlegenden Änderungen der Anforderungen an die Auftragsdatenverarbeitung gegenüber der jetzigen Rechtslage erkennen.

Bruno Schierbaum, **Sachkundige Arbeitnehmer – Anhörung durch Betriebsrat ohne Arbeitgebervertreter**, CuA 6/2015, S. 18 ff.
Ausgehend von dem Urteil des BAG vom 20.01.2015 (in diesem Heft S. 196) wird aufgezeigt, inwieweit der Betriebsrat neben externen Sachverständigen auch – und dies vorrangig – sachkundige Arbeitnehmer aus dem eigenen Unternehmen in Datenschutzfragen zu Rate ziehen kann, wozu auch der betriebliche Datenschutzbeauftragte zählt.

Thorsten Sörup/Sabrina Marquardt, **Datenschutz bei Connected Cars – Plädoyer für eine Branchenlösung der Automobilindustrie**, ZD 2015, S. 310 ff.
Statt zur Lösung der zahlreichen Rechtsfragen sog. Connected Cars nach dem Gesetzgeber zu rufen, wird vorgeschlagen, eine Branchenlösung auf der Basis des § 38a BDSG oder Art. 27 RL 95/46/EG in Betracht zu ziehen. Auf eine mögliche Vorbildregelung im US-amerikanischen Recht wird Bezug genommen.

Thilo Weichert, **Das Äußerungsrecht der Datenschutzaufsichtsbehörden** (Teile 1 und 2), DuD 2015, S. 323 und 397 ff.
Öffentliche Äußerungen sind ein wirksames, oft das wirksamste Instrument für Datenschutzbehörden zur Durchsetzung des Datenschutzrechts. Demgemäß gibt es eine differenzierte und umfassende Öffentlichkeitsarbeit und oft eine enge Kooperation zwischen Aufsichtsbehörden und Presse. Beleuchtet werden müssen jedoch die Grenzen öffentlicher Äußerungen der Aufsichtsbehörden vor dem Hintergrund des Verhältnismäßigkeitsgrundsatzes und der Neutralitätsverpflichtung von Amtsvertretern.

Peinliche Wortverdreher

Schreibhilfen im Smartphone sind für viele eine feine Sache. Zwei Buchstaben tippen und schon kann man sich aussuchen, was man schreibt. Das kann aber auch nerven, oder sogar nach hinten losgehen.

Zum Beispiel, wenn man folgende Nachricht von der Arbeit an seine Frau schickt. „Hallo Schatz, warte nicht mit dem Essen auf mich. Ich muss noch mit dem Chef zum petting." - „Spinnst Du?" – „Oh sorry, ich meinte zum Meeting." Die Wortvorschläge machen im Kontext oft keinen Sinn und sie können auch peinlich werden. Da kann aus evakuieren ejakulieren werden, aus Arche Noah Asche Noch, aus dir absagen dir bärchen, aus geschlagen geschlafen und aus gemerkt genervt. Leider kann man sich auf die falschen Vorschläge noch nicht einmal verlassen, weil jedes Handy neue Worte lernt und seine Vorschläge vom Nutzer abhängig macht. Deswegen ist eine Kontrolle unverzichtbar. Das ist vor allem bei E-Mails wichtig, die anders als SMS auch für offizielle Korrespondenz genutzt werden.

Ob Wortverdreher rechtliche Relevanz haben ist eine Frage des Einzelfalls. In der Regel dürften sie einfach als „Verschreiber" zu werten sein, die keine Konsequenzen nach sich ziehen. Wenn sie beleidigend sind und sich ein Empfänger dadurch mehr als auf den Schlips getreten fühlt, sind sie aber trotzdem dem Absender als Aussage zuzurechnen. Schließlich muss er prüfen, was er verschickt und er löst ja auch den Sendevorgang aus. Hier müsste man zumindest nachweisen, warum die Aussage ein Versehen ist.

Man kann Schreibhilfen natürlich abstellen. Bei IOS geht das unter Einstellungen, Allgemein, Tastatur. Bei Android muss man Einstellungen, Sprache und Eingabe, Tastatur, Autokorrektur, Aus klicken. Wer das nicht möchte, der kann unter seine Nachrichten natürlich auch einen erklärenden Standardzusatz schreiben. „Lieber Empfänger. Ich weiß, dass ein Meeting kein Petting ist und Evakuieren nichts mit Ejakulieren zu tun hat. Solche oder ähnliche Verdreher sind unbeabsichtigt. Bitte rechnen Sie sie mir nicht zu und wenden sich an den Programmierer meiner Autokorrekturvorschläge."

Einzigartig kommentiert.

Das Werk Online:
www.otto-schmidt.de/cr-online

Redeker (Hrsg.)
Handbuch der IT-Verträge
Loseblatt, z.Zt. 4.786 Seiten in 3 Ordnern, inkl. CD mit allen Mustern. Nur 159,– € bei einem Abonnement für mindestens zwei Jahre. Ergänzungslieferungen 1–3-mal im Jahr. ISBN 978-3-504-56008-9. Ohne Abonnement 299,– €. ISBN 978-3-504-560274

Das Handbuch für die IT-rechtliche Vertragsgestaltung: Es kommentiert und erläutert alle im EDV-Recht, IT-Recht und TK-Recht wesentlichen Verträge. Die Autoren stellen aktuelle Muster bereit, für Besonderheiten werden Ihnen alternative Formulierungen angeboten. Auf unzulässige Klauseln werden Sie hingewiesen. So durchschauen Sie in jedem Fall die komplizierten Sachverhalte der Materie und kommen beim Abschluss von Verträgen leichter zu besseren Ergebnissen. Sämtliche Vertragsmuster finden Sie auf der CD.

Neu in der Juli-Lieferung:

Vertragsmuster zu Kernthemen des IT-Rechts – vollständig überarbeitet, aktualisiert, kommentiert:
- Hardware-Wartung
- Vertrag über das Leasing eines kompletten EDV-Systems
- Domain-Übertragungs-Vertrag

Handbuch der IT-Verträge. Am besten gleich Probe lesen und bestellen bei **www.otto-schmidt.de/riv**

ottoschmidt