

# Kommunikation & Recht



Betriebs-Berater für

● Medien ● Telekommunikation ● Multimedia

12  
K&R

- Editorial: Grundrechte und Big Data · *Giovanni Buttarelli*
- 773 Ein Elefant im Porzellanladen – Der EuGH zu Personenbezug und berechtigtem Interesse · *Markus Kring* und *Johannes Marosi*
- 777 Die Datenschutz-Grundverordnung · *Dr. Carlo Piltz*
- 784 Der novellierte Jugendmedienschutz-Staatsvertrag – was ändert sich?  
*Dr. Kristina Hopf*
- 791 Tagesschau-App – OLG Köln, die Zweite  
*Prof. Dr. Karl-E. Hain* und *Tobias Brings-Wiesen*
- 794 Urheberrechtsschutz von Browsergames · *Alexander Bleckat*
- 799 Rechtsmissbrauch bei Abbruchjägern  
*Dr. Felix Buchmann* und *Anna-Lena Hoffmann*
- 801 Vorschlag der Kommission zur Weiterentwicklung des europäischen Rechtsrahmens für den Telekommunikationssektor  
*Prof. Dr. Torsten J. Gerpott*
- 808 Länderreport Österreich · *Prof. Dr. Clemens Thiele*
- 811 EuGH: Voraussetzungen für Personenbezug und Speicherung von IP-Adressen
- 814 EuGH: Auch digitale Bücher können verliehen werden
- 818 EuGH: Weiterverkauf von Software nur mit Originaldatenträger
- 822 EuGH: Irreführende Geschäftspraxis bei Preiswerbung im TV
- 826 BGH: Tannöd: Bemessung des Gegenstandswerts bei Filesharing mit Kommentar von *Franz Gernhardt*
- 847 OLG Frankfurt a. M.: Unzumutbare Belästigung durch SMS-Werbung für gemeinnütziges Projekt
- 848 OLG München: Fehlender Hinweis auf OS-Plattform wettbewerbswidrig
- 850 LG Hamburg: Appstore darf Apps mit Sportwetten-Werbung ablehnen

19. Jahrgang

Dezember 2016

Seiten 773 – 852



Markus Kring, Karlsruhe und Johannes Marosi, Mainz\*

## Ein Elefant im Porzellanladen – Der EuGH zu Personenbezug und berechtigtem Interesse

Zugleich Kommentar zu EuGH, Urteil vom 19. 10. 2016 – C-582/14, K&R 2016, 811 ff. (in diesem Heft)

### I. Das Problem

Was lange währt, wird endlich gut, sollte man jedenfalls meinen. Der Streit um den Personenbezug ist wohl einer – wenn nicht der – Evergreen des deutschen Datenschutzrechts. Das Verfahren hat Patrick Breyer bereits 2008 initiiert, wenn man einen „Vorprozess“ miteinbeziehen will, bereits 2006.<sup>1</sup> Vom AG Berlin-Tiergarten über das LG Berlin<sup>2</sup> und den BGH<sup>3</sup> hat der Streit nun auch den EuGH im Rahmen eines Vorabentscheidungsverfahrens gem. Art. 267 AEUV passiert und wird wohl – so viel darf schon einmal gesagt sein – dort nicht sein Ende finden. Neben dem Personenbezug hat sich der EuGH aber auch mit dem Umsetzungsspielraum des nationalen Gesetzgebers im Hinblick auf den Grundsatz des berechtigten Interesses auseinandergesetzt.

### II. Die Vorlagefragen

Aber zunächst zum Sachverhalt: Breyer rief mehrere Webseiten von Einrichtungen des Bundes ab. Bei dem Großteil dieser Webseiten wurden die Zugriffe in Protokolldateien festgehalten.<sup>4</sup> Dies geschehe, um Angriffe abzuwehren und die strafrechtliche Verfolgung von Angriffen zu ermöglichen.

Breyer erhob bei dem AG Berlin-Tiergarten eine Unterlassungsklage mit dem Ziel, der BRD oder (beauftragten) Dritten die Speicherung seiner IP-Adressen über das Ende des Zugriffs auf Webseiten des Bundes hinaus zu untersagen. Das AG hatte die Klage noch abgewiesen, das LG Berlin das Urteil dahingehend geändert, dass eine Speicherung zu untersagen sei, sofern Breyer während des Nutzungsvorgangs Personalien eingebe.

Der BGH hatte in dem Vorlagebeschluss zwar konstatiert, dass es sich bei der IP-Adresse um eine Einzelangabe über sachliche Verhältnisse handele, allerdings könne die keiner Person direkt zugeordnet werden. Dies könne nur über weitere Daten erfolgen, die beim Internetzugangsanbieter (ISP) vorlägen. Folglich war die erste Vorlagefrage, ob ein Personenbezug bei IP-Adressen nach der RL 95/46/EG (DSRL) für den Webseitenbetreiber auch dann besteht, wenn er diesen mit dem Zusatzwissen eines Dritten herstellen könne.

Als Folgefrage ergibt sich laut BGH, ob § 15 Abs. 1 TMG Raum für eine Auslegung lasse, die die Bedürfnisse der IT-Sicherheit berücksichtigt, etwa zum Schutz vor Denial

of Service (DoS)-Attacken. Entsprechend fragt der BGH, ob eine nationale Vorschrift, die eine Erhebung und Verwendung von Nutzerdaten im Rahmen eines Online-Mediendienstes abseits einer Einwilligung nur zur Ermöglichung des Dienstes sowie zur Abrechnung ermöglichen und wo das Interesse der Funktionsfähigkeit nicht über das Ende des Nutzungsvorgangs berücksichtigt werden könne, mit Art. 7 lit. f) DSRL vereinbar sei. Kernproblem der zweiten Vorlagefrage war also nicht, ob man die Funktionsfähigkeit eines Dienstes unter die Ermöglichung dieses Dienstes subsumieren kann, sondern vielmehr die systematische Auslegung, dass (nur) § 15 Abs. 4 TMG explizit eine Speicherung *über das Ende* des Nutzungsvorgangs vorsieht, zudem nur in speziellen Fällen.

### III. Die Entscheidung

#### 1. Zum Personenbezug

##### a) Herleitung

In Scarlet Extended hatte der EuGH bereits den Personenbezug von IP-Adressen *für den ISP* bejaht.<sup>5</sup> Im Unterschied dazu ging es in der Rechtssache Breyer aber um die Frage, ob es sich bei dynamischen IP-Adressen um personenbezogene Daten für den *Diensteanbieter* (i. S. d. TMG) handelt, wenn nur ein Dritter, hier der ISP, über das nötige Zusatzwissen zur Identifizierung der Nutzer verfügt.

Zunächst hält der EuGH fest, dass es sich nicht um eine Angabe über eine *bestimmte* Person handelt. Danach wendet er sich der Kernfrage des Falles zu, ob es sich um eine Angabe über eine *bestimmbare* Person handelt. Entscheidend sei, auf wessen Kenntnisse und Fähigkeiten für die Annahme des Personenbezugs abzustellen ist. Der Streit darüber, ob der Personenbezug relativ oder absolut zu bestimmen ist, wird schon seit langer Zeit geführt.<sup>6</sup> Nach einem relativen Verständnis soll es auf die Kenntnisse und

\* Mehr über die Autoren erfahren Sie auf S. VIII.

1 AG Berlin-Mitte, 27. 3. 2007 – 5 C 314/06, K&R 2007, 600 ff.

2 LG Berlin, 31. 1. 2013 – 57 S 87/08, ZD 2013, 618 ff.

3 BGH, 28. 10. 2014 – VI ZR 135/13, K&R 2015, 106 ff.

4 Dies beinhaltet: Name der abgerufenen Seite/Datei; in Suchfelder eingegebene Begriffe; Zeitpunkt des Abrufs; übertragene Datenmenge; Meldung, ob Abruf erfolgreich war sowie IP-Adresse.

5 EuGH, 24. 11. 2011 – C-70/10, K&R 2012, 35, 38, Rn. 51 – Scarlet Extended.

6 Siehe nur *Bergt*, ZD 2015, 365 ff.; *Brink/Eckhardt*, ZD 2015, 205 ff.

Möglichkeiten der verantwortlichen Stelle selbst ankommen. Die Theorie des absoluten Personenbezugs stellt demgegenüber darauf ab, ob irgendjemand zur Herstellung des Personenbezugs imstande ist. Neben diesen beiden Extrempositionen hat sich zudem eine Reihe vermittelnder Auffassungen herausgebildet.

Zutreffend stellt der EuGH fest, dass Art. 2 lit. a) DSRL eine indirekte Identifizierbarkeit ausreichen lasse, weshalb eine Herstellung des Personenbezugs durch Verknüpfung mehrerer Informationen genüge. In ErwG 26 DSRL sieht er ein Indiz, dass auch die Kenntnisse Dritter grundsätzlich relevant sein können. Die entscheidende Frage hierbei ist laut EuGH, ob die Verknüpfung der IP-Adresse und des Zusatzwissens des ISP ein Mittel sei, das der Diensteanbieter vernünftigerweise einsetzen könne.<sup>7</sup> Dies soll dann nicht der Fall sein, wenn die Identifizierung gesetzlich verboten ist oder wegen unverhältnismäßigen Aufwandes praktisch nicht durchführbar wäre.<sup>8</sup> Der Diensteanbieter verfüge ausweislich des Vorlagebeschlusses des BGH über rechtliche Möglichkeiten zur Erlangung der Informationen vom ISP und somit über Mittel, die vernünftigerweise zur Identifizierung des Nutzers eingesetzt werden könnten.

#### b) Bewertung

Der EuGH lässt es für die Annahme eines vernünftigen Mittels genügen, wenn dem für die Verarbeitung Verantwortlichen abstrakt eine rechtliche Möglichkeit zur Verfügung steht, die notwendigen Informationen zu erlangen. ErwG 26 DSRL legt er also so aus, dass die Kenntnisse des Dritten insofern für die Bestimmung des Personenbezugs relevant sind, als sich der für die Verarbeitung Verantwortliche vernünftigerweise zwecks Herstellung des Personenbezugs an diesen wenden könne. Der EuGH vertritt folglich eine vermittelnde Ansicht, die primär auf die Möglichkeiten des für die Verarbeitung Verantwortlichen abstellt und dabei das erlangbare Wissen Dritter mitberücksichtigt. Naheliegend ist, dies als eine relative Ansicht des Personenbezugs zu bezeichnen, die um objektivierende Elemente ergänzt wird.<sup>9</sup>

Mit dem Wortlaut der DSRL lässt sich das Abstellen auf eine lediglich abstrakte Möglichkeit zwar vereinbaren.<sup>10</sup> Dies führt aber dazu, dass losgelöst vom Verarbeitungskontext immer von personenbezogenen Daten auszugehen ist, sobald theoretisch rechtliche Mittel die Erlangung von für die Identifizierung notwendigem Zusatzwissen gestatten. Daher spricht viel dafür IP-Adressen in der Praxis immer als personenbezogene Daten zu behandeln.<sup>11</sup>

Bedauerlich ist, dass der EuGH sich nicht mit der Frage beschäftigt hat, unter welchen Voraussetzungen im Zusammenhang mit der Erlangung von Zusatzwissen ein unverhältnismäßiger Aufwand vorliegt. Möglicher Anknüpfungspunkt einer solchen Prüfung ist einerseits der Aufwand für die Erlangung des Zusatzwissens und andererseits der Aufwand der Verknüpfung des Zusatzwissens mit den bereits vorhandenen Daten zwecks Identifizierung. Es erscheint zumindest denkbar, dass selbst bei Bestehen einer rechtlichen Möglichkeit zur Identifizierung, wie z. B. aufgrund von § 406 e StPO durch Akteneinsicht in einem Strafverfahren, der für die Rechtsdurchsetzung erforderliche Aufwand im Verhältnis zum Zweck als unverhältnismäßig anzusehen wäre. Die Relevanz des zweiten Aspekts hat der Generalanwalt grundsätzlich erkannt. So deutet er an, dass selbst bei erlangbarem Zusatzwissen ein unverhältnismäßiger Identifizierungsaufwand vorliegen

kann.<sup>12</sup> Er hält eine Klärung der Maßstäbe für die Bestimmung der „vernünftigen Mittel“ aber nicht für entscheidungserheblich. Unklar bleibt damit leider die Abgrenzung zu einer hypothetischen Möglichkeit der Identifizierung, die nicht für die Annahme eines Personenbezugs ausreicht.<sup>13</sup>

Der Streit, ob pseudonyme Daten personenbezogene Daten darstellen,<sup>14</sup> dürfte mit dieser Entscheidung zugunsten der Annahme eines Personenbezugs entschieden sein. So wird die Möglichkeit sich mit einem unter Pseudonym angelegten Facebook-Log-in auf Seiten anderer Anbieter anzumelden nicht zu einer Verneinung des Personenbezugs führen, weil die Möglichkeit einer Identifizierung mithilfe rechtlicher Mittel vorliegt. Ob vertragliche Regelungen zu einem Ausschluss des Personenbezugs führen können, ist fraglich, da gewährleistet sein muss, dass die Einhaltung der vertraglichen Geheimhaltungsbestimmungen dauerhaft besteht.<sup>15</sup>

## 2. Anwendbarkeit der DSRL

Bevor sich der EuGH der eigentlichen Frage der Vereinbarkeit von TMG mit DSRL widmet, beschäftigt er sich zunächst noch mit dem Anwendungsbereich der DSRL. So wäre nach Art. 3 Abs. 2 Gedankenstrich 1 DSRL die DSRL nicht anwendbar, wenn es sich bei Verarbeitung der IP-Adressen um Tätigkeiten des Staates im strafrechtlichen Bereich handelt.

Der EuGH stellt hier mit Verweisung auf Lindqvist<sup>16</sup> und Satamedia<sup>17</sup> fest, dass sämtliche der Beispiele aus Art. 3 Abs. 2 Gedankenstrich 1 DSRL originär staatliche Aufgaben sind und keine Überschneidung mit dem Handeln Einzelner aufweisen. Im konkreten Fall handele es sich zwar um eine Behörde, diese verfolge aber keine strafrechtlichen Tätigkeiten, sondern handele – vorbehaltlich einer noch ausstehenden Prüfung durch das vorliegende Gericht – wie ein Einzelner.

Deutlich wird hier, dass nicht nur bei der Verarbeitung eine absolut kleinteilige Prüfung einzelner Schritte und Zwecke erfolgen muss, sondern auch hinsichtlich des Anwendungsbereichs präzise geprüft werden muss.

## 3. Vereinbarkeit mit dem TMG

### a) Herleitung

Den Abschluss der Entscheidung bildet die Vereinbarkeit von §§ 12, 15 TMG mit Art. 7 lit. f) DSRL. Hierfür

7 Zur Frage der Zurechenbarkeit von Zusatzwissen siehe Haase, Datenschutzrechtliche Fragen des Personenbezugs, 2015, S. 289 ff.

8 Für die Berücksichtigung illegalen Handelns aber z. B. Art. 29-Datenschutzgruppe, WP 136, S. 22; Pahlen-Brandt, K&R 2008, 288, 289.

9 Eine ähnliche Ergänzung der strengen relativen Theorie wird von Karg, DuD 2015, 520, 525 als objektiviert relativer Ansatz bezeichnet; Specht/Müller-Riemenschneider, ZD 2014, 71, 74 nennen dies hingegen „beschränkt-objektive Theorie der Personenbeziehbarkeit“.

10 Siehe für die Bedeutung der Bestimmbarkeit als Vorliegen einer Möglichkeit: Art. 29-Datenschutzgruppe, WP 136, S. 14.

11 Zumal nicht ersichtlich ist, ob es sich um dynamische oder statische IP-Adressen handelt; vgl. Specht/Müller-Riemenschneider, ZD 2014, 71, 75.

12 Generalanwalt beim EuGH, 12. 5. 2016 – C-582/14, Rn. 61.

13 Vgl. Art. 29-Datenschutzgruppe, WP 136, S. 17.

14 Hierzu Karg, DuD 2015, 520, 524.

15 Zu dieser Problematik vgl. Dammann, in: Simitis BDSG, 8. Aufl. 2014, § 3 Rn. 27; siehe auch die umstrittene Änderung der AGB zwecks Datenabgleich zwischen WhatsApp und Facebook und die dazu ergangene Anordnung des HmbBfDI, <https://www.datenschutz-hamburg.de/news/detail/article/anordnung-gegen-massendatenabgleich-zwischen-whatsapp-und-facebook.html>.

16 EuGH, 6. 11. 2003 – C-101/01, K&R 2004, 26 ff. – Lindqvist.

17 EuGH, 16. 12. 2008 – C-73/07, K&R 2009, 102 ff. – Satamedia.

kommt der EuGH zunächst auf die vom BGH dargelegte vorherrschende Auslegung von § 15 Abs. 1 TMG zu sprechen.<sup>18</sup> Danach wird noch einmal der Tenor von ASNEF/FECEDM<sup>19</sup> dargelegt, also, dass keine neuen Grundsätze in Bezug auf die Zulässigkeit der Verarbeitung personenbezogener Daten eingeführt und auch die Tragweite der vorgesehenen Gründe nicht durch zusätzliche Bedingungen verändert werden dürfe. § 15 TMG in der engen Auslegung aber stünde einer Berücksichtigung des berechtigten Interesses der IT-Sicherheit entgegen und würde somit die Tragweite des Grundsatzes verengen. Zudem würde kategorisch die Verarbeitung bestimmter Kategorien personenbezogener Daten ohne die Möglichkeit einer Einzelfallabwägung ausgeschlossen. Folglich sei eine Norm wie § 15 TMG unvereinbar mit Art. 7 lit. f) DSRL.

#### b) Bewertung

Der EuGH räumt zwar ein, dass Art. 5 DSRL den Mitgliedsstaaten einen Ermessensspielraum für die Umsetzung von Art. 7 biete,<sup>20</sup> allerdings sei dieser Spielraum wiederum mit dem Ziel der DSRL gem. Art. 1 DSRL,<sup>21</sup> dem Gleichgewicht zwischen dem freien Verkehr personenbezogener Daten und dem Schutz der Privatsphäre, in Einklang zu bringen.<sup>22</sup> Auch hier wird das „Mantra“ aus ASNEF/FECEDM vorgetragen, allerdings ohne auf die wohl äußerst relevante Rn. 35 zu sprechen zu kommen. Diese differenziert gerade zwischen zusätzlichen Bedingungen zu einem Grundsatz, die verboten sind, und nationalen Maßnahmen, die einen Grundsatz näher bestimmen.<sup>23</sup>

Eine Begründung, wieso § 15 TMG eine engere Tragweite aufweist als Art. 7 lit. f) DSRL, bleibt der EuGH schuldig. Es bleibt weiter unklar, was eine zulässige Präzisierung im Rahmen von Art. 7 lit. f) und Art. 5 DSRL darstellt und was unabhängig von einer zusätzlichen Bedingung eine verbotene Änderung der Tragweite eines der Grundsätze aus Art. 7 DSRL ist. So scheint sich der EuGH in Rn. 62 endgültig aus der „Kleinteiligkeit“ des Datenschutzrechtes befreien zu wollen: Art. 7 lit. f) DSRL hindere einen Mitgliedsstaat daran, „kategorisch und ganz allgemein die Verarbeitung bestimmter Kategorien personenbezogener Daten auszuschließen, ohne Raum für eine Abwägung der im konkreten Einzelfall einander gegenüberstehenden Rechte und Interessen zu lassen“. Im Grunde muss also *jeder* Erlaubnistatbestand für die Verarbeitung personenbezogener Daten auch einen Auffangtatbestand aufweisen, der Raum für eine Einzelfallbetrachtung lässt.<sup>24</sup> Die Bundesregierung war offenbar zwar auch davon ausgegangen, dass § 15 Abs. 1 TMG für Zwecke der IT-Sicherheit nicht hinreichend ist, wollte diesem Mangel aber zunächst mit einem eigenen Erlaubnistatbestand begegnen.<sup>25</sup>

Auch scheint der Rekurs des EuGH auf Rn. 47 von ASNEF/FECEDM nicht zielführend. So ging es dort um eine bestimmte Kategorie von Daten, eben aus öffentlich zugänglichen Quellen. Andere Kategorien von Daten waren gar nicht erst dem berechtigten Interesse zugänglich. Wenn man dies nun auf § 15 TMG überträgt, müsste die Verarbeitung etwa von IP-Adressen, kategorisch ausgeschlossen sein. Dies ist mitnichten der Fall. So können IP-Adressen gem. § 15 Abs. 1 TMG erhoben werden. Sie sind aber nach der Inanspruchnahme des Dienstes, außer in Fällen von § 15 Abs. 4 TMG, zu löschen. In Rn. 63 soll es dann aber wieder um einen

unberücksichtigten Zweck und keine Kategorie von Daten gehen. Ob sich Breyer so hinreichend von ASNEF/FECEDM abgrenzen lässt, ist schwer zu sagen. Hier hätte der EuGH weiter ausholen müssen.

Die allgemeine Herleitung des EuGH ergibt sich daraus, dass dort, wo ein berechtigtes Interesse bestehen könnte, dies auch notwendigerweise berücksichtigungsfähig sein muss. Das man hierfür den „Umweg“ einer Norm gehen und derweilen europarechtskonform auslegen könnte, scheint der EuGH gar nicht erst zu erwägen. Stichhaltiger wäre es für den nationalen Gesetzgeber also, Regelbeispiele vorzugeben und eine reduzierte Generalklausel vorzusehen.<sup>26</sup>

So hält der EuGH fest, dass eine Regelung wie § 15 TMG (in enger Auslegung des BGH) mit Art. 7 lit. f) DSRL unvereinbar wäre. Damit hat der EuGH allerdings nicht über die weite Auslegung entschieden.<sup>27</sup> Man könnte überlegen, ob die Vorlage gem. Art. 267 Abs. 2 AEUV bei einer weiten Auslegung überhaupt notwendig war.<sup>28</sup> Zudem stellt sich die Frage, ob die weite Auslegung von § 15 Abs. 1 TMG überhaupt möglich ist,<sup>29</sup> insbesondere im Hinblick auf § 15 Abs. 8 TMG. Über die Auslegung einer nationalen Norm kann der EuGH allerdings im Rahmen von Art. 267 AEUV nicht entscheiden, da es dort um die Auslegung von Unionsrecht geht.<sup>30</sup>

#### IV. Handwerkliches

Die Entscheidung gibt, abseits der bereits besprochenen Probleme, Grund zu einer kritischen Evaluation. So ist die Verwechslung der verwaltungsgerichtlichen mit der ordentlichen Gerichtsbarkeit der offensichtlichste Missstand.<sup>31</sup> Insgesamt wirkt die Behandlung essentieller Probleme des Datenschutzrechts, selbst bei einer prägnanten Herangehensweise, zu kurz, auch im Hinblick auf die knapp fünf Monate<sup>32</sup> zwischen den Schlussanträgen und der Entscheidung.<sup>33</sup> Sprachlich sorgen die unterschiedlichen Übersetzungen für Verwirrung, wie ein Berichtigungsantrag der Klägerseite zeigt.<sup>34</sup> Prüfungsökonomisch verwundert die späte Prüfung des Anwendungsbereichs der DSRL. Bei fehlender Anwendbarkeit der DSRL wäre

18 Vgl. etwa *Spindler/Nink*, in: Spindler/Schuster, TMG, 3. Aufl. 2015, § 15 Rn. 6; *Geminn/Richter*, in: Roßnagel, Europäische Datenschutz-Grundverordnung, 2017, § 4 Rn. 293.

19 EuGH, 24. 11. 2011 – C-468/10, C-469/10, K&R 2012, 40 ff. – ASNEF/FECEDM.

20 Insofern scheint auch das „nach Maßgabe“ in Art. 5 DSRL unproblematisch.

21 Den Artikel erwähnt der EuGH nicht explizit (Rn. 58).

22 Vgl. auch *Brühann*, EuZW 2009, 639, 642 f.

23 Vgl. zur Flexibilität auch EuGH, 6. 11. 2003 – C-101/01, EuR 2004, 291, 303 (Rn. 83) – Lindqvist.

24 Als Korrektiv bei dem Betroffenen soll hingegen das Widerspruchsrecht dienen *Brühann*, in: Nettesheim/Wolf, Grabitz/Hilf, Das Recht der Europäischen Union, 40. EL 2009, A30 RL 95/46/EG Art. 14 Rn. 7.

25 BT-Drs. 16/12225, S. 4 f.; zur Aufgabe der Umsetzung BT-Drs. 16/13259, S. 8.

26 Vgl. „die Leitlinien“: EuGH, 24. 11. 2011 – C-468/10, C-469/10, K&R 2012, 40, 42, Rn. 46 – ASNEF/FECEDM.

27 *Meyerdierks/Gendele*, ZD 2013, 626 ff.

28 Insofern verwunderlich: BGH, 28. 10. 2014 – VI ZR 135/13, K&R 2015, 106, 110, Rn. 44; vgl. auch Generalanwalt beim EuGH, 12. 5. 2016 – C-582/14, Rn. 94.

29 *Schmitz*, in Hoeren/Holznapel/Sieber, Multimedia-Recht, 42. EL 2015, Teil 16.2 Rn. 247.

30 *Ehricke*, in: Streinz, EUV/AEUV, 2. Aufl. 2012, Art. 267 Rn. 14.

31 EuGH, 19. 10. 2016 – C-582/14, K&R 2016, 811 ff., Rn. 17.

32 Bei Schrems waren es bei der doppelten Menge Randnummern knapp zwei Wochen.

33 Art. 7 lit. f) DSRL wird in 10 Randnummern abgehandelt.

34 [http://www.daten-speicherung.de/wp-content/uploads/Surfprotokollierung\\_2016-10-25\\_Berichtigungsantr\\_K1.pdf](http://www.daten-speicherung.de/wp-content/uploads/Surfprotokollierung_2016-10-25_Berichtigungsantr_K1.pdf).

zudem nicht der Rahmenbeschluss 2008/977/JI, sondern das nationale Recht mit der Definition des Personenbezugs aus § 3 Abs. 1 BDSG anwendbar gewesen.

Zu kurz greift letztlich auch die Beschränkung des Dritten auf den ISP. Zwar hatte der BGH diesen als konkretes Beispiel angeführt, die Vorlage war allerdings nicht auf diesen reduziert.<sup>35</sup>

## V. Konsequenzen

Eine unmittelbare Reaktion des Gesetzgebers im Hinblick auf §§ 11 ff. TMG ist nicht abzusehen. Hierzu müsste er sich neben § 15 TMG auch §§ 12, 14 TMG vornehmen. In Anbetracht des Geltungsbeginns der Datenschutzgrundverordnung (DSGVO) ab Mai 2018 und der ausstehenden Bundestagswahl wird § 15 TMG bis dahin wohl europarechtskonform auszulegen sein.<sup>36</sup> Dass andere Normen wie §§ 100 Abs. 1, 2 TKG und §§ 28 a, 28 b BDSG, die ähnlich betroffen sind,<sup>37</sup> überarbeitet werden, ist ebenso unwahrscheinlich. Hier wird wohl erst mit dem ABDSG eine „Flurbereinigung“ kommen.

## VI. Ausblick DSGVO

### 1. Personenbezug

Die DSGVO definiert den Begriff der personenbezogenen Daten im Wesentlichen wie die DSRL. Art. 4 Nr. 1 DSGVO enthält lediglich geringe Änderungen des Wortlauts. In ErwG 26 DSGVO findet sich nun die Formulierung, dass für die Frage, ob eine Person identifizierbar ist, alle Mittel berücksichtigt werden sollen, „die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden“. Dass nunmehr auf ein „allgemeines Ermessen“ anstatt auf „vernünftigerweise einsetzbare Mittel“ abgestellt wird, lässt keine Maßstabsveränderung erkennen und soll ausweislich der englischen Sprachfassung der DSRL und der DSGVO auch keine Änderung herbeiführen. Als Möglichkeit für eine Identifizierbarkeit nennt die DSGVO die Zuordnung zu einer Online-Kennung, wozu IP-Adressen gem. ErwG 30 DSGVO gehören.

Bemerkenswert ist, dass die DSGVO in ErwG 26 das Aussondern als Mittel zur Identifizierung einer Person nennt.<sup>38</sup> Ziel dieser Bestimmung ist, dass die durch technische Mittel wie z. B. IP-Adressen, Browser Fingerprints und Cookies erzeugten Nutzerprofile als personenbezogen anzusehen sind, obwohl der Name des Betroffenen dem Verantwortlichen nicht bekannt ist.<sup>39</sup> Insgesamt scheint die DSGVO den veränderten technischen Möglichkeiten der Identifizierung durch die Berücksichtigung von Online-Kennungen daher besser Rechnung zu tragen als die DSRL.<sup>40</sup>

Der Wortlaut der DSGVO steht einer Übertragung der vom EuGH entwickelten Formel zur Bestimmung des Personenbezugs nicht entgegen. Gleichwohl ist davon auszugehen, dass über diese Frage weiterhin gestritten werden wird, da nach dem Wortlaut auch ein extensiveres Verständnis möglich ist.

### 2. Berechtigtes Interesse

Die DSGVO bedarf als Verordnung gem. Art. 288 Abs. 2 AEUV keiner weiteren Umsetzung durch die Mitgliedsstaaten. Folglich ist die DSGVO qua Rechtsinstrument schon nicht konkretisierungsfähig. Zudem gibt es auch

keine dem Art. 5 DSRL entsprechende Norm, die die Rechtmäßigkeit der Verarbeitung näher konkretisieren lässt. Die explizite Öffnungsklausel des Art. 6 Abs. 2 DSGVO enthält nur anderweitige rechtliche Verpflichtungen (lit. c) und öffentliche Aufgaben (lit. e) sowie besondere Verarbeitungssituationen nach Kapitel IX. Während die DSRL noch eine nähere Konkretisierung erlauben sollte,<sup>41</sup> ist bei der DSGVO eine solche, trotz entsprechender Erwägungen seitens des Berichterstatters im Parlament, nicht vorgesehen.<sup>42</sup> Das (datenschutzrechtliche) TMG wird also in weiten Teilen entfallen.<sup>43</sup>

Zur näheren Konkretisierung des berechtigten Interesses nach Art. 6 Abs. 1 lit. f) DSGVO finden sich nur vereinzelte Hilfestellungen in den ErwG 47 bis 49. Diese haben aber, trotz aller Ausführlichkeit, eine ähnlich geringe Signalwirkung für die Verarbeitungspraxis wie etwa Working Paper der Art. 29-Datenschutzgruppe.<sup>44</sup> Eine völlig freie Abwägung scheint aber ein unüberschaubares Maß an Rechtsunsicherheit für Verarbeiter wie Betroffene zu schaffen. Daneben sollte auch der damit verbundene Aufwand für die ohnehin chronisch überlasteten Aufsichtsbehörden nicht vernachlässigt werden. Möglicherweise kann diesem in Grenzen durch Verhaltensregeln gem. Art. 40 Abs. 2 lit. b) DSGVO begegnet werden.<sup>45</sup>

Denkbar, aber mit der zukünftigen Rechtslage aus Art. 6 DSGVO nicht vereinbar, scheint auch ein an die AGB-Kontrolle im BGB angelehntes System. So würde nicht die Unwirksamkeit einzelner Vertragsklauseln vorgegeben, sondern bestimmte Verarbeitungssituationen würden erlaubt. Dies könnte auch mit dem System einer schwarzen und grauen Liste sowie einer allgemeinen (Auf-fang-)Klausel verbunden werden. So wäre zum einen das berechtigte Interesse hinreichend berücksichtigt, andererseits ausreichend Rechtssicherheit geschaffen. Je nachdem, wie der legislative Prozess ausgestaltet würde, denkbar wäre etwa ein delegierter Rechtsakt verbunden mit einem Mitspracherecht des Europäischen Datenschutzausschusses, wären auch im Hinblick auf die Technologie-neutralität<sup>46</sup> keine Probleme zu erwarten.

35 BGH, 28. 10. 2014 – VI ZR 135/13, K&R 2015, 106, 108, Rn. 26.

36 Mögliche Ansätze für eine zwischenzeitliche Anpassung des TMG: Marosi, DSRITB 2016, 435, 443 f.

37 Siehe Drewes, ZD 2012, 115 ff.

38 Siehe hierzu *Borgesius*, CLSR 2016, 256 ff.

39 *Albrecht/Jotzo*, Das neue Datenschutzrecht der EU, 2017, Teil 3 Rn. 3.

40 So kann sogar der Batterieladestand einem Nutzer eindeutig zugeordnet werden: <http://www.heise.de/newsticker/meldung/Datenschutzbedenken-Mozilla-entfernt-Akku-Fingerprinting-aus-Firefox-3405099.html>; siehe auch *Bertermann*, K&R 2015, 110, 111; *Mantz*, ZD 2013, 625, 625 f.

41 So BT-Drs. 12/8329, S. 17; ErwG 30 DSRL; *Brühmann*, in: *Nettesheim/Wolf* (Fn. 24), A30 RL 95/46/EG Art. 7 Rn. 21; vgl. auch Kommission in Generalanwalt beim EuGH, 12. 5. 2016 – C-582/14, Rn. 43 f.

42 *Albrecht/Jotzo*, (Fn. 39), Teil 3 Rn. 50 f.

43 *Geminn/Richter*, in: *Roßnagel* (Fn. 18), § 4 Rn. 268 ff.

44 Die gerichtliche Berücksichtigung sei hier im Hinblick auf die Zahl der tatsächlichen Verfahren mal dahingestellt.

45 Hierzu *Bergt*, DSRITB 2016, 483 ff.

46 Siehe hierzu *Roßnagel/Geminn/Jandt/Richter*, *Datenschutzrecht* 2016, 2016, S. XVII f.

#### Hinweise der Redaktion:

Siehe auch die Beitragsserie von *Piltz* zur EU-Datenschutz-Grundverordnung in K&R 2016, 557 ff., 629 ff., 709 ff. und 777 ff. sowie die Beiträge von *Voigt*, „Gesichtserkennung zu Werbezwecken – Erfolgt ein User Tracking bald auch offline?“, K&R 2016, 456 ff. und *Wilmer*, „Wearables und Datenschutz – Gesetze von gestern für die Technik von morgen?“, K&R 2016, 382 ff.