www.jusletter-it.eu

Maurits Haas

Sind dynamische IP-Adressen personenbezogene Daten?

Anmerkungen zu den Schlussanträgen des Generalanwalts Sánchez-Bordona zum Verfahren des EuGH C-582/14

By answering the request for preliminary ruling, whether dynamic IP addresses constitute personal data, the European Court of Justice may give a landmark decision on the contentious issue, in which case data have to be considered as personal data. Advocate General Sánchez-Bordona follows a subjective approach, according to which the resources of the controller shall be decisive to determine the scope. But due to the fact that all the means, which the controller could possibly use to identify a person shall be attributable to the controller, the scope of data protection law is still very broad.

Category: Articles
Region: Austria
Field of law: Data Protection

Citation: Maurits Haas, Sind dynamische IP-Adressen personenbezogene Daten?, in: Jusletter IT 22 September 2016

ISSN 1664-848X, http://jusletter-it.weblaw.ch, Weblaw AG, info@weblaw.ch, T +41 31 380 57 77

Inhaltsübersicht

I. Ausgangslage
1. IP-Adressen
2. Der Meinungsstand zum Personenbezug von IP-Adressen
a) Die Artikel 29-Datenschutzgruppe
b) Die Rechtslage in Österreich
c) Die Rechtslage in Deutschland
II. Das Verfahren EuGH C-582/14
1. Sachverhalt
2. Die Schlussanträge des Generalanwalts
a) Objektiver oder relativer Ansatz
b) Mittel zur Bestimmung eines Betroffenen
3. Auskunftsansprüche gegenüber dem Internetzugangsanbieter
a) Österreich
b) Deutschland
4. Zwischenfazit
III. Ausblick
1. Datenschutzgrundverordnung
2. Technische Entwicklungen
a) IPv6
b) Das Internet der Dinge
c) Big Data
IV. Fazit

I. Ausgangslage

[Rz 1] Am 12. Mai 2016 legte Generalanwalt Sánchez-Bordona dem Europäischen Gerichtshof seine Schlussanträge zu der Frage vor, ob eine dynamische IP-Adresse, mit der auf die Internetseite einer öffentlichen Stelle zugegriffen wird, für diese personenbezogene Daten darstellen, wenn der Internetzugangsanbieter über das zur Identifizierung des Betroffenen erforderliche Zusatzwissen verfügt. Diese Vorlagefrage ist über den konkreten Anlassfall hinaus von besonderem Interesse, da der EuGH damit über die grundsätzliche Frage des Datenschutzrechtes entscheiden könnte, wann Daten als personenbezogen anzusehen sind: Nach der relativen Methode, auf Grundlage des Wissens des für die Verarbeitung Verantwortlichen, oder nach der objektiven Methode, wenn dem für die Verarbeitung Verantwortlichen oder auch einem Dritten die Bestimmung des Betroffenen möglich ist.

1. IP-Adressen

[Rz 2] Internetprotokoll (IP)-Adressen dienen der Identifizierung eines Geräts in Computernetzwerken, die auf dem Internetprotokoll basieren. Die Adressierung ermöglicht den Geräten, Datenpakete auszutauschen und somit zu kommunizieren. So werden z.B. bei jedem Abruf einer Website IP-Adressen benötigt. Wenn man eine Internetadresse (www.name.com) eingibt, wird diese von einem Domain Name System (DNS)-Server in die zugehörige IP-Adresse übersetzt.[1] Das anfragende Gerät fordert von der IP-Adresse der Website die Übersendung von Daten an, der

[1] Vgl. http://www.itwissen.info/definition/lexikon/domain-name-system-DNS-DNS-System.html (alle angegebenen Websites zuletzt abgerufen am 11. September 2016).

Server der Website weiß anhand der vom anfragenden Gerät verwendeten IP-Adresse, wohin die Daten zu senden sind.

[Rz 3] In der zurzeit noch überwiegend genutzten Version 4 des Internet Protokolls (IPv4) werden 32-Bit-Adressen verwendet.[2] Damit ist die Darstellung von ca. 4,3 Milliarden verschiedenen Adressen möglich. Die Zuordnung der Geräte im Netzwerk muss eindeutig, d.h. z.B. einmalig im gesamten Internet, sein. Es war frühzeitig erkennbar, dass die Anzahl von IPv4-Adressen nicht ausreichen wird, da nicht einmal für jeden Menschen ein Gerät direkt an das Internet angeschlossen werden könnte. Aus diesem Grund wurde eine Umstellung auf die Version 6 des Internet Protokolls (IPv6) beschlossen, die 128-Bit-Adressen verwendet, mit denen die Darstellung von 2^{128} (ca. 340 Sextillionen) Adressen möglich ist.

[Rz 4] Um der Knappheit von IPv4-Adressen zu entgehen, vergeben Internetzugangsanbieter in den meisten Fällen keine statischen, sondern dynamische IP-Adressen. Statische IP-Adressen sind fest zugeordnete, sich nicht ändernde IP-Adressen. Bei jeder Einwahl des Geräts wird diesem dieselbe IP-Adresse zugewiesen. Statische IP-Adressen werden häufig von Unternehmen verwendet, können aber auch natürlichen Personen zugewiesen sein. Dynamische IP-Adressen hingegen werden bei jedem Einwahlvorgang eines Geräts ins Internet neu vergeben und wechseln zumeist darüber hinaus alle 24 Stunden. Da in der Regel nicht alle Kunden eines Internetzugangsanbieters gleichzeitig Zugang zum Internet wünschen, können IP-Adressen auf diese Art effizienter vergeben werden.

[Rz 5] Eine weitere Form, der Knappheit von IPv4-Adressen zu begegnen, ist die Network Address Translation (NAT). Dabei werden interne IPv4-Adressen, die von Geräten in einem privaten Netzwerk verwendet werden, durch die NAT einer öffentlichen IP-Adresse zugeordnet, womit die Geräte aus dem privaten Netzwerk in der Lage sind, mit Geräten aus dem öffentlichen Netzwerk zu kommunizieren. Das bekannteste Beispiel ist wohl der WLAN-Router, der allen Geräten des WLAN Zugang zum Internet bietet. Findet die Adressen-Übersetzung dynamisch statt,[3] ist jedem Gerät des lokalen Netzwerks in der Folge dieselbe öffentliche IP-Adresse zugeordnet. Die NAT kann aber auch bereits vom Internetzugangsanbieter vorgenommen werden (Large Scale NAT), sodass schon den Kunden keine öffentlichen IPv4-Adressen sondern private IPv4-Adressen des Internetzugangsanbieters zugewiesen werden. Beim Kunden kann eine zweite NAT stattfinden, wenn dieser mehrere Geräte seines privaten Netzwerks über die private IPv4-Adresse des Internetzugangsanbieters kommunizieren lässt. Durch die Network Address Translation ist es also nicht notwendig, jedem Gerät, das im Internet kommunizieren möchte, eine eigene öffentliche IP-Adresse zuzuweisen. Vielmehr teilen sich durch die NAT mehrere Geräte eine öffentliche IP-Adresse.

---

2 Vgl. https://www.iana.org/numbers.

3 Dazu wird die Port Adress Translation (PAT) verwendet, d.h. bei jeder Anfrage wird ein unterschiedlicher Quellport zugeteilt, um weiterhin eine eindeutige Adressierung von Anfrage und Antwort trotz gleicher IP-Adresse der verschiedenen Geräte zu ermöglichen. Vgl. http://de.ccm.net/contents/539-nat-adressenumsetzung.

2. Der Meinungsstand zum Personenbezug von IP-Adressen

[Rz 6] Personenbezogene Daten sind gemäß Art. 2 lit. a) der EU-Richtlinie 95/46/EG[4] (Datenschutzrichtlinie) «*alle Informationen über eine bestimmte oder bestimmbare natürliche Person; als bestimmbar wird eine Person angesehen, die direkt oder indirekt identifiziert werden kann, insbesondere durch Zuordnung zu einer Kennnummer oder zu einem oder mehreren spezifischen Elementen, die Ausdruck ihrer physischen, physiologischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität sind*». Auch nach dem im Einklang mit der Richtlinie erlassenen Datenschutzgesetz 2000 (DSG) und dem deutschen Bundesdatenschutzgesetz (BDSG) liegen personenbezogene Daten dann vor, wenn ein Betroffener bestimmt oder bestimmbar ist.[5] Erwägungsgrund 26 der Datenschutzrichtlinie konkretisiert: «*Bei der Entscheidung, ob eine Person bestimmbar ist, sollten alle Mittel berücksichtigt werden, die vernünftigerweise entweder von dem Verantwortlichen für die Verarbeitung oder von einem Dritten eingesetzt werden könnten, um die betreffende Person zu bestimmen.*»

[Rz 7] In Anbetracht dieser Rechtslage herrscht weitestgehend Einigkeit darüber, dass statische IP-Adressen personenbezogene Daten sind, wenn diese einer natürlichen Person zugeordnet sind, weil die immer gleiche numerische Zahl einer Person zugeordnet ist, welche durch eine WHOIS-Abfrage zu eruieren ist.[6] Ebenfalls unstrittig ist der Personenbezug von dynamischen IP-Adressen beim Internetzugangsanbieter, der die Adressen zuteilt und aufgrund des Vertrages mit dem Kunden weiß, welcher Person ein Anschluss zugeordnet ist.[7] Für Websitebetreiber sind dynamische IP-Adressen jedenfalls dann personenbezogene Daten, wenn sich der Nutzer durch einen Login mit personenbezogenen Daten identifiziert.[8]

[Rz 8] Hinsichtlich der Frage, ob dynamische IP-Adressen für einen Websitebetreiber personenbezogene Daten darstellen, wenn der Internetzugangsanbieter über das zur Identifizierung der betroffenen Person erforderliche Zusatzwissen verfügt, können nur dynamische IP-Adressen in Kombination mit einer zeitlichen Zuordnung gemeint sein, da ohne einen Zeitstempel die Zuordnung zu einer Person jedenfalls nicht möglich wäre. Es ist unstrittig, dass dynamische IP-Adressen beim Websitebetreiber keine Daten über eine «bestimmte» Person darstellen.[9] Es kommt also darauf an, ob durch die dynamische IP-Adresse eine Person «bestimmbar» ist.

a) Die Artikel 29-Datenschutzgruppe

[Rz 9] Die Artikel 29-Datenschutzgruppe bewertet dynamische IP-Adressen als Daten, die sich auf eine bestimmbare Person beziehen. Sie führt aus, es sei Internetzugangsanbietern und Ver-

---

4 Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. L 281 vom 23. November 1995, S. 31–50.

5 Vgl. § 4 Z 1 DSG und § 3 Abs. 1 BDSG.

6 Vgl. u.a. Ulrich Sachs, Datenschutzrechtliche Bestimmbarkeit von IP-Adressen, CR 8/2010, 548. Niko Härting, Datenschutz im Internet, CR 11/2008, 745. Jens Eckhardt, IP-Adressen als personenbezogenes Datum – neues Öl in Feuer, CR 5/2011, 340. Patrick Breyer, Personenbezug von IP-Adressen, ZD 8/2014, 400. Anderer Ansicht: Jan K. Köcher, Personenbezug von IP-Adressen: Ein Streitfall an der Nahstelle zwischen Persönlichkeit und Informationsgesellschaft, PIK 12/2010, 206 f.

7 Urteil des EuGH C-461/10 vom 19. April 2012, *Bonnier Audio*, Rz 52. Urteil des OGH 4 Ob 41/09x vom 14. Juli 2009.

8 Vgl. u.a. Mathias Bergt, Die Bestimmbarkeit als Grundproblem des Datenschutzrechts, ZD 8/2015, 370. Breyer (Fn. 6), ZD 8/2014, 401.

9 Vgl. Schlussanträge des Generalanwalts vom 12. Mai 2016 zu Urteil des EuGH C-582/14, *Breyer*, Rz 56.

waltern lokaler Netzwerke ohne großen Aufwand möglich, Internet-Nutzer zu identifizieren. Für Websitebetreiber gelte, dass der für die Verarbeitung Verantwortliche insbesondere dann vom Vorhandensein der Mittel ausgehe, die zur Identifizierung der betreffenden Personen vernünftigerweise eingesetzt werden könnten, wenn der Zweck der Verarbeitung der IP-Adressen in der Identifizierung von Computer-Nutzern bestehe.[10]

[Rz 10] Eine Ausnahme sieht die Artikel 29-Datenschutzgruppe in Fällen, in denen IP-Adressen aus technischen oder organisatorischen Gründen keine Identifizierung des Nutzers zulassen. Dies gelte z.B. für IP-Adressen, die einem Computer in einem Internet-Café zugewiesen seien, in dem keine Identifizierung der Kunden gefordert werde. Auch in diesem Fall seien die IP-Adressen aber wie personenbezogene Daten zu behandeln, wenn der Websitebetreiber nicht mit Sicherheit erkennen könne, dass die Daten zu nicht bestimmbaren Benutzern gehören.[11]

b) Die Rechtslage in Österreich

[Rz 11] Der Begriff «öffentliche IP-Adresse» wird in § 92 Abs. 3 Z 16 des Telekommunikationsgesetzes 2003 (TKG) definiert als «*einmalige numerische Adresse aus einem Adressblock, der durch die Internet Assigned Numbers Authority (IANA) oder durch eine regionale Vergabestelle einem Anbieter eines Internet-Zugangsdienstes zur Zuteilung von Adressen an seine Kunden zugewiesen wurde, die einen Rechner im Internet eindeutig identifiziert und im Internet geroutet werden kann*». Öffentliche IP-Adressen sind gemäß § 92 Abs. 3 Z 16 TKG Zugangsdaten[12] und somit eine besondere Art der Verkehrsdaten[13]. Ist eine öffentliche IP-Adresse einem Teilnehmer für die Dauer des Vertrages zur ausschließlichen Nutzung zugewiesen, handelt es sich zugleich um Stammdaten[14]. Die datenschutzrechtlichen Bestimmungen des TKG gelten für die Verarbeitung und Übermittlung von personenbezogenen Daten in Verbindung mit der Bereitstellung öffentlicher Kommunikationsdienste in öffentlichen Kommunikationsnetzen.[15] Die Rechtslage für Internetzugangsanbieter ist somit eindeutig.[16]

[Rz 12] Die Frage, ob IP-Adressen für einen Websitebetreiber personenbezogene Daten darstellen, wurde in Österreich eindeutig beantwortet. Die Datenschutzkommission sprach aus, dass IP-Adressen für einen Dritten jedenfalls «bestimmbare» und damit personenbezogene Daten darstellen, wenn der Zweck der Speicherung nicht eindeutig jegliche Identifizierungsabsicht aus-

10 Artikel 29-Datenschutzgruppe, WP 136, Stellungnahme 4/2007 zum Begriff «personenbezogene Daten», 19.

11 Artikel 29-Datenschutzgruppe, WP 136, Stellungnahme 4/2007 zum Begriff «personenbezogene Daten», 20.

12 Vgl. Urteil des OGH 4 Ob 41/09x vom 14. Juli 2009. «Zugangsdaten» sind jene Verkehrsdaten, die beim Zugang eines Teilnehmers zu einem öffentlichen Kommunikationsnetz beim Betreiber entstehen und für die Zuordnung der zu einem bestimmten Zeitpunkt für eine Kommunikation verwendeten Netzwerkadressierung zum Teilnehmer notwendig sind (§ 93 Abs. 3 Z 4a TKG).

13 «Verkehrsdaten» sind Daten, die zum Zwecke der Weiterleitung einer Nachricht an ein Kommunikationsnetz oder zum Zwecke der Fakturierung dieses Vorgangs verarbeitet werden (§ 93 Abs. 3 Z 4 TKG).

14 «Stammdaten» sind alle personenbezogenen Daten, die für die Begründung, die Abwicklung, Änderung oder Beendigung der Rechtsbeziehungen zwischen dem Benutzer und dem Anbieter oder zur Erstellung und Herausgabe von Teilnehmerverzeichnissen erforderlich sind; dies sind: a) Name, b) akademischer Grad, c) Anschrift, d) Teilnehmernummer und sonstige Kontaktinformationen für die Nachricht, e) Informationen über Art und Inhalt des Vertragsverhältnisses, f) Bonität (§ 93 Abs. 3 Z 3 TKG).

15 § 93 Abs. 1 TKG.

16 Der OGH hatte in der Entscheidung 11 Os 57/05z vom 26. Juli 2005 ausgesprochen, bei einer Auskunftserteilung durch den Internetzugangsanbieter über dynamische IP-Adressen liege lediglich eine Verarbeitung von Stammdaten vor. In der Entscheidung 4 Ob 41/09x vom 14. Juli 2009 revidierte er diese Ansicht dahingehend, dass zur Auskunftserteilung über Stammdaten zunächst Verkehrsdaten verarbeitet werden müssen.

schließe.[17] Werde die Identifizierungsabsicht ausgeschlossen, lägen «indirekt personenbezogene Daten»[18] vor. Bereits zuvor hatte die DSK in einer Empfehlung die von einer Leistungsverwertungsgesellschaft ermittelten dynamischen IP-Adressen als personenbezogene Daten angesehen.[19] Begründet wurde diese Ansicht im Wesentlichen damit, dass eine Identifizierung der Nutzer mittels IP-Adresse in dem vorliegenden Fall tatsächlich stattgefunden habe,[20] weshalb die Betroffenen «bestimmbar» gewesen seien. Auch der Rechtsprechung des Verfassungsgerichtshofes lässt sich entnehmen, dass er dynamische IP-Adressen als personenbezogene Daten qualifiziert.[21]

c) Die Rechtslage in Deutschland

[Rz 13] In Deutschland wird die Frage nach dem Personenbezug von IP-Adressen seit geraumer Zeit diskutiert. Dabei dient dieses Thema als Kristallisationspunkt für die grundsätzliche Frage des Datenschutzrechts, wann überhaupt personenbezogene Daten vorliegen. In der Lehre wurden in diesem Zusammenhang unterschiedliche Theorien zur «Bestimmbarkeit» einer Person aufgestellt. Nach dem Ansatz des relativen Personenbezugs ist eine Person als bestimmbar anzusehen, wenn eine Identifizierung mit den Mitteln des für die Verarbeitung Verantwortlichen ohne unverhältnismäßigen Aufwand durchgeführt werden kann.[22] Der Ansatz des objektiven Personenbezugs hält demgegenüber eine Person bereits dann für bestimmbar, wenn ein Dritter über das nötige Wissen verfügt, um die Person zu identifizieren, selbst wenn der Dritte dieses Wissen noch nicht mit dem für die Verarbeitung Verantwortlichen geteilt hat.[23] Dementsprechend sind dynamische IP-Adressen, die vom Internetzugangsanbieter einem Anschluss zugeordnet werden können, nach dem objektiven Ansatz auch für einen Websitebetreiber personenbezogene Daten, nach dem relativen Ansatz hingegen nicht.[24] Die gegensätzlichen Positionen finden sich nicht nur in der Lehre, sondern auch in der Rechtsprechung.[25] Der Bundesgerichtshof ersuchte schließlich den EuGH um Vorabentscheidung.[26]

---

17 Entscheid der Datenschutzkommission K121.358/0009-DSK/2008 vom 20. Juni 2008.

18 § 4 Z 1 DSG: «Nur indirekt personenbezogen» sind Daten für einen Auftraggeber, Dienstleister oder Empfänger einer Übermittlung dann, wenn der Personenbezug der Daten derart ist, dass dieser Auftraggeber, Dienstleister oder Übermittlungsempfänger die Identität der Betroffenen mit rechtlich zulässigen Mitteln nicht bestimmen kann.»

19 Entscheid der Datenschutzkommission K213.000/0005-DSK/2006 vom 29. September 2006.

20 Die Identifizierung war aufgrund eines gerichtlichen Beschlusses zur Bekanntgabe, wem die dynamische IP-Adresse zum fraglichen Zeitpunkt zugeordnet war, wegen des Verdachts eines Verstoßes gegen § 91 Abs. 1 UrhG und der tatsächlichen Speicherung der IP-Adressen beim Internetzugangsanbieter möglich. Letzteres wurde von der DSK als unzulässige Speicherung von Verkehrsdaten gewertet.

21 Urteil des VfGH B 1031/11 vom 29. Juni 2012. Vgl. dazu auch Michael Kalteis, Polizeiliche Ermittlungen von IP-Adressen nur mit richterlicher Genehmigung?, ZfV 2013/246.

22 Vgl. Jens Eckhardt/Stefan Brink, Wann ist ein Datum ein personenbezogenes Datum?, ZD 5/2015, 205f m.w.N. Bergt (Fn. 8), ZD 8/2015, 365 ff. m.w.N.

23 Vgl. Eckhardt/Brink (Fn. 22), ZD 5/2015, 205 f. m.w.N. Bergt (Fn. 8), ZD 8/2015, 365 ff. m.w.N.

24 Vgl. Beschluss des BGH VI ZR 135/13 vom 28. Oktober 2014, Rz 42 f.

25 Für einen Personenbezug dynamischer IP-Adressen: Urteil des AG Berlin-Mitte 5 C 314/06 vom 27. März 2007. Gegen einen Personenbezug dynamischer IP-Adressen: Urteil des AG München 133 C 5677/08 vom 30. September 2008; Urteil des LG Wuppertal 25 Qs 10 Js 1977/08-177/10 vom 19. Oktober 2010; Urteil des OLG München 6 W 496/11 vom 4. Juli 2011; Urteil des OLG Hamburg 5W 126/10 vom 3. November 2010.

26 Beschluss des BGH VI ZR 135/13 vom 28. Oktober 2014.

II. Das Verfahren EuGH C-582/14

1. Sachverhalt

[Rz 14] Der Kläger macht einen Unterlassungsanspruch gegen die Bundesrepublik Deutschland geltend, mit dem er die Unterlassung der Speicherung seiner IP-Adresse über das Ende des Abrufs einer Website der Beklagten hinaus erwirken möchte, soweit die Speicherung nicht im Störungsfall zur Wiederherstellung der Seite erforderlich ist. Die von Einrichtungen der Beklagten bereitgestellten Websites erfassen Namen der abgerufenen Dateien bzw. Seiten, in Suchfelder eingegebene Begriffe, den Zeitpunkt des Abrufs, die übertragene Datenmenge, Informationen über den Erfolg des Abrufs und die IP-Adresse des zugreifenden Rechners. Diese Daten werden über den jeweiligen Nutzungsvorgang hinaus zum Zweck der Abwehr von Angriffen und zur strafrechtlichen Verfolgung von Angreifern gespeichert.[27] Voraussetzung für den Unterlassungsanspruch ist u.a., dass es sich bei der IP-Adresse des Klägers um personenbezogene Daten handelt.

2. Die Schlussanträge des Generalanwalts

a) Objektiver oder relativer Ansatz

[Rz 15] Generalanwalt Sánchez-Bordona geht – auch in Hinblick auf die Diskussion in Deutschland – zunächst auf die Frage ein, ob Erwägungsgrund 26 der Datenschutzrichtlinie dahingehend auszulegen sei, dass wenn irgendein Dritter zusätzliche Daten erlangen kann, die zur Identifizierung einer Person verbunden werden können, personenbezogene Daten vorliegen.[28] Seine Einschränkung auf Mittel, die vernünftigerweise von *bestimmten Dritten* eingesetzt werden könnten,[29] klärt diese Frage nicht eindeutig. In der Folge geht der Generalanwalt aber davon aus, dass der für die Verarbeitung Verantwortliche vernünftige Mittel einsetzen können muss, um eine Person zu bestimmen. Darunter seien auch Anfragen an Dritte zu verstehen, an die sich der für die Verarbeitung Verantwortliche *vernünftigerweise* wenden könnte.[30] Im vorliegenden Fall handele es sich beim Internetzugangsanbieter um den Dritten, an den zuerst zu denken sei.[31]

[Rz 16] Der Generalanwalt geht also insofern von einem relativen Ansatz aus, als der für die Verarbeitung Verantwortliche den Bezugspunkt des Anwendungsbereichs des Datenschutzrechts darstellen soll. Dabei bezieht er aber auch die Möglichkeit des für die Verarbeitung Verantwortlichen mit ein, sich an Dritte wenden zu können.

b) Mittel zur Bestimmung eines Betroffenen

[Rz 17] Im Folgenden behandelt der Generalanwalt die Frage, was als «Mittel, dass vernünftigerweise eingesetzt werden könnte» i.S.d. Erwägungsgrundes 26 der Datenschutzrichtlinie zu verstehen ist. Er führt aus, ein vernünftiges Mittel liege für den Verarbeiter nicht vor, wenn zwar ein Dritter die notwendigen Informationen habe, der Kontakt mit diesem Dritten aber faktisch einen

27 Vgl. Beschluss des BGH VI ZR 135/13 vom 28. Oktober 2014, Rz 6 ff.

28 Schlussanträge des Generalanwalts (Fn. 9), Rz 64.

29 Schlussanträge des Generalanwalts (Fn. 9), Rz 67.

30 Schlussanträge des Generalanwalts (Fn. 9), Rz 68.

31 Schlussanträge des Generalanwalts (Fn. 9), Rz 69.

sehr hohen personellen und wirtschaftlichen Aufwand erfordern würde oder wenn er praktisch nicht durchführbar oder gesetzlich verboten wäre.[32] Für Generalanwalt Sánchez-Bordona hängt die Frage, ob ein vernünftiges Mittel vorliegt, sich Daten vom Dritten zu beschaffen, somit wesentlich auch davon ab, dass die Möglichkeit «*im Rahmen des Gesetzes realisierbar*» ist.[33] Es müsse z.B. die Speicherung und Weitergabe der Daten (hier des Internetzugangsanbieters) gesetzlich möglich sein.[34]

[Rz 18] Dabei sieht der Generalanwalt jede rechtlich zulässige Möglichkeit der Erlangung des Zusatzwissens als *vernünftiges Mittel* an, unabhängig davon, wie beschränkt sie in ihrer Anwendung ist.[35] Ob der Zugang zu personenbezogenen Daten *de facto* durch eine Verletzung der Vorschriften über den Datenschutz möglich ist, könne keine Rolle spielen.[36] Dem Generalanwalt zufolge sind somit nur rechtlich zulässige Mittel als vernünftig i.S.d. Erwägungsgrundes 26 der Datenschutzrichtlinie anzusehen und alle rechtlich zulässigen Mittel haben als vernünftig zu gelten.

[Rz 19] Dem Argument der deutschen Regierung, der Internetzugangsanbieter dürfe die Informationen nicht ohne Weiteres, sondern nur im Einklang mit den Datenschutzvorschriften zugänglich machen,[37] begegnet der Generalanwalt mit der Aussage, der Internetzugangsanbieter könne natürlich berechtigt sein, die Herausgabe der Daten zu verweigern, aber auch das Gegenteil sei möglich.[38] Er unterstreicht damit noch einmal, dass es nur darauf ankommen soll, ob überhaupt jemals ein rechtlich zulässiges Mittel vorliegt, mit dem die Bestimmung einer Person vorgenommen werden könnte, wovon er im Anlassfall auszugehen scheint.[39]

[Rz 20] Entgegen den Ansichten der deutschen Regierung soll es zudem nicht auf den tatsächlichen Gebrauch einer Möglichkeit zur Identifizierung einer Person ankommen, sondern nur darauf, ob ein Mittel zur Identifizierung zur Verfügung stünde.[40] Dem Generalanwalt zufolge ist das Potenzial der Daten entscheidend «– *allein oder in Verbindung mit anderen Daten – der Identifizierung einer natürlichen Person zu dienen*».[41] Der Websitebetreiber muss sich demnach alle *Mittel* zurechnen lassen, mit deren Hilfe die Bestimmung einer Person *vernünftigerweise* möglich sein könnte.[42] Die Vorlagefrage ist für den Generalanwalt folglich dahingehend zu beantworten, dass die dynamische IP-Adresse für den Websitebetreiber personenbezogene Daten darstellen.[43]

---

32 Schlussanträge des Generalanwalts (Fn. 9), Rz 68.

33 Schlussanträge des Generalanwalts (Fn. 9), Rz 73.

34 Schlussanträge des Generalanwalts (Fn. 9), Rz 72.

35 Schlussanträge des Generalanwalts (Fn. 9), Rz 73.

36 Schlussanträge des Generalanwalts (Fn. 9), Fußnote 20.

37 Schlussanträge des Generalanwalts (Fn. 9), Rz 71.

38 Schlussanträge des Generalanwalts (Fn. 9), Rz 72.

39 Der Generalanwalt geht in seiner folgenden Argumentation davon aus, der Websitebetreiber könne den Internetzugangsanbieter «jederzeit» um die zusätzlichen Daten bitten (Rz 75).

40 Schlussanträge des Generalanwalts (Fn. 9), Rz 76.

41 Schlussanträge des Generalanwalts (Fn. 9), Rz 77.

42 Keppeler sieht deshalb überwiegende Elemente der objektiven Theorie. Vgl. Lutz M. Keppeler, «Objektive Theorie» des Personenbezugs und «berechtigtes Interesse» als Untergang der Rechtssicherheit?, CR 6/2016, 362.

43 Schlussanträge des Generalanwalts (Fn. 9), Rz 74, 78.

3. Auskunftsansprüche gegenüber dem Internetzugangsanbieter

[Rz 21] Dem Generalanwalt kommt die Aufgabe zu, das Unionsrecht auszulegen. Im Anlassfall ist aber auch entscheidend, ob nach nationalem Recht die Abfrage von zusätzlichen Informationen durch den Websitebetreiber beim Internetzugangsanbieter zulässig ist. Die deutsche Regierung bringt diesbezüglich vor, eine Abfrage sei nicht ohne Weiteres möglich. Der Generalanwalt geht ohne genauere Prüfung der nationalen Rechtslage trotzdem davon aus, dass eine rechtlich zulässige Möglichkeit zur Erlangung der Daten besteht. Da es für den Anwendungsbereich des Datenschutzrechts im Anlassfall darauf ankommen könnte, unter welchen Voraussetzungen eine Auskunftserteilung des Internetzugangsanbieters an den Websitebetreiber zulässig ist, folgt eine kurze Übersicht über die rechtlichen Voraussetzungen der Auskunftserteilung in Österreich und Deutschland.

a) Österreich

[Rz 22] Die rechtliche Zulässigkeit einer Abfrage von Informationen über dynamische IP-Adressen durch den Dienstanbieter beim Internetzugangsanbieter hängt wesentlich davon ab, ob die anfragende Stelle privat oder staatlich ist.

[Rz 23] Für die Auskunftserteilung an Private kommt in Österreich das Urhebergesetz (UrhG) oder das E-Commerce-Gesetz (ECG) in Frage. Der OGH entschied im Jahr 2009, ein Dritter könne nicht auf Grundlage von § 87b Abs. 3 UrhG[44] die Herausgabe von Informationen über die Identität von Nutzern, denen Urheberrechtsverstöße vorgeworfen werden, beim Internetzugangsanbieter verlangen, weil der Internetzugangsanbieter dazu unrechtmäßigerweise Verkehrsdaten verarbeiten müsste.[45] Die Auskunftspflicht nach § 18 Abs. 4 ECG[46] richtet sich dem Gesetzeswortlaut nach an Host-Provider. Der OGH nahm allerdings bereits eine analoge Anwendung des § 18 Abs. 4 ECG auf Telekommunikationsunternehmen, die ein öffentliches Kommunikationsnetz betreiben, an.[47] Auch in diesem Fall ist aber eine Auskunftserteilung des Internetzugangsanbieters unzulässig, wenn er dazu Verkehrsdaten verarbeiten müsste.[48] Für Private gibt es demnach keine rechtlich zulässige Möglichkeit, die Inhaber dynamischer IP-Adressen direkt vom Internetzugangsanbieter zu erfragen.

[Rz 24] Die Sicherheitsbehörden dürfen gemäß § 53 Abs. 3a Z 3 des Sicherheitspolizeigesetzes (SPG) von Betreibern öffentlicher Telekommunikationsdienste und sonstigen Dienstanbietern i.S.d. § 3 Z 2 ECG Auskunft über Namen und Anschrift eines Benutzers, dem eine IP-Adresse

---

44 Vermittler im Sinne des § 81 Abs. 1a haben dem Verletzten auf dessen schriftliches und ausreichend begründetes Verlangen Auskunft über die Identität des Verletzers (Name und Anschrift) beziehungsweise die zur Feststellung des Verletzers erforderlichen Auskünfte zu geben. In die Begründung sind insbesondere hinreichend konkretisierte Angaben über die den Verdacht der Rechtsverletzung begründenden Tatsachen aufzunehmen. Der Verletzte hat dem Vermittler die angemessenen Kosten der Auskunftserteilung zu ersetzen.

45 Urteil des OGH 4 Ob 41/09x vom 14. Juli 2009. Vgl. auch Urteil des EuGH C-557/07 vom 19. Februar 2009, *LSG/Tele2*.

46 Die in § 16 genannten Diensteanbieter haben den Namen und die Adresse eines Nutzers ihres Dienstes, mit dem sie Vereinbarungen über die Speicherung von Informationen abgeschlossen haben, auf Verlangen dritten Personen zu übermitteln, sofern diese ein überwiegendes rechtliches Interesse an der Feststellung der Identität eines Nutzers und eines bestimmten rechtswidrigen Sachverhalts haben sowie überdies glaubhaft machen, dass die Kenntnis dieser Informationen eine wesentliche Voraussetzung für die Rechtsverfolgung bildet.

47 Urteil des OGH 4 Ob 7/04i 16. März 2004.

48 Vgl. Wolfgang Zankl, ECG: E-Commerce-Gesetz, Verlag Österreich (2016), Rz 362.

zu einem bestimmten Zeitpunkt zugewiesen war, verlangen, wenn diese Daten wesentliche Voraussetzungen zur Abwehr einer allgemeinen Gefahr oder im Rahmen der ersten allgemeinen Hilfeleistungspflicht benötigt werden.[49] Im Rahmen des polizeilichen Staatsschutzes dürfen diese Auskünfte gemäß § 11 Abs. 1 Z 5 des Polizeilichen Staatsschutzgesetzes (PStSG) zur erweiterten Gefahrenerforschung und zum Schutz vor verfassungsgefährdeten Angriffen zu Gruppierungen, Einzelpersonen sowie deren jeweiligen Kontakt- und Begleitpersonen eingeholt werden, wenn die Erfüllung der Aufgabe durch den Einsatz anderer Ermittlungsmaßnahmen aussichtslos wäre. In der Strafprozessordnung (StPO) werden Anbieter von Kommunikationsdiensten dazu verpflichtet, auf Anordnung der Staatsanwaltschaft gemäß § 76a Abs. 2 Z 1 StPO Auskunft darüber zu geben, wem zu welchem Zeitpunkt eine öffentliche IP-Adresse zugeordnet war, und an einer «Auskunft über Daten einer Nachrichtenermittlung» i.S.d. § 134 Z 2 StPO auf Anordnung der Staatsanwaltschaft mit gerichtlicher Bewilligung mitzuwirken. Gemäß § 18 Abs. 2 ECG haben Dienstanbieter (u.a. Access-Provider) auf Anordnung eines befugten Gerichts Informationen über Nutzer ihrer Dienste zur Verhütung, Ermittlung, Aufklärung oder Verfolgung gerichtlich strafbarer Handlungen bereitzustellen. Die Verarbeitung von Verkehrsdaten ist für Betreiber öffentlicher Kommunikationsdienste in § 99 Abs. 5 TKG geregelt, der auf die genannten Bestimmungen der StPO, des SPG und des PStSG verweist.

[Rz 25] Staatlichen Stellen ist es folglich im Rahmen gesonderter Tatbestände möglich, Informationen über den Inhaber einer dynamischen IP-Adresse beim Internetzugangsanbieter zu erfragen. Für die Zugangsanbieter besteht aber keine Speicherpflicht[50], somit können die Daten nur abgefragt werden, wenn sie tatsächlich vorhanden sind. Private könnten durch eine Anzeige und eine folgende Akteneinsicht[51] die fraglichen Informationen erhalten.

b) Deutschland

[Rz 26] Auch in Deutschland ist danach zu unterscheiden, ob die anfragende Stelle staatlich oder privat ist. Im Falle von Urheberrechtsverletzungen[52] kann der Rechteinhaber vom Internetzugangsanbieter gemäß § 101 Abs. 2 Z 3 des deutschen Urheberrechtsgesetzes (dUrhG) Auskunft über den Rechtsverletzer verlangen. Die Auskunftserteilung unterliegt allerdings einem Richtervorbehalt, weil dazu Verkehrsdaten verarbeitet werden müssen.[53]

[Rz 27] Strafverfolgungsbehörden dürfen gemäß § 100j Abs. 1 u. 2 der deutschen Strafprozessordnung (dStPO) Auskunft über Bestandsdaten vom Internetzugangsanbieter anhand einer zu einem bestimmten Zeitpunkt vergebenen IP-Adresse verlangen, soweit dies für die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes eines Beschuldigten erforderlich ist. Die Telekommunikationsdienste haben dem gemäß § 113 Abs. 1 des deutschen Telekommunikati-

---

49 Zur Verfassungskonformität: Urteile des VfGH G31/08–G29/08, G30/08, G35/08, G147/08 u.a. vom 1. Juli 2009; Urteil des VfGH B 1031/11 vom 29. Juni 2012.

50 Vgl. Urteil des VfGH G 47/2012 u.a. vom 27. Juni 2014. Vgl. auch Urteile des VfGH G31/08–G29/08, G30/08, G35/08, G147/08 u.a. vom 1. Juli 2009 und Urteil des VfGH B 1031/11 vom 29. Juni 2012.

51 § 68 StPO.

52 Der BGH stellte klar, dass eine Rechtsverletzung *in gewerblichem Ausmaß* nicht Voraussetzung ist (Beschluss des BGH I ZB 80/11 vom 19. April 2012).

53 § 101 Abs. 9 dUrhG.

onsgesetzes (dTKG) nachzukommen.[54] Seit Wiedereinführung der Vorratsdatenspeicherung sind Telekommunikationsdienste dazu verpflichtet, zugewiesene IP-Adressen mit Datum und Uhrzeit für 10 Wochen zu speichern.[55] Die Erhebung dieser Verkehrsdaten ist bei Tatverdacht für gesondert aufgezählte schwere Straftatbestände zulässig, soweit die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise wesentlich erschwert oder aussichtslos wäre und die Erhebung der Daten in einem angemessenen Verhältnis zur Bedeutung der Sache steht.[56]

[Rz 28] Im Unterschied zur österreichischen Rechtslage sind Informationen über zugewiesene IP-Adressen also beim Internetzugangsanbieter verpflichtend zu speichern und eine direkte Abfrage durch Private ist nicht vollkommen ausgeschlossen. Die Auskunftserteilung an Private unterliegt aber einem Richtervorbehalt. Ansonsten ist es nur Behörden erlaubt, vom Internetzugangsanbieter bei Vorliegen gesondert normierter Tatbestandsvoraussetzungen Auskunft zu verlangen. Der Weg über eine Anzeige und folgende Akteneinsicht ist auch in Deutschland möglich.

4. Zwischenfazit

[Rz 29] Der Generalanwalt nimmt eine sinnvolle Abgrenzung des Anwendungsbereichs dahingehend vor, dass Ausgangspunkt der Beurteilung eines Personenbezugs nur der für die Verarbeitung Verantwortliche sein kann. Dieser kann sich selbstverständlich aber auch im Rahmen seiner Möglichkeiten an Dritte wenden, um zusätzliche Informationen zu erhalten. Dem Wortlaut des Erwägungsgrundes 26 nach wäre auch ein objektiver Ansatz denkbar, womöglich sogar naheliegender[57] gewesen. Wie der Generalanwalt allerdings richtig erkennt, würde der objektive Ansatz durch seine Schutzrichtung die Ausuferung des Anwendungsbereichs anlegen.[58]

[Rz 30] Der Generalanwalt nimmt den Personenbezug von Daten immer dann an, wenn es dem für die Verarbeitung verantwortlichen unter Einsatz aller Mittel vernünftigerweise möglich wäre, eine Person zu bestimmen, unabhängig davon, ob er tatsächlichen die Bestimmung der Person vornehmen möchte. Diese Ansicht ist insbesondere in Hinblick auf Erwägungsgrund 26 nachvollziehbar (Vgl. «[…] *alle Mittel*, […], *die vernünftigerweise* […] *eingesetzt werden* ***könnten***»). Die Auslegung der deutschen Regierung, die auf eine tatsächliche Verknüpfung der Daten beim Internetzugangsanbieter abstellt, ist mit der Datenschutzrichtlinie nur schwer zu vereinbaren, weil auch Informationen über eine «bestimmbare» Person geschützt sein sollen.[59] Erhält der Websitebetreiber die notwendigen Informationen vom Zugangsanbieter, ist darin jedenfalls bereits der Prozess der Bestimmung einer Person zu sehen.

---

54 Weitere Abrufnormen sind §§ 7, 20b und 22 des Bundeskriminalamtgesetzes (BKAG), § 22a des Bundespolizeigesetzes (BPolG), §§ 7, 15 des Zollfahndungsdienstgesetzes (ZFdG), § 8d des Bundesverfassungsschutzgesetzes (BVerfschG), § 2b des Bundesnachrichtendienstgesetzes (BNDG) und § 4b des Gesetzes über den militärischen Abschirmdienst (MAD-G). Vgl. Jakob Dalby, Grundlagen der Strafverfolgung im Internet und in der Cloud, Springer Verlag (2016), 69.

55 § 113b Abs. 1 Z 1 i.V.m. Abs. 3 dTKG.

56 § 100g Abs. 2 dStPO.

57 Kalteis (Fn. 21), ZfV 2013/246.

58 Vgl. Schlussanträge des Generalanwalts (Fn. 9), Rz 68

59 Der Wortlaut der Datenschutz-Richtlinie ist diesbezüglich eindeutig, selbst wenn man die Eröffnung des Anwendungsbereichs bereits bei «Bestimmbarkeit» als nicht sinnvoll erachtet (Vgl. Rolf H. Weber, Internet of things: Privacy issues revisited, Computer Law & Security Review 31 [2015], 623).

[Rz 31] Es zeigt sich, dass die Auslegung des Generalanwalts zwar auf einen relativen Personenbezug von Daten abstellt, da diese Mittel aber nicht tatsächlich eingesetzt werden müssen, sondern Bestimmbarkeit bereits vorliegt, wenn die Mittel potenziell eingesetzt werden könnten, ergibt sich trotz des relativen Ansatzes ein sehr weitgehender Anwendungsbereich des Datenschutzrechts. Meines Erachtens müsste die Auslegung des Generalanwalts aber auch dazu führen, dass die Beurteilung, ob ein Personenbezug vorliegt, abhängig von den Möglichkeiten der einzelnen für die Verarbeitung Verantwortlichen vorzunehmen wäre. Ein großer Technologiekonzern müsste sich demnach andere Mittel als vernünftig zurechnen lassen als ein kleines (technologiefernes) Startup.

[Rz 32] Entscheidend für den Anwendungsbereich des Datenschutzrechts ist zudem, welche Mittel als *vernünftig* i.S.d. Erwägungsgrundes 26 der Datenschutz-Richtlinie gelten sollen. Der Generalanwalt trifft eine Aussage darüber, dass nur legale Mittel in Frage kommen, was begrüßenswert ist.[60] Eine Auslegung, die einen Rechtsbruch als «Mittel, das *vernünftigerweise* eingesetzt werden könnte» bezeichnet würde, widerspräche m.E. den Grundlagen des Rechtsstaates. Der Schutz vor einer Privilegierung rechtswidrigen Verhaltens muss dabei in der Rechtsordnung selbst angelegt sein, wie es derzeit durch einschlägige (Verwaltungs-) Straftatbestände geschieht.[61]

[Rz 33] Der Generalanwalt plädiert aber auch dafür, alle legalen Mittel grundsätzlich als *vernünftig* anzusehen, unabhängig davon, wie eingeschränkt ihr tatsächlicher Anwendungsbereich ist. Diese Ansicht teilt der deutsche BGH offensichtlich nicht, demzufolge es nicht ausreichen soll, dass etwa die Staatsanwaltschaft die zusätzlichen Informationen vom Internetzugangsanbieter fordern dürfte.[62] Die Auskunftserteilung ist weder in Österreich noch in Deutschland auf direktem Wege an einen Privaten (bzw. einen staatlichen Websitebetreiber) möglich. Über eine Anzeige und folgende Akteneinsicht im Strafverfahren könnte eine dynamische IP-Adresse allerdings einer Person zugeordnet werden. Dem Generalanwalt genügt diese rechtlich zulässige Möglichkeit offensichtlich, um alle dynamischen IP-Adressen als personenbezogene Daten beim Websitebetreiber anzusehen. Der BGH[63] und in diesem Sinne wohl auch die deutsche Regierung[64] weisen hingegen darauf hin, dass im Anlassfall eine Auskunftserteilung rechtlich nicht zulässig ist.

[Rz 34] Mag es im konkreten Fall für den Websitebetreiber nicht zulässig sein, eine Auskunft vom Internetzugangsanbieter zu verlangen, muss trotzdem beachtet werden, dass der Websitebetreiber die dynamischen IP-Adressen nicht nur speichert, sondern auch dazu verwendet, strafrechtlich relevantes Verhalten zu verfolgen. Dem Prozess der Speicherung und der Prüfung strafbarer Handlungen werden alle auf die Website zugreifenden IP-Adressen unterworfen, um bei Vorliegen der Tatbestandsmerkmale eine Identifizierung der dahinterstehenden Person zu ermöglichen. Es ist somit nicht im Voraus erkennbar, welche IP-Adressen einer Identifizierung zugeführt werden dürfen und welche nicht. Insofern kommt es zu einer Erhebung personenbezogener Daten, selbst wenn ex-post betrachtet nur eine geringe Anzahl der erhobenen IP-Adressen einen Auskunftsanspruch gewähren. Es kann zudem nur schwer argumentiert werden, ein Strafverfahren anzustrengen bzw. alle rechtlich zur Verfügung stehenden Mittel auszuschöpfen sei unvernünf-

60 In Deutschland wurde z.T. die Meinung vertreten, auch illegale Mittel müssten in die Beurteilung mit einbezogen werden. Vgl. Bergt (Fn. 8), ZD 2015, 370.

61 Vgl. u.a. §§ 118a, 119a StGB; §§ 51, 52 Abs 1 DSG.

62 Beschluss des BGH VI ZR 135/13 vom 28. Oktober 2014, Rz 44.

63 Beschluss des BGH VI ZR 135/13 vom 28. Oktober 2014, Rz 44.

64 Vgl. Schlussanträge des Generalanwalts (Fn. 9), Rz 71.

tig oder erfordere unverhältnismäßigen Aufwand. Der Auslegung des Generalanwalts ist deshalb m.E. zu folgen.

[Rz 35] Unabhängig vom Anlassfall ist darauf hinzuweisen, dass zwar Bestimmbarkeit bereits vorliegt, wenn die potenzielle Möglichkeit besteht, Mittel zur Identifizierung einer Person anzuwenden, aber Erwägungsgrund 26 sich nur auf solche Mittel beziehen kann, die **nach** Erhebung der Daten eingesetzt werden könnten. Es wäre nämlich bspw. abwegig, anzunehmen, dynamische IP-Adressen seien schon deshalb personenbezogene Daten, weil die durchaus vernünftige Möglichkeit besteht, ein Anmeldesystem für die Website zu programmieren. Gleiches muss m.E. auch gelten, wenn ein Internetzugangsanbieter keine Speicherung der LogFiles vornimmt,[65] weil er dazu nicht verpflichtet ist. In diesem Sinne kommt es schließlich doch auch darauf an, welche Mittel tatsächlich eingesetzt werden.

III. Ausblick

1. Datenschutzgrundverordnung

[Rz 36] Auch nach der EU-Datenschutz-Grundverordnung (DS-GVO) ist die Verarbeitung personenbezogener Daten Anknüpfungspunkt für den sachlichen Anwendungsbereich des Datenschutzrechts. Personenbezogene Daten sind demnach alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Als identifizierbar wird eine Person angesehen, die direkt oder indirekt identifiziert werden kann.[66] Erwägungsgrund 26 DS-GVO führt aus: «*Um festzustellen, ob eine natürliche Person identifizierbar ist, sollten alle Mittel berücksichtigt werden, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren, wie beispielsweise das Aussondern. Bei der Feststellung, ob Mittel nach allgemeinem Ermessen wahrscheinlich zur Identifizierung der natürlichen Person genutzt werden, sollten alle objektiven Faktoren, wie die Kosten der Identifizierung und der dafür erforderliche Zeitaufwand, herangezogen werden, wobei die zum Zeitpunkt der Verarbeitung verfügbare Technologie und technologische Entwicklungen zu berücksichtigen sind.*» IP-Adressen finden explizit Erwähnung in Erwägungsgrund 30[67], ihre Einordnung wird aber offen gelassen.

[Rz 37] Der Anwendungsbereich der DS-GVO könnte m.E. gegenüber der Datenschutz-Richtlinie sowohl weiter als auch enger verstanden werden. Mittel, *die nach allgemeinem Ermessen wahrscheinlich genutzt werden*, könnten im Gegensatz zu *vernünftigen Mitteln* u.U. auch rechtswidrige Mittel sein. Auf der anderen Seite kommt es bei Mitteln, *die nach allgemeinem Ermessen wahrscheinlich genutzt werden* zwar weiterhin auf eine potenzielle Möglichkeit der Identifizierung einer Person an, diese Möglichkeit muss aber immerhin nach allgemeinem Ermessen ***wahrschein-***

65 Wie es häufig bei der Zuteilung von IP-Adressen an Smartphones in Österreich der Fall ist. Eine ähnliche Frage könnte sich im Rahmen öffentlicher WLAN-Netze auch in Deutschland stellen (s. dazu Keppeler [Fn. 42], CR 6/2016).

66 Art 4 Z 1 DS-GVO.

67 «Natürlichen Personen werden unter Umständen Online-Kennungen wie IP-Adressen und Cookie-Kennungen, die sein Gerät oder Software-Anwendungen und -Tools oder Protokolle liefern, oder sonstige Kennungen wie Funkfrequenzkennzeichnungen zugeordnet. Dies kann Spuren hinterlassen, die insbesondere in Kombination mit eindeutigen Kennungen und anderen beim Server eingehenden Informationen dazu benutzt werden können, um Profile der natürlichen Personen zu erstellen und sie zu identifizieren.»

lich genutzt werden. Nach der Datenschutz-Richtlinie genügte die abstrakte Möglichkeit, dass die *Mittel vernünftigerweise verwendet werden* ***könnten***. Die Formulierungen unterscheiden sich zwar im Detail, trotzdem kann m.E. davon ausgegangen werden, dass die Entscheidung des EuGH zu m Verfahren C-582/14 in der Sache *Breyer* das Verständnis des Personenbezugs von Daten auch für den Anwendungsbereich der DS-GVO maßgeblich beeinflussen wird.

2. Technische Entwicklungen

[Rz 38] Die Diskussion um den Anwendungsbereich des Datenschutzrechts wird im Anlassfall vor dem EuGH anhand von dynamischen IPv4-Adressen geführt. Die Entscheidung könnte aber über den Anlassfall hinaus für weitere technische Entwicklungen Bedeutung haben.

a) IPv6

[Rz 39] Wie bereits erwähnt, wird aufgrund der begrenzten Anzahl von IPv4-Adressen eine Umstellung auf IPv6-Adressen vorgenommen. IPv6-Adressen bestehen aus zwei Teilen: dem Global Routing Präfix und dem Interface Identifier. Das Präfix wird vom Internetzugangsanbieter vergeben. Aufgrund des größeren Adressrahmens wäre es denkbar, dass dieser Teil unter Anwendung von IPv6 statisch vergeben würde.[68] Damit wäre die Identifizierung eines Nutzers für Websitebetreiber deutlich vereinfacht, weil schon eine einmalige Identitätspreisgabe genügen würde, um das betreffende Gerät mit einer Person dauerhaft zu verbinden. Eine solche Entwicklung wäre aus datenschutzrechtlicher Sicht in Hinblick auf die Privatsphäre von Betroffenen bedenklich. Große Internetzugangsanbieter in Deutschland erklärten diesbezüglich bereits, auch IPv6-Adressen dynamisch vergeben zu wollen.[69]

[Rz 40] Der Interface Identifier wird von dem verwendeten Gerät erzeugt, wodurch Geräte eindeutig bezeichnet und wiedererkannt werden könnten. Um eine Identifizierung dieser Art zu verhindern, wurden allerdings Privacy Extensions entwickelt.[70] Ob IPv6-Adressen personenbezogene Daten darstellen, hängt von der konkreten technischen Umsetzung ab, wobei eine Orientierung an den Überlegungen zu IPv4-Adressen angebracht erscheint.

b) Das Internet der Dinge

[Rz 41] Der Begriff «Internet der Dinge» soll eine Entwicklung beschreiben, in der immer mehr Gegenstände des täglichen Lebens Daten selbständig erheben und in der Lage sind, in einem Netzwerk zu kommunizieren. Diese «intelligenten Gegenstände» könnten die Umgebung der Menschen auf deren Bedürfnisse abstimmen und somit unterstützend wirken (ohne aufzufallen). Bereits heute sind umfassende Datenerhebungen bspw. durch Smartphones, Autos, smart homes oder diverse Wearables bekannt. Die große Anzahl von neuen Sensoren führt zu einem exponen-

68 Thomas Nietsch, Datenschutzrechtliches Gebot zur Vergabe dynamischer IP-Adressen im IPv6, CR 11/2011, 764 f.

69 Vgl. Ole Reissmann, Provider versprechen Datenschutz bei IPv6, Spiegel Online vom 4. Mai 2011. http://www.spiegel.de/netzwelt/web/neues-internet-protokoll-provider-versprechen-datenschutz-bei-ipv6-a-760274.html.

70 Vgl. Christoph Wegener/Jörg Heidrich, Neuer Standard – Neue Herausforderungen: IPv6 und Datenschutz, CR 7/2011, 481.

tiellen Anstieg verfügbarer Daten.[71] Diese Entwicklung wird sich im Internet der Dinge weiter verstärken. Zahlreiche Dienste sind insbesondere auf Grundlage von intensiven Datenerhebungen denkbar, bei denen die Daten miteinander verknüpft oder mit Hintergrunddatenbanken[72] abgeglichen werden.

[Rz 42] Wesentliches datenschutzrechtliches Problem dieser Entwicklung ist die Möglichkeit der Erstellung präziser Persönlichkeitsprofile[73] – diese sind allerdings häufig essenzieller Bestandteil oder sogar Voraussetzung für die Erbringung des gewünschten Dienstes.[74] Es könnten zudem durch die umfassende Datenerhebung auch zahlreiche Informationen zu Dritten verarbeitet werden, die den fraglichen Dienst gar nicht nutzen (wollen). Die Artikel 29-Datenschutzgruppe sieht deshalb die Gefahr, dass durch das Internet der Dinge in Zukunft die Möglichkeit, anonym zu bleiben, begrenzt werden könnte.[75] Diese Gefahr vergrößere sich auch dadurch, dass De-anonymisierungen durch die schiere Anzahl von erhobenen Daten begünstigt werden, weshalb laut Artikel 29-Datenschutzgruppe u.U. sogar Daten, die erst nach Anwendung von Anonymisierungstechniken verarbeitet werden, als personenbezogen anzusehen sein sollen (!).[76]

[Rz 43] Die Vorlagefrage in der Rechtssache *Breyer* ist auch für den Anwendungsbereich des Datenschutzrechts im Internet der Dinge interessant. Viele der erhobenen Daten werden nämlich zunächst keine Informationen über eine bestimmte Person darstellen, es wird somit entscheidend darauf ankommen, ob Bestimmbarkeit vorliegt.

[Rz 44] Im Internet der Dinge zeigt sich noch einmal deutlich, dass der objektive Ansatz zu einer Ausuferung des datenschutzrechtlichen Anwendungsbereichs führen würde. Müsste sich jeder für die Verarbeitung Verantwortliche auch das Wissen anderer Datenverarbeiter zurechnen lassen, würden nahezu alle erhobenen Daten personenbezogen sein, weil die große Anzahl einzelner Daten in Verbindung mit (allen) anderen erhobenen Daten die Identifizierung einer Person sehr wahrscheinlich ermöglichen würde.

[Rz 45] Nach der Ansicht des Generalanwalts käme es dann zu einer Erhebung personenbezogener Daten, wenn der für die Verarbeitung Verantwortliche eine Verknüpfung der Daten vernünftigerweise vornehmen könnte. Es ist dabei durchaus denkbar, dass sogar der Betreiber eines Systems selbst nicht immer zuverlässig einschätzen kann, ob er aus einer Kombination nicht personenbezogener Daten Personen identifizieren könnte.[77] In diesem Fall ist das Konzept des Generalanwalts wohl insofern tragfähig, als abhängig von den Möglichkeiten des jeweiligen für die Verarbeitung Verantwortlichen festgelegt wird, ob Bestimmbarkeit vorliegt – dazu wäre etwa eine Risikoanalyse der Datenverarbeitung denkbar.[78]

---

71 Vgl. Thilo Weichert, Big Data und Datenschutz, ZD 2013, 3. https://www.datenschutzzentrum.de/uploads/bigdata/20130318-bigdata-und-datenschutz.pdf.

72 Vgl. Kai Hoffmann/Gerrit Hornung, Rechtliche Herausforderungen des Internets der Dinge, in: Florian Sprenger/Christoph Engemann (Hrsg.), Internet der Dinge – Über smarte Objekte, intelligente Umgebungen und die technische Durchdringung der Welt, Transcript Verlag (2016), 194.

73 Vgl. Hoffmann/Hornung (Fn. 72), 192.

74 Vgl. Alexander Rossnagel, Datenschutz in der Welt allgegenwärtigen Rechnens, Information Technology 2/2007, 84.

75 Artikel 29-Datenschutzgruppe, WP 223, Stellungnahme 8/2014 zu den jüngsten Entwicklungen im Internet der Dinge, 9 f.

76 Artikel 29-Datenschutzgruppe, WP 223, Stellungnahme 8/2014 zu den jüngsten Entwicklungen im Internet der Dinge, 12.

77 Hoffmann/Hornung (Fn. 72), 194.

78 Hoffmann/Hornung (Fn. 72), 194.

c) Big Data

[Rz 46] Besonderes Augenmerk wird seit geraumer Zeit auf Big Data-Analysen gelegt. Darunter werden Verfahren zur Strukturierung und Auswertung großer Datenbestände verstanden, die sich häufig aus unterschiedlichsten Quellen speisen. Für den Anwendungsbereich des Datenschutzrechts ist «Big Data» eine Herausforderung, weil aufgrund der Verfahren Verbindungen zwischen einzelnen zunächst nicht personenbezogenen Daten hergestellt werden können, die im Ergebnis personenbezogene Informationen enthalten. Damit können nahezu alle Daten dazu dienen, eine Person in Verbindung mit anderen Daten zu identifizieren. Selbst anonymisierte Daten können durch die Zusammenführung mit anderen Daten aus unterschiedlichsten Quellen (bspw. im Internet veröffentlichte Daten) wieder de-anonymisiert werden.[79]

[Rz 47] Einige Autoren sehen bereits eine Unterscheidung zwischen personenbezogenen und anonymen Daten als nicht mehr möglich an.[80] Andere ziehen zumindest in Erwägung die Entwicklung zum Anlass zu nehmen, dem objektiven Ansatz zu folgen.[81] Auch der Generalanwalt befürwortet einen präventiven Schutz des Datenschutzrechts mit Blick auf zukünftige Entwicklungen.[82] Die Artikel 29-Datenschutzgruppe weist allerdings darauf hin, dass Verarbeitungen zu Big Data-Analysen nicht immer personenbezogene Daten umfassen.[83] Vertreter des strikt relativen Ansatzes zeigen auf, warum auch nach diesem Modell keine Schutzlücke für Betroffene durch Big Data zu entstehen droht.[84]

[Rz 48] Die Gefährdung von Big Data geht im Wesentlichen von Wahrscheinlichkeitsvoraussagen aus, die Betroffene diskriminieren könnten.[85] Verschärfen kann sich dieses Problem dadurch, dass die Berechnungen der Analysen für den Menschen nicht mehr nachvollziehbar sind.[86] Eine Abgrenzung des datenschutzrechtlichen Anwendungsbereichs wird – ohne einen strikten Zweckbindungsgrundsatz, der allerdings schon an sich Big Data Analysen entgegensteht – in der Folge nur schwer möglich sein, weil es im Vorhinein kaum feststellbar sein wird, welche Daten zur Identifizierung einer Person dienen könnten und welche nicht.

IV. Fazit

[Rz 49] Das Urteil des EuGH in der Sache *Breyer* wird über den Anlassfall hinaus für den Anwendungsbereich des Datenschutzrechts wegweisend sein – dies sowohl für zukünftige technische Anwendungen als auch im Hinblick auf die Auslegung der DS-GVO.

---

79 Vgl. Weichert (Fn. 71), ZD 2013, 16.

80 Niko Härting/Jochen Schneider, Das Ende des Datenschutzes – es lebe die Privatsphäre, CR 12/2015, 822.

81 Sachs (Fn. 6), CR 8/2010, 551.

82 Schlussanträge des Generalanwalts (Fn. 9), Rz 66.

83 Erklärung der nach Artikel 29 eingesetzten Datenschutzgruppe über die Auswirkungen der Entwicklung von Big-Data-Technologien auf den Schutz natürlicher Personen im Hinblick auf die Verarbeitung ihrer personenbezogenen Daten in der EU, 3. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp221_de.pdf.

84 Eckhardt/Brink (Fn. 23), ZD 2015, 207.

85 Peter Schaar, Datenschutz in Zeiten von Big Data, HMD Praxis der Wirtschaftsinformatik (2014), 843.

86 Oliver Stiemerling, «Künstliche Intelligenz» – Automatisierung geistiger Arbeit, Big Data und das Internet der Dinge, CR 12/2015, 764.

[Rz 50] Die von Generalanwalt Sánchez-Bordona in seinen Schlussanträgen vorgelegte Auslegung der Datenschutzrichtlinie ist überzeugend. Ob die zugrundeliegenden Vorschriften sinnvoll sind, ist eine andere Frage. Denn der Ansicht des Generalanwalts zu folgen bedeutet auch, den Anwendungsbereich des Datenschutzrechts äußerst weit zu ziehen. Nahezu allen Daten kommt das Potenzial zu, in Verbindung mit anderen Daten (in der Zukunft) der Identifizierung einer natürlichen Person zu dienen, wenn es nicht auf den konkreten Fall ankommen soll, sondern darauf, dass solche Daten jemals zur Bestimmung einer Person führten.

[Rz 51] Die Konsequenz wäre, dass wenn ein Datensatz aus tausenden von Daten der gleichen Art (bspw. dynamische IP-Adressen) eine Information über eine bestimmte oder bestimmbare Person darstellte, alle Daten dieser Art für jeden für die Verarbeitung Verantwortlichen, dem dieselben Mittel zur Verfügung stehen, als personenbezogen anzusehen wären. Diese Ansicht mag für den Schutz der Privatsphäre von Betroffenen erstrebenswert sein. Es ist aber zu bedenken, dass dadurch der Anwendungsbereich des Datenschutzrechts auch dann eröffnet ist, wenn sich eine Gefahr für die Privatsphäre einer Person gegenüber dem für die Verarbeitung Verantwortlichen nicht realisiert, weil er die zur Bestimmung notwendigen Mittel gar nicht einsetzt und etwa auch nicht vorhat, dies jemals zu tun.

Herr Mag. iur. Maurits Haas ist Dissertant der Arbeitsgruppe Rechtsinformatik an der Universität Wien und juristischer Mitarbeiter der Rechtsanwaltskanzlei Lichtenberger & Partner Rechtsanwälte GbR.