

Personenbezug von IP-Adressen

Internetnutzung und Datenschutz

Anonymität
Surf-Protokollierung
Verkehrsdaten
Identifizierbarkeit
Bestandsdatenauskunft

■ Der BGH hat 2009 ein „Recht des Internetnutzers auf Anonymität“ anerkannt. Doch bewegen wir uns im Datennetz wirklich anonym, solange wir unsere Identität nicht bewusst offenlegen? Was Anonymität im Netz eigentlich bedeutet, ist seit Jahren in Rechtswissenschaft und Rechtspraxis umstritten und in Deutschland bisher noch nicht höchstrichterlich geklärt. Anlässlich der Novellierung der Datenschutzrichtlinie (DS-RL) ist in Brüssel erneut um die Frage gerungen worden. Dieser Aufsatz untersucht den Personenbezug von Internetprotokoll-Adressen (IP-Adressen) als unserer ständigen Datenspur im Netz und plädiert für einen umfassenden Datenschutz.

■ In 2009, the German Supreme Court (“BGH”) recognized an “Internet user’s right to anonymity”. But do we truly move about the data network anonymously so long as don’t knowingly disclose our identity? The issue of what anonymity on the Web actually means has been controversial in jurisprudence and legal practice for years and has not yet been decided by the highest courts in Germany. This question was once again struggled with in Brussels on the occasion of the amendment to the Data Protection Guideline (“DS-RL”). This article will investigate personal references of Internet protocol addresses (IP addresses) as our constant data track on the net and will speak for comprehensive data protection.

I. Einleitung

Das Internet als weltweites Informations- und Kommunikationsnetz eröffnet uns zuvor nie gekannte Möglichkeiten und Chancen – und hat doch einen großen Haken: Technisch ist es problemlos möglich, unsere Internetnutzung umfassend aufzuzeichnen. Anbieter von Diensten im Internet machen von dieser Möglichkeit vielfach auch Gebrauch. Während sich Zeitungen im Schutz der Anonymität lesen und Briefe ohne Absender versenden lassen, setzen vergleichbare Aktivitäten im Netz die Offenbarung einer Kennziffer voraus, der IP-Adresse. Anders als ein Kfz-Kennzeichen wird unsere IP-Adresse mit jeder Eingabe und jedem Klick im Netz automatisch an den jeweiligen Diensteanbieter übertragen und kann von diesem auch unschwer protokolliert werden.

Umstritten ist, ob uns die Datenschutzgesetze vor einer solchen „Surf-Protokollierung“ schützen. Einen Schutz gewähren Datenschutzgesetze grundsätzlich nur für personenbezogene Daten, also Daten, die einer bestimmten oder bestimmbar Person zugeordnet werden können (§ 3 Abs. 1 BDSG). Ist die IP-Adresse ein personenbezogenes Datum, das unmittelbar nach Ende der Nutzung einer Website wieder zu löschen ist (§§ 13 Abs. 4, 15 Abs. 4 TMG)?

Verbreitet anerkannt ist der Personenbezug im Fall dauerhaft von der Registrierungsstelle zugewiesener IP-Adressen, sog. „statischer“ IP-Adressen. Wer Inhaber einer statischen IP-Adresse ist, ist bei der Registrierungsstelle typischerweise öffentlich einsehbar. Die meisten privaten Internetnutzer surfen jedoch mit einer nur vorübergehend zugewiesenen IP-Adresse (dynamische IP-Adressen) im Netz. Umstritten ist der Personenbezug dieser IP-Adressen, denn öffentliche Verzeichnisse nennen als Inhaber dieser IP-Adressen nur den Internet-Zugangsanbieter, der die Adressen an seine Kunden „vermietet“. Zwar halten die Internet-Zugangsanbieter verbreitet fest, wann welchem Kunden welche IP-Adresse zugewiesen war.¹ Diese Verkehrsdaten unterliegen jedoch dem Schutz des in Art. 10 GG und § 88 TKG normierten Fernmeldegeheimnisses.

IP-Adressen könnten schon deshalb stets als personenbezogene Daten zu behandeln sein, weil man einer Adresse nicht ansieht, ob sie statisch oder dynamisch vergeben worden ist. Muss das Datenschutzrecht auf sämtliche IP-Adressen angewandt werden, um es in Bezug auf statische IP-Adressen einhalten zu können? So einfach lässt sich die Frage des Personenbezugs dyna-

misch zugewiesener IP-Adressen wohl nicht umschiffen: Einerseits wäre es für Anbieter technisch durchaus machbar, dynamische IP-Adressen bekannter Internet-Zugangsanbieter von sonstigen IP-Adressen zu trennen. Andererseits bleibt die Unterscheidung maßgeblich, wenn ein Internetnutzer Individualansprüche auf Nichtspeicherung, Löschung oder Berichtigung von Internet-Nutzungsdaten geltend macht.

Es bleibt also bei der Frage, ob die Nutzer dynamisch zugewiesener IP-Adressen rechtlos sind, weil ihre Datenspur keine personenbezogenen Daten i.S.d. Datenschutzrechts darstellen.

II. Der Begriff des Personenbezugs

Das Datenschutzrecht gilt nur für personenbezogene Daten (§ 1 BDSG). Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbar natürlichen Person (§ 3 Abs. 1 BDSG). Für die Frage der Bestimmbarkeit einer Person ist auf die vernünftigerweise dem Verantwortlichen für die Verarbeitung oder einem Dritten zur Verfügung stehenden Mittel zur Identifizierung abzustellen (Erwägungsgrund 26 RL 95/46/EG). Der Begriff „vernünftigerweise“ wird dabei i.S.v. „realistischerweise“ zu verstehen sein. Die Herstellung des Personenbezugs muss also nicht nur theoretisch denkbar, sondern auch praktisch möglich sein.

Vertreter eines sog. „relativen“ Begriffs des Personenbezugs erkennen die Worte „oder einem Dritten“ in der Definition der Bestimmbarkeit in Erwägungsgrund 26 der Datenschutzrichtlinie (RL 95/46/EG – DS-RL) nicht an. Verstöße gegen das Datenschutzrecht ließen sich vernünftigerweise ausschließen. Ein Datum solle deshalb nur dann personenbezogen sein, wenn gerade die jeweils speichernde Stelle den Nutzer identifizieren könne.² Der Begriff des Personenbezugs soll nach dieser Auffassung also „relativ“ sein: Ein und dasselbe Datum könne personenbezogen oder „anonym“ sein – je nachdem, wer über das Datum verfüge. Könne die jeweils speichernde Stelle den Betroffenen mit eigenen Mitteln nicht identifizieren, sei das Datenschutzrecht nicht anwendbar. Anzuwenden sei das Datenschutzrecht erst, wenn die Daten an eine Stelle übermittelt werden sollten, die über das zur Identifizierung erforderliche Zusatzwissen ver-

¹ S. <http://wiki.vorratsdatenspeicherung.de/Speicherdauer> sowie zur rechtlichen Würdigung Breyer, MMR 2011, 573.

² Gola/Schomerus, BDSG, 8. Aufl., § 3 Rdnr. 9.

füge. Dieser Übermittlungsvorgang und die anschließende Verarbeitung seien dann nur nach den Regelungen des Datenschutzrechts zulässig.³

III. Personenbezug auf Grund zulässigerweise verfügbaren Zusatzwissens

Unstreitig ist danach der Personenbezug einer IP-Adresse immer dann, wenn die speichernde Stelle selbst über legale Mittel der Identifizierung verfügt. Dies ist nicht selten der Fall:

1. Offenlegung der Identität durch den Nutzer

Telemedienanbieter können eine IP-Adresse und damit das Nutzungsverhalten einer Person zuordnen, wenn der Nutzer während eines Nutzungsvorgangs seine Identität offen gelegt hat, z.B. durch Benutzung eines Kontaktformulars, durch Auslösung einer Bestellung oder durch Anmeldung als registrierter Nutzer. Mithilfe der genutzten IP-Adresse und ggf. weiterer Indizien (z.B. Verlauf der abgerufenen Seiten, Cookies, „Fingerabdruck“ des Browsers) kann der Anbieter in diesen Fällen auch die der Identifizierung vorangegangene und nachfolgende Nutzung des Portals durch den Nutzer rekonstruieren.

2. Zusammenführung mit Kenntnissen anderer Diensteanbieter

Eine Identifizierung kann dem Telemedienanbieter auch im Zusammenwirken mit anderen Anbietern möglich sein, die ihrerseits die Identität des Nutzers einer IP-Adresse kennen. Dabei kommt keineswegs nur der Internet-Zugangsanbieter in Betracht. Telemedienanbieter protokollieren neben der IP-Adresse nicht selten die vom Nutzer zuletzt – extern – besuchte Internetseite („Referer“). Angenommen, ein Nutzer klickt in einem von ihm genutzten E-Mail-Dienst auf einen Link zu einem Internetangebot. Dadurch kann bei dem E-Mail-Anbieter in Erfahrung gebracht werden, welcher seiner Kunden zum maßgeblichen Zeitpunkt die protokollierte IP-Adresse genutzt hat. Der E-Mail-Anbieter kennt oftmals die Identität seiner registrierten Nutzer. In ähnlicher Weise kann eine Identifizierung über die Anbieter von Internetforen, von Suchmaschinen usw. erfolgen, bei denen der Nutzer namentlich registriert ist und über die er auf das Ziel-Telemedium gelangt. Entsprechende Auskünfte dürfen Telemedienanbieter „zur Rechtsdurchsetzung“ in weitem Umfang erteilen (§§ 14 Abs. 2, 15 Abs. 5 Satz 4 TMG). Vorformulierte Einwilligungsklauseln sehen vielfach Möglichkeiten zur Datenübermittlung und -zusammenführung vor. Der US-amerikanische Gesetzgeber unterwirft die dort ansässigen Anbieter keinerlei Restriktionen im Umgang mit unseren Daten.

Teilweise erlauben Nutzungsdaten schon in Verbindung mit offenen Quellen eine Identifizierung des Nutzers. So konnte die New York Times aus den um die IP-Adresse bereinigten Nutzungsprotokollen einer Suchmaschine mehrere Nutzer identifizieren, wobei sie nur Telefonbücher und andere öffentliche Informationen zu Hilfe nahm.⁴ Teilweise ergibt sich schon aus den betrachteten Seiten oder eingegebenen Suchworten die Identität des Nutzers einer IP-Adresse.

3. IPv6

Im Zuge der anstehenden Umstellung auf das IPv6-Protokoll ist zu befürchten, dass allen Internetnutzern dauerhaft dieselbe IP-Adresse zugewiesen wird oder dass jedenfalls ein Teil dieser Adresse (Präfix) dauerhaft unverändert bleibt. Telemedienanbieter können dann über ihre gesamten Datenbestände (samt empfangener E-Mails) hinweg recht einfach eine Zuordnung ihrer Surf-Protokolle zur Person eines Nutzers vornehmen. Es genügt, dass sich der Nutzer der IP-Adresse zu irgendeinem Zeitpunkt einmal (bewusst oder unbewusst) identifiziert hat oder dem Anbieter einmal selbst die Identifizierung gelungen ist.

4. Staatliche Telemedien

Der Staat kann Nutzer seiner Internetportale mithilfe von Auskunftersuchen an Internet-Zugangsanbieter legal identifizieren, und zwar nach § 113 TKG in Verbindung mit diversen fachgesetzlichen Erhebungsbefugnissen. Die Fälle des § 113 TKG, die dem Staat eine Identifizierung eröffnen, sind nicht nur theoretisch denkbar, sondern treten praktisch häufig auf. So hat alleine die *Deutsche Telekom AG* im Jahr 2013 mehr als 28.000 Kunden gegenüber Behörden des Bundes und der Länder namhaft gemacht.⁵ Der neu gefasste § 113 TKG wird die Zahl der Identifizierungen nochmals sprunghaft ansteigen lassen, weil erstmals eine Schnittstelle zum automatisierten Datenaustausch vorgesehen ist (§ 113 Abs. 5 Satz 2 TKG).⁶ Vor diesem Hintergrund ist die Annahme nicht vertretbar, die Identifizierung eines Internetnutzers durch den Staat im Zuge von Ermittlungen wegen des Verdachts einer Straftat oder Ordnungswidrigkeit, im Zuge der Gefahrenabwehr oder bei der Wahrnehmung nachrichtendienstlicher Aufgaben lasse sich vernünftigerweise ausschließen.

Im Rahmen der Prüfung der Zulässigkeit einer Verfassungsbeschwerde gegen § 113 TKG hat das *BVerfG* ausgeführt, ausreichend sei die Darlegung, „mit einiger Wahrscheinlichkeit von solchen Maßnahmen berührt zu werden.“ Das *BVerfG* hat dies mit der Begründung angenommen, „dass die durch § 112 Abs. 2 und § 113 Abs. 1 TKG ermöglichten Auskünfte eine große Streubreite haben und Dritte auch zufällig erfassen können.“⁷

Das *BVerfG* hat ausgesprochen, dass der Gesetzgeber mit dem TMG „das Entstehen vermeidbarer Datensammlungen grundsätzlich zu verhindern sucht“. Der Gesetzgeber würde „die Diensteanbieter nach dem TMG grundsätzlich zur Löschung von nicht für die Abrechnung erforderlichen Daten verpflichten (vgl. § 13 Abs. 4 Nr. 2, § 15 TMG) und so auch gegenüber privatwirtschaftlichen Anreizen verhindern, dass die Internetnutzung inhaltlich in allgemeinen kommerziellen Datensammlungen festgehalten wird und damit rekonstruierbar bleibt.“⁸ Diese Ausführungen des *BVerfG* können aber nur zutreffen, wenn ein Personenbezug von IP-Adressen von Internetnutzern angenommen wird. Nur so wird in rechtlicher und tatsächlicher Hinsicht verhindert, dass die Internetnutzung „rekonstruierbar bleibt“, selbst wenn man nur das legale Mittel von Auskünften nach § 113 TKG berücksichtigt.

5. Zwischenergebnis

In vielen Fällen ist eine IP-Adresse bereits dann identifizierbar, wenn man mit den Vertretern der Theorie des „relativen Personenbezugs“ nur die der verantwortlichen Stelle selbst legalerweise zur Verfügung stehenden Mittel berücksichtigen wollte. Das erforderliche Zusatzwissen kann der Anbieter aus anderen Quellen oder Sammlungen haben oder der Nutzer kann es in einem anderen Zusammenhang offenbart haben.⁹ Im Fall staatlicher Internetdienste begründet überdies das Auskunftsrecht nach § 113 TKG einen Personenbezug von IP-Adressen in staatlicher Hand.

³ *Gola/Schomerus* (o. Fußn. 2), § 3 Rdnr. 10 und 44a.

⁴ About AOL search data scandal, abrufbar unter: <http://search-logs.com/aol/about>.

⁵ *Deutsche Telekom AG*, Jahresbericht Auskunft an Sicherheitsbehörden v. 5.5.2014, abrufbar unter: <http://www.telekom.com/sicherheitsbehoerden>.

⁶ Unter dem Az. 1 BvR 1873/13 ist eine Vb des *Autors* u.a. gegen § 113 TKG n.F. anhängig.

⁷ *BVerfG MMR* 2012, 410 m. Anm. *Meinicke*.

⁸ *BVerfGE* 125, 260, 348 Rdnr. 270.

⁹ *Mantz*, *ZD* 2013, 605 m.w.Nw.

Bei strikter Anwendung der „Relativitätslehre“ wäre ein Personenbezug zwar möglicherweise nur derjenigen IP-Adressen anzunehmen, die tatsächlich identifiziert werden dürften. Der speichernden Stelle ist es aber nicht möglich, diejenigen IP-Adressen von einer Datenspeicherung auszunehmen, die sie mit legalen Mitteln identifizieren kann oder später wird identifizieren können. Ist zumindest ein nicht abgrenzbarer Teil der Daten, welche Anbieter über die Nutzer ihrer Internetportale sammeln, personenbezogen, so können die Anbieter dem Datenschutzrecht nur durch Anonymisierung aller Daten gerecht werden.¹⁰

IV. Personenbezug auf Grund des nicht zulässigerweise verfügbaren Zusatzwissens

Fraglich ist indes, ob sich der Personenbezug einer dynamischen IP-Adresse nicht schon allgemein daraus ergibt, dass jedenfalls der Internet-Zugangsanbieter den Kunden identifizieren kann, dem die IP-Adresse zugewiesen ist oder war. Ergibt sich schon aus der objektiven Identifizierbarkeit ein Personenbezug?

1. Grammatikalische Auslegung

Mit dem Wortlaut des § 3 BDSG, des Art. 2 lit. a DS-RL sowie des vom *BVerfG* umschriebenen Grundrechts auf informationelle Selbstbestimmung erscheint es unvereinbar, den Anwendungsbereich des Datenschutzrechts auf Angaben über Personen zu reduzieren, die gerade von der speichernden Stelle ausschließlich mit legalen Mitteln identifiziert werden können. Europarecht, Verfassungsrecht und Bundesrecht stellen bei der Definition des Anwendungsbereichs des Datenschutzrechts darauf ab, ob die Person, auf die sich eine Angabe bezieht, „bestimmbar“ oder „identifizierbar“ ist, ob also die Ermittlung ihrer Identität möglich ist. Im Wortlaut der einschlägigen Normen findet sich kein Anhaltspunkt dafür, dass neben der faktischen Möglichkeit der Identifizierung auch deren rechtliche Zulässigkeit zur Voraussetzung gemacht werden soll.

Als „reale Möglichkeit“ wird im allgemeinen Sprachgebrauch angesehen „das Seinkönnen einer Sache, eines Geschehens, einer Relation, die objektive Denkbarekeit, gemäß den Gesetzen der Erfahrung, der erfahrbaren Wirklichkeit“.¹¹ Unmöglich ist nach dem allgemeinen Sprachverständnis, was entweder den Denkgesetzen oder der wissenschaftlich verarbeiteten Erfahrung widerspricht.¹² Rechtsverletzungen – gerade bei der Verarbeitung personenbezogener Daten – sind zweifellos als reale Möglichkeit anzusehen, wir erleben sie immer wieder. Die Sanktionsbewehrung durch den Gesetzgeber zeigt, dass dieser Rechtsverletzungen für möglich hält.

2. Systematische Auslegung

a) Europarechtskonforme Auslegung

§ 3 BDSG ist europarechtskonform auszulegen und anzuwenden. Die Beschränkung des Anwendungsbereichs des Datenschutzrechts auf Angaben, welche die verarbeitende Stelle selbst mit legalen Mitteln der betroffenen Person zuordnen kann, ist mit der DS-RL unvereinbar. Der einer solchen Einschränkung des Anwendungsbereichs entgegenstehende Wille des Richtliniengebers wird aus den Erwägungsgründen besonders deutlich, in denen es heißt: „26. Die Schutzprinzipien müssen für alle Informationen über eine bestimmte oder bestimmbare Person gelten. 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.“

Zu berücksichtigen sind also auch Daten, die Dritten zur Verfügung stehen, im Fall dynamischer IP-Adressen etwa dem Inter-

net-Zugangsanbieter des Nutzers. Erwägungsgründe zu Richtlinien entfalten zwar keine unmittelbare Wirkung. Nach der Rechtsprechung des *EuGH* ist ein Erwägungsgrund, der genauere Vorgaben als der Richtlinienentwurf enthält, bei der Auslegung der Richtlinie aber zu berücksichtigen.¹³

b) Verfassungskonforme Auslegung

§ 3 BDSG ist daneben auch verfassungskonform auszulegen und anzuwenden. Dass die Bestimmbarkeit nach rein objektiven Gesichtspunkten zu beurteilen ist, ergibt sich schon aus dem Volkszählungsurteil des *BVerfG*. Das *BVerfG* hatte u.a. über eine Regelung zu befinden, welche die Weitergabe pseudonymisierter Volkszählungsfragebögen an Amtsträger und für den öffentlichen Dienst besonders Verpflichtete für wissenschaftliche Zwecke erlaubte.¹⁴ Das *BVerfG* geht bei seiner rechtlichen Würdigung erkennbar davon aus, dass die pseudonymisierten Daten auch nach ihrer Weitergabe an den öffentlich verpflichteten Wissenschaftler, der eine Identifizierung selbst nicht mit legalen Mitteln vornehmen kann, personenbezogen bleiben („indirekter Personenbezug“) und daher weiterhin in den Schutzbereich des informationellen Selbstbestimmungsrechts fallen. Nur auf dieser Grundlage ist die Erörterung der Frage zu erklären, welche Sicherungen und Vorkehrungen der Schutz des informationellen Selbstbestimmungsrechts erfordere. Nur so ist auch die Bezugnahme des Gerichts auf § 5 BDSG zu verstehen, welcher es in der damaligen Fassung den bei der Datenverarbeitung beschäftigten Personen untersagte, „geschützte personenbezogene Daten unbefugt zu einem anderen als dem zur jeweiligen rechtmäßigen Aufgabenerfüllung gehörenden Zweck zu verarbeiten, bekanntzugeben, zugänglich zu machen oder sonst zu nutzen“. Das *BVerfG* hielt das Datenschutzrecht für anwendbar, obwohl die speichernde Stelle die Daten mit legalen Mitteln nicht zuordnen konnte.

c) Systematik des Bundesrechts

Das Bundesrecht bestätigt auch an anderer Stelle, dass der Anwendungsbereich des Datenschutzrechts nicht auf Angaben beschränkt sein soll, welche gerade die verarbeitende Stelle mit legalen Mitteln der betroffenen Person zuordnen kann. So stellt § 3 Abs. 6 BDSG für die Frage der Identifizierbarkeit eines Datums ausschließlich auf den damit verbundenen „Aufwand an Zeit, Kosten und Arbeitskraft“ ab und nicht auf die Frage der rechtlichen Zulässigkeit. Das Gesetz kennt keine „relativ anonymen“ Daten, sondern nur insgesamt anonymisierte Daten.

Auch § 15 Abs. 3 Satz 1 TMG widerlegt das relative Verständnis der Identifizierbarkeit. Die gesetzliche Ermächtigung zur Erstellung pseudonymisierter Nutzungsprofile in § 15 Abs. 3 Satz 1 TMG wäre überflüssig, wenn die Bestimmbarkeit der Nutzer schon durch das bußgeldbewehrte (§ 16 Abs. 2 Nr. 5 TMG) Identifizierungsverbot des § 15 Abs. 3 Satz 3 TMG entfielen.¹⁵ § 16 Abs. 2 Nr. 5 TMG belegt, dass der Gesetzgeber trotz des Verbots der Identifizierung von einer bloßen Pseudonymisierung und damit von einer fortbestehenden Bestimmbarkeit ausgeht.

Sachs meint, § 13 Abs. 6 TMG spreche für den relativen Begriff der Identifizierbarkeit. Hielte man IP-Adressen in der Hand von Telemedienanbietern für personenbezogen, sei es nämlich technisch unmöglich, eine vollständig anonyme Nutzung zu ermöglichen.¹⁶ Dem ist zu widersprechen: Nach § 13 Abs. 6 TMG hat

¹⁰ S. http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_de.pdf, 20.

¹¹ *Eisler*, Wörterbuch der philosophischen Begriffe, 2. Aufl.

¹² *Eisler* (o. Fußn. 11).

¹³ *EuGH* NVwZ 2004, 843 Rdnr. 22.

¹⁴ *BVerfGE* 65, 1, 69 f. Rdnr. 215.

¹⁵ *Ott*, K&R 2009, 308, 311.

¹⁶ *Sachs*, CR 2010, 547, 550.

der Diensteanbieter „die Nutzung von Telemedien und ihre Bezahlung anonym oder unter Pseudonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist“. Die verschiedenen Varianten und das Wort „soweit“ zeigen, dass die Norm nicht in jedem Fall die Möglichkeit einer vollständig anonymen Bereitstellung voraussetzt. I.Ü. ist eine vollständig anonyme Nutzbarkeit z.B. durch Einsatz von Anonymisierungsdiensten möglich. § 13 Abs. 6 TMG ist in letzter Zeit dahin praktisch relevant geworden, dass Anbieter den Einsatz von Anonymisierungsdiensten zur Nutzung ihres Angebots nicht durch Sperr- und Filterlisten unmöglich machen dürfen. Bereits aus diesem Grund ist § 13 Abs. 6 TMG nicht ohne Anwendungsbereich, wenn man IP-Adressen generell als potenziell identifizierbar und personenbezogen ansieht.

3. Historische Auslegung

Die historische Auslegung des § 3 BDSG ist unergiebig, weil die Materialien zu der Streitfrage schweigen.

4. Teleologische Auslegung

In Anbetracht des klaren Wortlauts der einschlägigen Normen ist eine teleologische Auslegung – in Betracht käme wohl nur eine teleologische Reduktion – nicht mehr zulässig. Wollte man sie aber vornehmen, so spricht der Sinn und Zweck des Datenschutzrechts für dessen Anwendbarkeit auf von Dritten identifizierbare Daten:

a) Datenschutzrecht als Missbrauchsvorbeugung

Gegen die Annahme eines Personenbezugs wird angeführt, dem Risiko einer Identifizierung mit rechtswidrigen Mitteln sei hinreichend dadurch begegnet, dass die Zusammenführung der dazu erforderlichen Datenbestände verboten sei, u.U. sogar unter Strafe stehe (§ 206 StGB). Eine solche illegale Handlung lasse sich nicht als normalerweise und ohne großen Aufwand durchzuführende Methode ansehen.

In der Realität ist indes zu beobachten, dass das Datenschutzrecht vielfach missachtet wird und seine Restriktionen Verstöße nicht wirksam verhindern.¹⁷ Zur Speicherung von Verbindungsdaten bei TK-Unternehmen hat das *BVerfG* entschieden, „das Risiko eines Missbrauchs der Verkehrsdaten durch das Telekommunikationsunternehmen oder durch Dritte, die sich unbefugter Zugang zu ihnen verschaffen“, sei „nicht völlig auszuschließen“.¹⁸ Auch eine nur kurzfristige Datenspeicherung berühre das Interesse des Betroffenen in nicht ganz unerheblichem Ausmaß und begründe einen Lösungsanspruch. Zur Vorratsspeicherung von Verkehrsdaten wiederum hat das *BVerfG* entschieden, die „Missbrauchsmöglichkeiten, die mit einer solchen Datensammlung verbunden sind, verschärfen deren belastende Wirkung“. Da die Speicherungspflicht kleinere Diensteanbieter mitbetreffe, stoße die Sicherung vor Missbrauch ungeachtet aller möglichen und erforderlichen Anstrengungen des Gesetzgebers auch in Blick auf deren Leistungsfähigkeit auf strukturelle Grenzen. Mit der Datenansammlung sei „zwangsläufig die Gefahr von Schwachstellen und das Risiko von Manipulationen durch interessierte Dritte“ verbunden.¹⁹

Daraus ergibt sich, dass das *BVerfG* das Risiko von Missbrauch – also von Rechtsverstößen – als nicht nur theoretisches Risiko ansieht, welches „nicht ohne Grund befürchtet werden“ muss. Nie hat das *BVerfG* einen Eingriff in den Schutzbereich der Informationsgrundrechte – also den Anwendungsbereich des Datenschutzes – verneint, weil sich das Risiko eines Datenmissbrauchs praktisch ausschließen lasse.

Das BDSG erhebt das Gebot der Datenvermeidung in § 3a BDSG zum ersten, übergeordneten Gebot des Datenschutzes. Dies macht deutlich, dass sich das Datenschutzrecht nicht darauf beschränken soll, Verletzungen des Persönlichkeitsrechts zu verbieten (dieses Verbot besteht schon nach bürgerlichem Recht). Gegenstand des Datenschutzrechts ist vielmehr ein vorgelagerter Schutz, also die Vorbeugung von Persönlichkeitsrechtsverletzungen. Jeder Mensch soll verhindern können, dass vermeidbare Datensammlungen über ihn überhaupt erst entstehen. Dieser vorgelagerte Schutz des Persönlichkeitsrechts ist weitaus wirksamer. Unterbleibt schon die Ansammlung von Daten, ist ihre missbräuchliche oder versehentliche Verwendung von vornherein ausgeschlossen. Die Vertreter der Theorie des relativen Personenbezugs verkennen diesen Grundgedanken des informationellen Selbstbestimmungsrechts, wenn sie einen Schutz vor Ansammlung mittelbar identifizierbarer Daten nicht für erforderlich erachten. Alleine schon aus der Ansammlung eines solchen Datenschutzes erwachsen Begehrlichkeiten und Risiken von Persönlichkeitsrechtsverletzungen, deren Vermeidung Sinn und Zweck des Datenschutzrechts ist.

Der Einzelne wäre schutzlos gestellt, würde man eine unbeschränkte Sammlung und Speicherung von Informationen über ihn mit dem Argument zulassen, seine Identität könne von der momentan speichernden Stelle mit legalen Mitteln nicht bestimmt werden. Die relativierende Auffassung würde ein Eldorado für Kreditauskunfteien, Detekteien, Werbeunternehmen usw. eröffnen. Diese könnten dann nämlich unbegrenzt sensible Daten über jegliche Personen ansammeln und weitergeben, solange sie nicht den Namen der Betroffenen, sondern nur deren Personalausweisnummer, Kundennummer, Kfz-Kennzeichen, Kontonummer o.Ä. speicherten. Sie könnten sich dann darauf berufen, dass sie selbst die Betroffenen mit legalen Mitteln nicht bestimmen könnten. Die Betroffenen müssten aber befürchten, dass die Zuordnung der Kennnummer jederzeit vorgenommen werden und dadurch Aufschluss über ihr Verhalten und ihre Persönlichkeit gewonnen werden könnte. Dies uneingeschränkt zuzulassen, wäre mit dem Grundrecht auf informationelle Selbstbestimmung offensichtlich unvereinbar. Sich darauf zu verlassen, dass es nie zu einer Zuordnung kommen werde, wäre aller Erfahrung nach unverantwortlich.

Ob und wie pseudonymisierte Datensammlungen verwendet oder weitergegeben werden, kann der Betroffene weder überschauen noch verhindern. Schon alleine das Risiko einer unkontrollierbaren Wissensnutzung und -generierung kann Menschen in ihrer Freiheit wesentlich hemmen, aus eigener Selbstbestimmung zu planen oder zu entscheiden.

Insgesamt ist festzuhalten, dass es der Sinn und Zweck des Datenschutzes, die unbefangene Ausübung von Grundrechten zu gewährleisten, gebietet, die Schutzvorschriften auch auf Daten zu erstrecken, die aktuell nicht mit legalen Mitteln identifizierbar sind. Denn schon die – erfahrungsgemäß nicht unbegründete – Befürchtung von Nachteilen infolge einer Identifizierung beeinträchtigt die freie Entfaltung der Persönlichkeit. Die Menschen sehen ein reales Risiko von Datenmissbrauch und richten ihr Verhalten darauf ein. Die Rechtsordnung muss dem Rechnung tragen. Dies ermöglicht die Theorie des „relativen Personenbezugs“ nicht. Dass ein Datum bei der aktuell speichernden Stelle „relativ anonym“ sein mag, beruhigt im Zeitalter des Internet niemanden und gewährleistet keinen wirksamen Schutz. Die Vertreter dieser Auffassung vermögen auch nicht schlüssig zu erklären, warum die Anbieter von einer wirksamen Anonymisierung mit Nutzungsende absehen, obgleich eine Identifizierung doch angeblich nie erfolgen soll. Die identifizierbare Speicherung lässt sich in Wahrheit nur so erklären, dass die Möglichkeit einer Identifizierung offen gehalten werden soll.

¹⁷ S. nur die Datenbank von Datenschutzverletzungen, abrufbar unter: www.projekt-datenschutz.de.

¹⁸ *BVerfG* NJW 2007, 3055 Rdnr. 17.

¹⁹ *BVerfGE* 125, 260, 320 Rdnr. 212.

b) Das Argument der Strafverfolgungsvorsorge

Motivation der Vertreter eines „relativen Personenbezugs“ von IP-Adressen mag teilweise die Befürchtung sein, Straftaten und andere Rechtsverletzungen im Internet könnten ohne Protokollierung der Internetnutzung generell nicht mehr verfolgt werden.²⁰ Immerhin hat auch das *BVerfG* eine Vorratsdatenspeicherung von IP-Adressen nicht schlechthin für unverhältnismäßig erklärt, weil „das Internet keinen rechtsfreien Raum bilden“ dürfe.²¹ Diese Argumentation zur Ablehnung eines Personenbezugs von IP-Adressen heranzuziehen, ist jedoch in mehrfacher Hinsicht nicht haltbar:

Es ist bereits methodisch unzulässig, den Anwendungsbereich des Datenschutzes anhand von Eingriffsinteressen zu bestimmen. Das *BVerfG* hat schon früh deutlich gemacht, dass eingriffsorientierte Gesichtspunkte bei der Definition des Schutzbereichs eines Grundrechts keinen Platz haben.²² Grundrechtliche Schutzbereiche ließen sich „nicht nach Eingriffsnotwendigkeiten zuschneiden“. Die Möglichkeit von Grundrechtsmissbräuchen könne ein rechtfertigender Grund für Grundrechtsbeschränkungen, nicht aber für Schutzbereichsbegrenzungen sein.

Ferner wäre die Annahme falsch, ohne eine anlasslose und unterschiedslose Vorratsspeicherung der Internetnutzung seien Straftaten im Internet generell nicht verfolgbar. Das Gegenteil beweist bereits die amtliche Kriminalstatistik. Laut *BKA*²³ wurde im Jahr 2012 in Deutschland im Bereich der Internetkriminalität eine Aufklärungsquote von 60,1% erzielt, und zwar unter Geltung des Lösungsgebots des § 15 TMG. Die Aufklärungsquote von Internetdelikten übersteigt die durchschnittliche Aufklärungsquote registrierter Straftaten von 54,4% deutlich. Dasselbe ergibt sich für die einzelnen Deliktsbereiche: Betrugsdelikte im Internet werden häufiger aufgeklärt als sonstige Betrugsdelikte. Datenveränderung und Computersabotage werden häufiger aufgeklärt als Sachbeschädigungen.

Eine anlasslose, dauerhafte und flächendeckende Vorratsspeicherung der Internetnutzung wäre auch auf Grundlage der Rechtsprechung des *BVerfG* eklatant unverhältnismäßig. Laut *BVerfG* sei „maßgeblich für die Rechtfertigungsfähigkeit“ einer Vorratsdatenspeicherung, „dass sie nicht direkt durch staatliche Stellen erfolgt, dass sie nicht auch die Kommunikationsinhalte erfasst und dass auch die Speicherung der von ihren Kunden aufgerufenen Internetseiten durch kommerzielle Diensteanbieter grundsätzlich untersagt ist.“²⁴ Außerdem erforderlich sei die „gesetzliche Gewährleistung eines besonders hohen Standards der Datensicherheit“,²⁵ die gesetzliche Beschränkung der Datennutzung auf die „Ahndung von Straftaten, die überragend wichtige Rechtsgüter bedrohen oder zur Abwehr von Gefahren für solche Rechtsgüter“,²⁶ ein Richtervorbehalt für die Abfrage oder Übermittlung der Daten²⁷ und eine nachträgliche Benachrichtigung der Betroffenen.²⁸

An jeder einzelnen dieser verfassungsrechtlichen Anforderungen fehlt es im vorliegenden Zusammenhang: Eine Protokollierung des Internet-Nutzungsverhaltens durch Telemedienanbieter würde im Fall staatlicher Portale direkt bei staatlichen Stellen erfolgen. Sie würde auch den Inhalt der abgerufenen oder eingegebenen Informationen umfassen und kommerziellen Diensteanbietern die Speicherung der von ihren Kunden aufgerufenen Internetseiten ermöglichen. Es existiert keinerlei gesetzliche Gewährleistung für die Sicherheit der Datenbestände. Nach den §§ 15 Abs. 5 Satz 4, 14 Abs. 2 TMG ist die Datennutzung nicht gesetzlich beschränkt auf die „Ahndung von Straftaten, die überragend wichtige Rechtsgüter bedrohen oder zur Abwehr von Gefahren für solche Rechtsgüter“, und es existiert auch kein Richtervorbehalt; ebenso wenig ist eine Benachrichtigung von Datenübermittlungen vorgesehen.

Vor allem betrifft eine Speicherung des Internet-Nutzungsverhaltens den Inhalt der Internetnutzung und hat damit eine andere Qualität als eine Speicherung von Verbindungsdaten. Eine Vorratsspeicherung der Inhalte der Internetnutzung kann niemals verhältnismäßig sein; sie ist selbst nach der Rechtsprechung des *BVerfG* ausgeschlossen (vgl. auch § 113a Abs. 8 TKG a.F.).

Schließlich sei darauf hingewiesen, dass die Verneinung des Personenbezugs von IP-Adressen mit dem Ziel der Erleichterung der Verfolgung von Rechtsverletzungen zu einem widersprüchlichen Ergebnis führen würde: Anbieter von Telemedien dürften danach das Nutzungsverhalten nur dann zur Verfolgungsvorsorge speichern, wenn sie den Nutzer nicht identifizieren könnten und deswegen § 15 TMG nicht anwendbar wäre. Dies führte zu dem Ergebnis, dass ein Surfer durch Identifizierung und Anmeldung auf einem Internetportal spurlos surfen und Informationen veröffentlichen könnte, was das Ziel der Verfolgungsvorsorge ad absurdum führen würde. Dies kann der Gesetzgeber nicht gewollt haben.

5. Widersprüche der Theorie des „relativen Personenbezugs“

Die Theorie des „relativen Personenbezugs“ überzeugt auch aus sich heraus nicht. Nach ihr soll das Datenschutzrecht nämlich zwar nicht für die Speicherung, wohl aber für die Übermittlung „relativ“ personenbezogener Daten an eine Stelle mit Zusatzwissen gelten. Diese in freier Rechtsschöpfung vorgenommene Unterscheidung findet keinerlei Stütze im Gesetz. Die gesetzlichen Regelungen sowohl der Datenspeicherung wie auch der Datenübermittlung beziehen sich gleichermaßen auf personenbezogene Daten. Es ist in sich widersprüchlich, dass ein und dasselbe Datum für ein und dieselbe Stelle einmal (bei der Speicherung) nicht personenbezogen, ein andermal (bei der Übermittlung) aber personenbezogen sein soll.

Nicht überzeugend ist auch, dass eine Identifizierbarkeit mit rechtswidrigen Mitteln nur dann außer Betracht bleiben soll, wenn das erforderliche Zusatzwissen bei einem Dritten liegt, nicht aber, wenn es bei der speichernden Stelle selbst liegt. Wäre die Identifizierbarkeit tatsächlich nur unter Berücksichtigung legaler Mittel zu bestimmen, müsste schon eine rechtlich abgesicherte Pseudonymisierung den Personenbezug entfallen lassen (entgegen § 15 Abs. 3 TMG).

Die Vertreter der relativierenden Auffassung versuchen, den uneingeschränkten gesetzlichen Begriff der Bestimmbarkeit ad absurdum zu führen mit dem Argument, dass letztlich „alle Daten in einer bestimmten Kombination und mit geeignetem Zusatzwissen wieder auf bestimmte Personen zurückbezogen werden“ könnten und dass bei zutreffender Auslegung des Merkmals der Bestimmbarkeit „alle nur denkbaren Daten dem Datenschutzrecht unterfallen“ würden. Dies ist falsch, denn durch eine wirksame Anonymisierung lässt sich ein Personenbezug jederzeit ausschließen. Anonyme Daten einschließlich anonymer Internet-Nutzungsprotokolle sind nicht personenbezogen und unterliegen nicht dem Datenschutzrecht. Dementsprechend haben die Datenschutz-Aufsichtsbehörden in ihrem B. v. 26./27.11.2009 nicht jede Aufzeichnung von IP-Adressen als unzulässig bezeichnet, sondern die hinreichend verkürzte Aufzeich-

²⁰ So *LG Berlin* ZD 2013, 625.

²¹ *BVerfGE* 125, 260, 343 Rdnr. 260.

²² *BVerfGE* 85, 386, 397 Rdnr. 49.

²³ Polizeiliche Kriminalstatistik 2012.

²⁴ *BVerfGE* 125, 260, 324 Rdnr. 218.

²⁵ *BVerfGE* 125, 260, 325 Rdnr. 221.

²⁶ *BVerfGE* 125, 260, 328 Rdnr. 227.

²⁷ *BVerfGE* 125, 260, 337 Rdnr. 247.

²⁸ *BVerfGE* 125, 260, 336 Rdnr. 243.

nung von IP-Adressen für zulässig erachtet.²⁹ Wird eine IP-Adresse etwa durch Verkürzung um zwei Byte wirksam anonymisiert, so unterfällt sie dem Datenschutzrecht ebenso wenig wie sonstige anonyme Daten über das Internet-Nutzungsverhalten.

6. Zwischenergebnis

Die Auslegung ergibt, dass bei der Frage der Bestimmbarkeit der Person, auf die sich eine Angabe bezieht, alle vernünftigerweise dem Verantwortlichen für die Verarbeitung oder einem Dritten zur Verfügung stehenden Mittel zu berücksichtigen sind. Ob die Identifizierung gegen Rechtsvorschriften verstoßen würde, spielt keine Rolle. Für den praxisrelevanten Fall der dynamisch zugewiesenen IP-Adressen gilt danach: Da jedenfalls der Internet-Zugangsanbieter regelmäßig eine Identifizierung seiner Kunden anhand von IP-Adresse und Zeitpunkt des Zugriffs vornehmen kann, sind dynamisch zugewiesene IP-Adressen als personenbezogene Nutzungsdaten i.S.d. § 15 TMG zu behandeln. Sie sind auf die Person des Inhabers des genutzten Internetan-

schlusses bezogen. Selbst wenn der genaue Zeitpunkt des Zugriffs unbekannt ist, genügt eine ausreichende zeitliche Eingrenzung, um eine dynamische IP-Adresse zuordnen zu können.

V. Fazit

§ 3 BDSG, Art. 2 lit. a DS-RL sowie das Grundrecht auf informationelle Selbstbestimmung gebieten es, Internet-Protokolladressen stets als personenbezogene Daten zu behandeln. Namentlich ist auch die dynamisch zugewiesene IP-Adresse des Nutzers, die im Zusammenhang mit der Nutzung öffentlich zugänglicher Telemedien im Internet übertragen wird, als personenbezogen anzusehen. Vorausgesetzt ist nicht, dass der Anbieter des Telemediums selbst die Identifizierung vornehmen kann. Die einzige Möglichkeit zur Beseitigung des Personenbezugs einer IP-Adresse ist ihre Anonymisierung im Wege der hinreichenden Verkürzung.



Patrick Breyer

ist Landtagsabgeordneter in Schleswig-Holstein, Themenbeauftragter der Piratenpartei für Datenschutz und Mitglied im Arbeitskreis Vorratsdatenspeicherung.

²⁹ Oberste Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich, B. v. 26./27.11.2009, abrufbar unter: <https://www.datenschutz-mv.de/datenschutz/themen/bschlue/Analyse.pdf>.