FIZ Karlsruhe

Leibniz-Institut für Informationsinfrastruktur

Karlsruher Institut für Technologie

universität innsbruck

Deutscher Bundestag
1. Untersuchungsausschuss
der 18. Wahlperiode

MAT A SV-19a

zu A-Drs.: 574 a

Deutscher Bundestag
1. Untersuchungsausschuss
28. Feb. 2017

Sachverständigengutachten zur Anhörung des 1. Untersuchungsausschusses des Deutschen Bundestages der 18. Wahlperiode zum Thema:

„Wie bzw. auf welche unterschiedliche Art und Weise wird der Begriff der Verkehrs- und Nutzungsdaten wissenschaftlich im technischen und juristischen Kontext gebraucht? Wie ist dieser vom Begriff der Metadaten abzugrenzen?"

(Beweisbeschluss SV-19a vom 15. Dezember 2016)

Autoren:

Prof. Dr. Franziska Boehm[1]

Prof. Dr. Rainer Böhme[2]

Markus Andrees[3]

[1] Die Verfasserin ist Bereichsleiterin für Immaterialgüterrecht am FIZ Karlsruhe – Leibniz-Institut für Informationsinfrastruktur GmbH und Professorin für Immaterialgüterrecht am Karlsruher Institut für Technologie (KIT).

[2] Der Verfasser ist Professor für Informatik und Leiter des Security and Privacy Lab an der Universität Innsbruck.

[3] Der Verfasser ist wissenschaftlicher Mitarbeiter und Doktorand am Institut für Internet-, Telekommunikations- und Medienrecht (ITM) der Westfälischen Wilhelms-Universität in Münster.

Inhaltsverzeichnis

A. Vorbemerkungen

Dieses Sachverständigengutachten beantwortet die Fragen des 1. Untersuchungsausschusses der 18. Wahlperiode des Bundestages zur juristischen und technischen Auseinandersetzung mit dem Begriff der Metadaten im Zusammenhang mit technischen Kommunikationssystemen (Beweisbeschluss SV-19a vom 15. Dezember 2016).

Zunächst wird kurz die Methodik erläutert. Im Anschluss daran werden die Fragen des Beweisbeschlusses in der dort genannten Reihenfolge beantwortet

Für die Verwendung der in den Fragen genannten Begriffe im **technischen Kontext** gibt es keine verbindliche Quelle. Um eine gewisse Intersubjektivität zu gewährleisten, wurden die von der Internet Engineering Task Force (IETF) herausgegebenen Request for Comments (RFCs) als Quellen für den Gebrauch von Begriffen im technischen Kontext herangezogen und systematisch untersucht. Zwischen April 1969, dem Zeitpunkt der Veröffentlichung von RFC 1, und Dezember 2016 liegen insgesamt 7929 RFCs vor. RFCs werden überwiegend von Ingenieuren verfasst und unterliegen einem Qualitätssicherungsprozess mit Möglichkeiten zur Stellungnahme. Sie gelten als de-facto Standardisierungsdokumente für die im Internet verwendeten Protokolle und sind maßgebliche Referenz bei deren Implementierung in technische Systeme. Auch wissenschaftliche Veröffentlichungen zur Internet-Technik beziehen sich in der Regel auf RFCs. Die Sachverständigen sind der Meinung, dass sich der Gebrauch von Begriffen im technischen Kontext durch ihre Verwendung – in englischer Übersetzung – in RFCs widerspiegelt und die durch die Analyse der RFCs gewonnenen Einsichten repräsentativ für die relevante technische Domäne sind.

Bei der Bestimmung von Begriffen im **juristischen Kontext** wurden die verfügbaren Quellen aus nationalen, internationalen und EU Gesetzen und Gesetzgebungsprozessen sowie aus nationaler und internationaler Literaturrecherche und Rechtsprechung ausgewertet, analysiert und kontextbezogen eingeordnet.

B. Wie bzw. auf welche unterschiedliche Art und Weise wird der Begriff der Verkehrs- und Nutzungsdaten wissenschaftlich im technischen und juristischen Kontext gebraucht? Wie ist dieser vom Begriff der Metadaten abzugrenzen?

I. Verkehrsdaten im juristischen Kontext

Der Begriff **Verkehrsdaten** ist ein „terminus technicus", dem aus juristischer Sicht eine eindeutige Bedeutung zugemessen wird. Er ist legal definiert in § 3 Nr. 30 TKG. Dort heißt es: „Verkehrsdaten sind Daten, die bei der Erbringung eines Telekommunikationsdienstes (TK-Dienst) erhoben, verarbeitet oder genutzt werden."

Sämtliche Daten, die bei der jeweiligen Inanspruchnahme eines TK-Dienstes entstehen, sind in diese Kategorie einzuordnen. Konkrete Beispiele sind Beginn, Dauer und Ende einer Verbindung, Rufnummern der Teilnehmer, Standorte der Teilnehmer bei Einsatz von Mobilfunkgeräten sowie die

Datenmenge einer Nachricht.[4] Außerdem fallen unter die Verkehrsdaten Leitwege, das verwendete Protokoll, Format der Nachricht, das Netz, von dem die Nachricht ausgeht bzw. an das gesendet wird, die in Anspruch genommene Telekommunikationsdienstleistung, die Endpunkte von festgeschalteten Verbindungen sowie deren Zeitpunkt und Dauer und sonstige zum Aufbau und zur Aufrechterhaltung sowie zur Entgeltabrechnung erforderlichen Verbindungsdaten.[5]

Die Legaldefinition geht auf die Definition in Art. 2 lit. b RL 2002/58/EG zurück.[6] Mit der Umsetzung in nationales Recht wurde der bis dahin genutzte Begriff der Verbindungsdaten ersetzt. In diesem Zusammenhang wurde der Anwendungsbereich auf alle Arten der Übertragung elektronischer Nachrichten erweitert und damit der Begriff von der Fokussierung auf Anrufe gelöst.[7] Verkehrsdaten gehören zu den datenschutzrechtlich sensibelsten Daten, da sich aus ihnen Rückschlüsse auf bestimmte Umstände der Kommunikation schließen lassen.[8] Sie unterfallen dem Schutz des Fernmeldegeheimnisses aus Art. 10 Abs. 1 GG.[9] Auf die Legaldefinition in § 3 Nr. 30 TKG nehmen eine Reihe von Bestimmungen außerhalb des TKG Bezug: § 101 Abs. 9 UrhG; § 140b Abs. 9 PatG; § 24b Abs. 9 GebrMG; § 19 Abs. 9 MarkenG; § 46 Abs. 9 GeschmMG und § 37b Abs. 9 SortSchG. Dies unterstreicht die über das TKG hinausgehende allgemeingültige rechtliche Bedeutung dieses Begriffs.

II. Verkehrsdaten im technischen Kontext

Der Begriff „traffic data" wird in weniger als 30 RFCs verwendet. Erstmals taucht er im Jahr 1990 in RFC 1168 auf. Dort bezieht er sich auf die Anzahl der Nachrichten in einem bestimmten Zeitraum, also statistische Daten über die Umstände mehrerer Kommunikationsvorgänge. Vergleichbar eng wird der Begriff in RFC 5472 (2009) und RFC 7937 (2016) verwendet.

Andere RFCs weiten den Begriff aus. RFC 2041 (1996) verwendet „traffic data" synonym für die Ausgabe von tcpdump, einem Standardprogramm das den kompletten Netzverkehr mitschneiden kann. Diese Verwendung, welche in mehreren RFCs anzutreffen ist, impliziert Inhalte wie Umstände von Kommunikationsvorgängen. Die Einbeziehung von Kommunikationsinhalten geht auch explizit aus RFC 6561 (2012) hervor, die sich mit der Erkennung von Schadsoftware durch Analyse der Nutzdaten auf der Anwendungsschicht befasst.[10]

Auffällig ist die Verwendung des Begriffes in Zusammenhängen mit Regulierung. RFC 4084 (2005) verwendet den Begriff im Abschnitt „wiretapping and interception". Sie unterscheidet zwischen Abhören zur Echtzeit und Vorratsdatenspeicherung, nicht aber zwischen Kommunikationsinhalten und –umständen. RFC 5982 (2010) verwendet den Begriff im Zusammenhang mit zu gewährleistender Vertraulichkeit von erhobenen und auf Vorrat gespeicherten Verkehrs- und Inhaltsdaten. Bezüge zum Datenschutz sind in RFC 6235 (2011), RFC 7373 (2014) und RFC 7626 (2015) zu finden. Es handelt sich aber um eher allgemeine Hinweise, bspw. „consider omitting

---

[4] *Graf*, in: Beck'scher Online-Kommentar, § 3 TKG, Rn. 20.
[5] *Ricke*, in: Spindler/Schuster, § 3 TKG, Rn. 49.
[6] *Braun*, in: Geppert/Schütz, § 3 TKG, Rn. 93.
[7] *Ohlenburg*, MMR 2003, 82, 83. Zur Entsprechung mit Begriff dem Verbindungsdaten, vgl: *Ohlenburg*, MMR 2004, 431, 434.
[8] *Braun*, in: Geppert/Schütz, § 3 TKG, Rn. 93.
[9] *BVerfG*, Beschl. v. 24.1.2012 - 1 BvR 1299/05, BVerfGE 130, 151, Rn. 128 = NJW 2012, 1419, 1421; Urt. v. 27.2.2008 - 1 BvR 370/07, 1 BvR 595/07, BVerfGE 120, 274, Rn. 183 = NJW 2008, 822, 825; Urt. v. 27.7.2005 - 1 BvR 668/04, BVerfGE 113, 348, Rn. 82 = NJW 2005, 2603, 2609; Urt. v. 12.03.2003 - 1 BvR 330/96, 1 BvR 348/99, BVerfGE 107, 299, Rn. 50 = NJW 2003, 1787, 1788.
[10] Die Betrachtung von elektronischer Kommunikation in Schichten wird unten unter Frage B, Teil VI, Abschn. 1 näher erläutert.

especially privacy-sensitive values"[11] oder „Interpreting general privacy laws [...] in the context of DNS traffic data is not an easy task".[12]

Interessant ist weiterhin RFC 7687 (2015), die eine Beziehung zwischen den Begriffen „traffic data" und „metadata" herstellt. Auf sie wird unten in Frage B, Teil VI, Abschn. 1 näher eingegangen.

Festzuhalten ist, dass der Begriff Verkehrsdaten bzw. dessen englische Übersetzung keine feststehende Bedeutung im technischen Kontext hat und insgesamt relativ selten verwendet wird.

III. Nutzungsdaten im juristischen Kontext

Der Begriff der **Nutzungsdaten** ist ebenfalls ein „terminus technicus". Der aus juristischer Sicht entscheidende Inhalt wird im Rahmen von § 15 TMG festgelegt. Diese Norm beruht auf § 6 Abs. 1 TDDSG, dem Vorgängergesetz des TMG. Danach waren Nutzungsdaten als „insbesondere a.) Merkmale zur Identifikation des Nutzers, b.) Angaben über Beginn und Ende sowie über den Umfang der jeweiligen Nutzung und c.) Angaben über die vom Nutzer in Anspruch genommenen Teledienste" definiert. Da es sich bei dieser Aufzählung um einen nicht umfassenden Beispielskatalog handelte, waren weitere Datenkategorien nicht ausgeschlossen.

In § 15 TMG heißt es nun: „Der Diensteanbieter darf personenbezogene Daten eines Nutzers nur erheben und verwenden, soweit dies erforderlich ist, um die Inanspruchnahme von Telemedien zu ermöglichen und abzurechnen (Nutzungsdaten)." Diese Legaldefinition vermischt jedoch Zulässigkeitsvoraussetzungen und Definition.[13] Eindeutiger ist die Definition in der Gesetzesbegründung: „Nutzungsdaten sind personenbezogene Daten, die dem Nutzer die Nachfrage nach Telediensten ermöglichen; es handelt sich dabei um Daten, die während der Nutzung eines Teledienstes, z. B. Interaktionen des Nutzers mit dem Diensteanbieter, entstehen."[14] Nutzungsdaten können eine große Nähe zu den Kommunikationsinhalten aufweisen und deswegen die Verkehrsdaten in ihrer Sensitivität noch übertreffen.[15]

IV. Nutzungsdaten im technischen Kontext

Der Begriff der **Nutzungsdaten** wird in technischen Zusammenhängen selten gebraucht. Die einzige Definition in einem RFC setzt den Begriff „usage data" quasi Verkehrsdaten gleich.[16] Ähnlich gelagert ist die Verwendung im Sinne der Bandbreitennutzung in zwei RFCs.[17] Die meisten RFCs , die „usage data" enthalten, verwenden den Begriff im Zusammenhang mit Abrechnungszwecken.[18] Lediglich in RFC 3881 (2004) findet sich ein Bezug zur Zugriffsüberwachung für Anwendungen im Gesundheitsbereich.

Insgesamt erscheint der juristische Fachterminus „Nutzungsdaten" für die Definition und Implementierung von Standards zu unspezifisch. Stattdessen würden Techniker Begriffe wählen, die

---

[11] RFC 7373 (2014), S. 10.
[12] RFC 7626 (2015), S. 12.
[13] *Spindler/Nink*, in: Spindler/Schuster, § 15 TMG, Rn. 2.
[14] BT-Drs. 13/7385, S. 24.
[15] *Dix/Schaar*, in: Roßnagel, § 15 TMG, Rn. 23.
[16] RFC 2063 (1997): „Within this document the term ‚usage data' is used as a generic term for the data obtained using the traffic flow measurement architecture." Ebenso RFC 2722 (1999). Ähnlich gleichsetzend RFC 3272 (2002): „such as the number of packets and bytes for each group".
[17] RFC 4546 (2006), RFC 6057 (2010)
[18] Insb. RFC 2975 (2000), auch RFC 2707 (1999) im Zsh. mit Drucker-Nutzung, RFC 2721 (1999), RFC 2924 (2000), RFC 3141 (2001), RFC 3752 (2004), RFC 3955 (2004) und RFC 6208 (2011) im Zsh. mit Cloud-Nutzung.

entweder auf den konkreten Zweck der Daten hinweisen (z.B. Benutzerkennung, Passwort, Anzahl und Zeitpunkt von Login(-versuchen), Sitzungs- bzw. Session-Kennung, Länge oder Anzahl der übertragenen Datensätze) oder, falls es zur persistenten Speicherung kommt, die Art der Datenhaltung beschreiben (z.B. allgemein Log-Daten, Sitzungsverlauf, Transaktionshistorie, Zugriffsstatistik).

V. Das Verhältnis von Verkehrsdaten zu Nutzungsdaten

Das Verhältnis von Nutzungsdaten zu Verkehrsdaten lässt sich plastisch anhand zweier Kreise beschreiben, die gewisse Schnittmengen aufweisen, ohne vollständig deckungsgleich zu sein. Am Beispiel einer IP-Adresse zeigt sich, dass ein und dasselbe Datum sowohl Nutzungs- als auch Verkehrsdatum sein kann. Umgekehrt ist beispielsweise ein Login-Datum bestehend aus Nutzerkennung und Passwort für ein Telemedium lediglich ein Nutzungsdatum.

Ob von Nutzungs- oder Verkehrsdaten zu sprechen ist, hängt davon ab, in welchem Zusammenhang die Daten verarbeitet werden. Anbieter von TK-Diensten unterliegen rechtlichen Beschränkungen, sofern sie Verkehrsdaten verarbeiten. Anbieter von Telemedien sind in der Datenverarbeitung eingeschränkt, sofern es sich um Nutzungsdaten handelt.

Da die Einordnung eines Dienstes als TK-Dienst oder Telemedium in Zeiten der Medienkonvergenz Schwierigkeiten bereitet[19], schlägt diese Einordnungsproblematik auch auf die Zuordnung zu den beiden Datenkategorien durch. Vor diesem Hintergrund erklärt sich das Bemühen um einen abstrakteren Begriff, wie den der Metadaten, auf den zurückgegriffen werden kann, wenn es nicht um einen Datenumgang durch Anbieter von TK-Diensten oder Telemedien geht.

VI. Abgrenzung des Begriffes der Verkehrs- und Nutzungsdaten vom Begriff der Metadaten

1. Technische Vorbemerkungen

Um sich der Klärung des Begriffes Metadaten anzunähern, müssen verschiedene Arten von Daten unterschieden werden. Dafür ist es erforderlich, sich den grundsätzlichen Aufbau moderner elektronischer Kommunikationssysteme zu vergegenwärtigen. Ihre wesentlichen Merkmale sind:

- Digitale Übertragung: Kommunikationsinhalte werden digitalisiert und beim Empfänger bei Bedarf in analoge Signale umgewandelt.
- Digitale Vermittlung: Der Leitweg wird von Digitalrechnern festgelegt. Zur Adressierung kommen dabei zum Kommunikationszeitpunkt eindeutige Kennungen der Endgeräte zum Einsatz.
- Dienstintegration: Viele verschiedene Anwendungen werden über die gleiche physikalische Kopplung von Geräten bereitgestellt.
- Heterogenität: Weltweite Kommunikation durchläuft eine Vielzahl von mit unterschiedlichen Technologien realisierten Teilnetzen, deren Kopplungselemente die übertragenen Daten regelmäßig und automatisch umschreiben, um sie an die unterschiedlichen Standards anzupassen.

[19] Deutlich wird dies insbesondere an dem Umgang mit OTT-Diensten: *VG Köln*, Urt. v. 11.11.2015 - 21 K 450/15 (nicht rechtskräftig), MMR 2016, 141; Vgl. dazu auch: *Grünwald/Nüßing*, MMR 2016, 91; *Schumacher*, K&R 2015, 771; *Gersdorf*, K&R 2016, 91; *Kühling/Schall*, CR 2015, 641.

Insbesondere die Internet-Kommunikation ist darüber hinaus paketvermittelt. Digitale oder digitalisierte Kommunikationsinhalte werden in eine Folge von Datenpakete aufgeteilt und jeweils einzeln im Netz vermittelt und übertragen. Jedes Datenpaket enthält mindestens eine eindeutige Kennung des Empfangsgeräts, in der Regel eine eindeutige Kennung des Sendegeräts sowie eine eindeutige Ordnungsnummer des Datenpakets innerhalb der Sequenz.

Zur Beherrschung der erheblichen Entwurfskomplexität von modernen Kommunikationssystemen kommen Schichtmodelle als Abstraktionstechnik zum Einsatz. In Reinform werden alle Kommunikationsstandards genau einer Schicht zugeordnet und unabhängig von anderen Schichten definiert und implementiert. Grundsätzlich bedienen sich höhere Schichten der Dienste niedriger Schichten und verfeinern diese durch zusätzliche bereitgestellte Funktionalität. Schnittstellen definieren die Übergabepunkte zwischen den Schichten. Beispielsweise legt die unterste Schicht 1 die Übersetzung von logischen Symbolen in physikalische Größen fest, welche sich auf einem Übertragungsmedium ausbreiten. Schicht 2 darüber fügt Fehlerkorrekturverfahren hinzu, um den Einfluss von Störungen zu begrenzen. Der modulare Aufbau von Schichtarchitekturen reduziert die Entwurfskomplexität moderner Kommunikationssysteme: Schicht 2 kann unabhängig vom Übertragungsmedium (z.B. kabelgebundene elektrische Signale, kabelgebundene Lichtsignale, kabellose elektromagnetische Wellen) spezifiziert und implementiert werden. In einem konkreten Kommunikationssystem wird lediglich die zu den technischen Gegebenheiten passende Implementierung von Schicht 1 verwendet. Weiterhin wird Dienstintegration durch alternative Implementierung höherer Schichten realisiert, die sich alle niedrigeren Schichten teilen. Die Kopplung heterogener Teilnetze erfolgt schließlich durch parallele Implementierung von einer oder mehreren niedrigeren Schichten.

Die Verwendung von Schichtmodellen ist für die technische Bestimmung des Metadaten-Begriffes erheblich, denn welche Informationen Kommunikationsinhalt bzw. Kommunikationsumstände (welche den Metadaten zuzuordnen wären, vgl. dazu ausführlich Frage B, Teil VI) darstellen, hängt von der betrachteten Schicht ab. Abbildung 1 illustriert dies beispielhaft anhand von paketvermittelter Internet-Kommunikation.

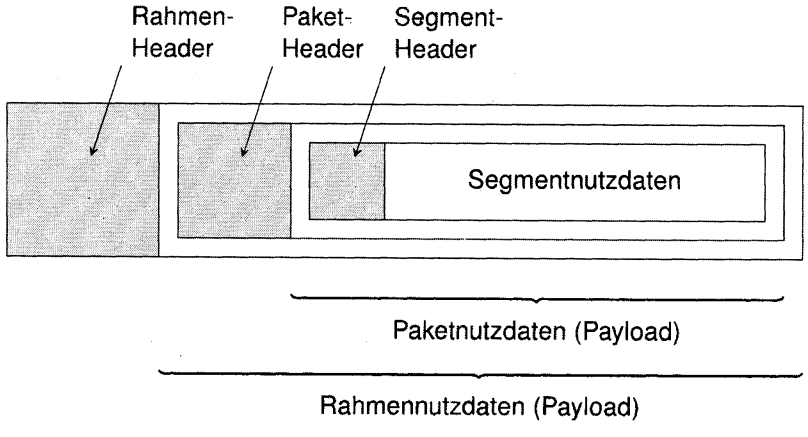

Abb. 1. Verschachtelung von Kommunikationsinhaltsdaten und Kommunikationsumstandsdaten über die Schichten 2 bis 4 des TCP/IP-Schichtmodells bei der Internet-Kommunikation[20]

[20] Bildquelle: *Böhme*, Vorlesungsfolienskript „Rechnernetze und Internettechnik", Universität Innsbruck, 2015.

Der Begriff des Pakets wird beim TCP/IP-Schichtmodell der Internet-Kommunikation im engeren Sinne nur auf Schicht 3, der sog. Vermittlungsschicht, verwendet. Diese Schicht implementiert das IP-Protokoll. Den Paketnutzdaten wird ein Paket-Header (Kopf) vorangestellt, welcher inhaltsbeschreibende (z.B. Länge) sowie inhaltsergänzende, hauptsächlich vermittlungsrelevante Informationen enthält. Beispielweise befinden sich die IP-Adressen von Sender und Empfänger im Paket-Header. Trotzdem wäre es voreilig, die Paketnutzdaten als Kommunikationsinhalte zu betrachten und die im Paket-Header enthaltenen Einträge als Daten über die Kommunikationsumstände. Denn die Nutzdaten auf Schicht 3 enthalten Header-Daten von Schicht 4, der sog. Transportschicht. Diese Schicht implementiert u.a. das TCP-Protokoll. Datenpakete werden hier als Segmente bezeichnet. Eine Trennung von Daten zu Kommunikationsinhalten bzw. -umständen auf Basis von technischen Standards und Konventionen ist damit nur möglich, wenn die für den Betrachter relevante Schicht festgelegt ist. Dies schränkt die Möglichkeit einer pauschalen Abgrenzung verschiedener, in technischen Kommunikationssystemen auftretender Datenarten ein.

Einfache Faustregeln zur Umgehung dieser Festlegung gibt es nicht. Stets die niedrigste Schicht anzunehmen, würde einen Großteil der Verkehrs- und Metadaten fälschlich als Kommunikationsinhalte klassifizieren. Stets die höchste Schicht anzunehmen, gebietet sich nicht, denn dienstintegrierende Netze verschachteln regelmäßig ganze Protokollstapel: Beim Abruf oder Versand einer E-Mail über einen Web-Browser werden bspw. Verkehrs- und Metadaten der E-Mail in den Nutzdaten des HTTP-Protokolls übertragen, welches bei typischer Internet-Kommunikation (Abruf von Hypertext-Dokumenten) die höchste Schicht (Anwendungsschicht) realisiert. Gleiches gilt bei der Kommunikation vieler verbreiteter mobiler Anwendungen (Apps), welche das auf der Anwendungsschicht (Schicht 7) verortete HTTP-Protokoll ähnlich wie eine Transportschicht (Schicht 4) verwenden. Noch komplizierter ist die Situation bei Anwendungen, die eine eigene Adressierung realisieren bspw. bei Peer-to-Peer-Netzen oder der Verwendung von Anonymisierungsdiensten. **Es bleibt festzuhalten, dass aus technischer Sicht eine scharfe Abgrenzung zwischen Metadaten und Inhaltsdaten, die sich auf alle Arten elektronischer Kommunikation verallgemeinern ließe, nicht möglich ist.**

2. Technische Begriffsbestimmung

Der Begriff Metadaten ist Technikern viel gebräuchlicher als die Begriffe Verkehrs- und Nutzungsdaten. Mehr als 300 der untersuchten RFCs verwenden an mindestens einer Stelle die Begriffe „metadata" oder „meta data".

a. Metadaten im Zusammenhang mit elektronischer Datenverarbeitung

Im technischen Kontext wird der Begriff der Metadaten prinzipiell **unabhängig von Kommunikation** verwendet. Ganz allgemein sind Metadaten „Daten über Daten".[21] RFC 5388 (2008) definiert Metadaten beispielsweise als Konfiguration des (in diesem Fall speziellen) Datenerfassungsprogramms. Diese Praxis steht im Gegensatz zum Begriff der Verkehrsdaten, welcher ausschließlich im Zusammenhang mit Kommunikation auftritt.

Metadaten entstehen zum Beispiel in Dateisystemen und haben sowohl inhaltsbeschreibenden als auch inhaltsergänzenden Charakter.[22] So sind Datum und Uhrzeit der Erstellung sowie die Nutzerkennung des Bearbeiters typische Metadaten, die für jede einzelne Datei festgehalten werden.

---

[21] Z.B. RFC 4403 (2006), deutlicher in RFC 4949 (2007): „Descriptive information about a data object; i.e., data about data, or data labels that describe other data" (S. 190).
[22] RFC 1813 (1995), RFC 3010 (2000), RFC 3530 (2003).

Im Zusammenhang mit elektronischen Medien wird der Begriff Metadaten auch für bibliographische Angaben verwendet.[23] RFC 2431 (1998) differenziert in diesem Zusammenhang inhaltsbeschreibende Metadaten (z.B. Titel, Betreff, Quelle, etc.) von Metadaten, die das Urheberrecht betreffen (z.B. Autor, Rechteinhaber, etc.) sowie von Metadaten zur Instanz eines Werkes (z.B. Erstellungsdatum, Format, Kennung, Sprache, etc.). RFC 5257 (2008) und RFC 5464 (2008) sehen explizit vor, dass Benutzer selbst Metadaten an in E-Mail-Postfächern gespeicherte Nachrichten hinzufügen können, um die Verwaltung der Nachrichten zu unterstützen. Metadaten im Kontext der Langzeitarchivierung werden bspw. in RFC 4810 (2007) exemplarisch definiert.

Metadaten werden nicht nur im Dateisystem sondern bei vielen Dateiformaten auch direkt in der Datei gespeichert. Drei Beispiele dafür zur Veranschaulichung:

- Das verbreitete Word-Dokumentformat speichert unter anderem die Zeitpunkte der letzten Änderung, des letzten Ausdrucks und den Namen sowie Initialen der Person, die das Dokument ursprünglich erzeugt hat.

- Im von Digitalkameras und Smartphones verwendeten JPEG-Format für Digitalfotos werden regelmäßig Informationen über Kameramodell, Benutzereinstellungen, Belichtung und, falls verfügbar, die GPS-Koordinaten der Kamera zum Aufnahmezeitpunkt als Metadaten hinzugefügt.

- Videodateien enthalten Metadaten über die Kodierung und zur Synchronisation von Bild und Ton, welche laut RFC 4539 (2006) „strukturelle Metadaten" sind. Diese sind zur korrekten Darstellung bzw. Wiedergabe erforderlich. Davon zu unterscheiden sind deskriptive Metadaten (z.B. Titel, Schauspieler, Interpreten, Szenenbeschreibungen), die Inhalte beschreiben oder ergänzen.

Werden solche Dateien über Kommunikationsnetze übertragen, ist es Aufgabe der Anwendung (hier: Übertragungssoftware), auch die Metadaten zu übertragen und ggf. im Dateisystem des Zielrechners konsistent anzupassen. Aus Sicht der (unteren) Schichten des Kommunikationssystems erscheinen die übertragenen Metadaten wie Kommunikationsinhalte und sind nicht immer von diesen unterscheidbar. Im Umkehrschluss bedeutet dies, dass eine Maßnahme, die Metadaten aus beobachteten Datenverbindungen auswerten soll, auch Kommunikationsinhalte in die Auswertung einbeziehen muss.

b. Metadaten, die ausschließlich bei elektronischer Kommunikation entstehen

Grundsätzlich entstehen bei der Dateiübertragung weitere **Metadaten der Kommunikation**, die man auch als Verkehrsdaten bezeichnen kann. Damit wird bereits deutlich, dass Metadaten eine Übermenge der Verkehrs- und Nutzungsdaten darstellen und mit diesen Kategorien nur dann zusammenfallen, wenn sie durch genauere Bestimmung eingeschränkt sind. Ausgewählte Metadaten einer bestimmten Dienstnutzung sind entsprechend mit deren Nutzungsdaten assoziierbar. Ausgewählte Metadaten eines bestimmten Kommunikationsaktes sind etwa mit dessen Verkehrsdaten deckungsgleich. Dies wird auch in RFC 7687 (2015) deutlich, welche definiert:

> „It is useful to distinguish different kinds of metadata: explicit (or metadata proper) and implicit (sometimes called traffic data). Implicit metadata is things that can be derived from a message or are necessary for its delivery, such as the destination address, the size, the time,

[23] Bspw. in RFC 2220 (1997), RFC 5141 (2008)

or the frequency with which messages pass. Explicit metadata is things like quality ratings, provenance, or copyright data: data about the data, useful for an application, but not required to deliver the data to its endpoint." (S. 12 f.)

Umgekehrt ist den Sachverständigen kein Verkehrs- oder Nutzungsdatum bekannt, welches sich nicht als Metadatum bezeichnen ließe.

3. Juristische Begriffsbestimmung: Metadaten de lege lata

Der Begriff der Metadaten ist bislang kein juristisch anerkannter Begriff. Für ihn existiert im Gegensatz zu den Verkehrs- und Nutzungsdaten keine allgemeingültige Definition.[24] Es handelt sich allerdings um einen im Recht bzw. im Umgang mit dem Recht häufig genutzten Begriff. Aus der Art der Verwendung lässt sich ein bestimmter Bedeutungsgehalt ableiten.

a. Verwendung des Begriffes Metadaten in nationalen Gesetzen

Auf Ebene individueller deutscher Gesetze findet sich der Begriff der Metadaten an verschiedenen Stellen. Als einziges geltendes Gesetz definiert § 3 Abs. 2 Geodatenzugangsgesetz (GeoZG) für seinen Anwendungsbereich Metadaten. Danach handelt es sich um Informationen, die Geodaten oder Geodatendienste beschreiben und es ermöglichen, Geodaten und Geodatendienste zu ermitteln, in Verzeichnisse aufzunehmen und zu nutzen.

§ 12 Abs. 1 S. 3 E-Governmentgesetz nutzt ebenfalls den Begriff der Metadaten. Danach sollen die durch die Behörden zur Verfügung gestellten Daten „mit Metadaten versehen werden". Das damit im Zusammenhang stehende Informationsweiterverwendungsgesetz (IWG) greift ebenfalls auf den Begriff zurück (vgl. §§ 3, 8 IWG). Beide Gesetze verzichten auf eine Definition. In den Gesetzesbegründungen finden sich jedoch Hinweise, dass mit Hilfe der Metadaten das Auffinden des eigentlichen Datensatzes erleichtert werden soll.[25] Metadaten werden als Beschreibungen des eigentlichen Datensatzes verstanden.[26]

b. Verwendung des Begriffes Metadaten in Gesetzentwürfen

Auch in aktuell diskutierten nationalen Gesetzesvorhaben erscheint der Begriff der Metadaten. Im Entwurf des Gesetzes zur Einführung der elektronischen Akte in Strafsachen und zur weiteren Förderung des elektronischen Rechtsverkehrs ist durch § 32 StPO-E die Rechtsgrundlage für die Einführung der elektronischen Akte gelegt. Im Rahmen der Gesetzesbegründung zur vorgesehenen Verordnungsermächtigung in § 32 Abs. 3 StPO-E wird auf den Inhalt der durch die Verordnung festzulegenden Standards eingegangen. Diese Standards sollen auch die erforderlichen Metadaten einbeziehen. Metadaten werden in diesem speziellen Kontext unter Bezugnahme auf DIN ISO 15489-1:2002-12, 3.12 als Daten, die andere Daten beschreiben, definiert. [27]

c. Verwendung des Begriffes Metadaten in ergänzenden Dokumenten

Auch in sonstigen Veröffentlichungen im Rahmen von Gesetzgebungsprozessen, in denen auf das Wort Metadaten zurückgegriffen wird, ist dieser Sinngehalt erkennbar. Für das Satellitendatensicherheitsgesetz geht der Gesetzgeber beispielsweise davon aus, dass die Sensitivitätsprüfung eines einzelnen Datensatzes sich anhand der Metadaten durchführen lässt, da

---

[24] *Krüger/Möllers*, MMR 2016, 728, 728.
[25] BT-Drs. 17/11473, S. 44.
[26] BT-Drs. 18/4614, S. 20.
[27] Vgl. BT-Drs. 18/9416, S. 44.

diese eine abstrakte Beschreibung des konkreten Datensatzes enthalten.[28] Im Bundesstatistikgesetz werden Metadaten als beschreibende Informationen über die Datenbestände bei Verwaltungsdaten vorgestellt.[29]

d. Erwähnung in der juristischen Literatur allgemein

In der rechtswissenschaftlichen Literatur hat sich das Verständnis von Metadaten als „beschreibenden Informationen" soweit ersichtlich ebenfalls durchgesetzt. Dort fehlt es zwar ebenso wie auf Ebene der einzelnen Gesetze regelmäßig an einer näheren Auseinandersetzung mit dem tatsächlichen Inhalt des Begriffes. An dessen Verwendung zeigt sich aber, dass die ihm zugewiesene Bedeutung in dieselbe Richtung geht. So werden beispielsweise die Informationen, die die näheren Umstände der Telekommunikation beschreiben, als Metadaten zusammengefasst.[30]

e. Metadaten im Bereich elektronischer Kommunikation

Speziell im Zusammenhang mit der Datenverarbeitung in elektronischen Kommunikationsnetzwerken erfolgt die Nutzung des Begriffes Metadaten jedoch mit einem (leicht) verschobenen inhaltlichen Akzent.

Statt die beschreibende Funktion der Daten zu betonen, hat sich der **Begriff Metadatum als Gegenpol zu den sog. Inhaltsdaten entwickelt.**[31] Durch die Gegenüberstellung dieser Datenkategorien erfolgt eine negative Definition, die die Auseinandersetzung mit konkreten Fällen und deren juristische Handhabung vereinfacht. Gerade im Zusammenhang mit der Aufarbeitung der Massenüberwachung durch verschiedene Geheimdienste wird im internationalen Kontext auf die Unterscheidung zwischen Metadaten und Inhaltsdaten abgestellt.[32] Auch auf supranationaler/völkerrechtlicher Ebene ist die Grenzziehung zwischen Inhaltsdaten auf der einen und sonstigen (Meta-)Daten auf der anderen Seite gebräuchlich.[33]

Ob die fraglichen Daten beschreibender Natur sind, ist damit in den Hintergrund gerückt. Charakteristisch für die Einordnung als Metadaten ist vielmehr, dass sie nicht den Inhalt der elektronischen Kommunikation wiedergeben. Während sich im eigentlichen Sinne des Begriffs Metadaten eine enge Beziehung zwischen beschreibenden und beschriebenen Daten aufdrängt, wird bei Metadaten der elektronischen Kommunikation im Gegensatz dazu eine strikte Grenze betont.[34] Zu ihnen gehören alle Daten, die nicht Inhalt der elektronischen Kommunikation sind. Es handelt sich

---

[28] Vgl. BT-Drs. 16/4763, S. 27.
[29] BT-Drs. 18/7561, S. 24.
[30] *Dix/Schaar*, in: Roßnagel, § 15 TMG, Rn. 7; *Graulich*, S. 243; *Wenzel*, NZWiSt 2016, 85, 89.
[31] Vgl. für die Gegenüberstellung z.B.: *Dix/Kipker/Schaar*, ZD 2015, 300, 302; *Schellenberg*, ZRP 2014, 24, 25.
[32] Vgl. *US Court of Appeal for the 2nd Circuit in New York*, Urt. v. 7.5.2015 – 14-42, S. 7f., abrufbar unter: http://pdfserver.amlaw.com/nlj/NSA_ca2_20150507.pdf; *Investigatory Powers Tribunal (IPT)*, No. IPT/15/110/CH, Urt. V. 17.10.2016, Rn. 4, 26, abrufbar unter: http://www.ipt-uk.com/docs/Bulk_Data_Judgment.pdf; *Federal Court of Canada*, Urt. v. 4.10.2016, 2016 FC 1105, Rn. 84, abrufbar unter: http://cas-cdc-www02.cas-satj.gc.ca/rss/DES%20%28warrant%29%20nov-3-2016%20public%20judgment%20FINAL%20%28ENG%29.pdf.
[33] Vgl. *Menschenrechtsrat der Vereinten Nationen*, Bericht des Hohen Kommissars der Vereinten Nationen für Menschenrechte über das Recht auf Privatsphäre im digitalen Zeitalter, 30. Juni 2014, A/HRC/27/37, Rn. 19, abrufbar unter: http://www.un.org/depts/german/menschenrechte/a-hrc-27-37.pdf; *Council of Europe*, Committee on Legal Affairs and Human Rights, Report on Mass Surveillance, S. 6, abrufbar unter: http://website-pace.net/documents/19838/1085720/20150126-MassSurveillance-EN.pdf/df5aae25-6cfe-450a-92a6-e903af10b7a2.
[34] Vgl. *Administration White Paper*, Bulk Collection of Telephony Metadata Under Section 215 of the USA Patriot Act 15, S. 2; abrufbar unter: http://big.assets.huffingtonpost.com/Section215.pdf.

damit um Daten, die technischer Natur sind und für die Durchführung des Kommunikationsprozesses erforderlich sind. Dabei ist es unerheblich, wie genau der Entstehungsprozess dieser Daten aussieht. Ob sie nun deshalb anfallen, weil eine Person einen Kommunikationsprozess initiiert hat, oder ob sie unabhängig von menschlichem Handeln im Rahmen eines autonomen Kommunikationsvorgangs zwischen einzelnen Maschinen entstehen (dazu ausführlich Frage C), ändert nichts an ihrer Zuordnung zu den Metadaten.

Die negative Bedeutungszuweisung kann jedoch nicht verschleiern, dass es sich auch bei diesen technisch bedingten Daten immer noch um beschreibende Daten handelt. Zwar stellen Metadaten elektronischer Kommunikation den Inhalt nicht direkt dar; sie beschreiben aber dafür die Umstände der Kommunikation.[35] Beispiele dafür sind die Funkzelle, Zeit, Ort, Datum einer ein- und ausgehenden Verbindung oder die zugewiesene Nutzerkennung der Kommunikationspartner. Je mehr allerdings über die Umstände bekannt ist, desto leichter lassen sich Rückschlüsse auf den Inhalt ziehen. Hinzu kommt, dass die genannten Beispiele in aller Regel als strukturierte Daten vorliegen und sich deshalb besonders gut für eine automatische Auswertung eignen. Im Gegensatz zu oftmals unstrukturiert vorliegenden Inhaltsdaten (z.B. natürlich sprachlicher Text, digitalisierte Töne und Bilder) ist die Auswertung strukturierter Daten weniger rechenaufwändig und die getroffenen Schlussfolgerungen sind zuverlässiger.[36]

4. Zwischenfazit

Im technischen Kontext wird der Begriff der Metadaten generell häufig und auch ohne direkten Bezug zur elektronischen Kommunikation verwendet. Metadaten beschreiben oder ergänzen andere Daten. Kommt es zur Datenübertragung, werden Metadaten und in Bezug stehende Daten gleicherweise als Kommunikationsinhalte übermittelt. Darüber hinaus entstehen bei der Datenübertragung weitere Metadaten der Kommunikation. Sie können für die Übertragung notwendig sein oder werden aufgrund von Konventionen ohne zwingende Notwendigkeit erhoben und übermittelt. Die Architektur von Kommunikationssystemen nach dem Prinzip der Schichtmodelle erschwert eine scharfe Trennung von Metadaten und den Daten, mit denen sie im Zusammenhang stehen. Es bietet sich die Vorstellung von Metadaten auf einer Vielzahl von hierarchisch angeordneten Ebenen an. Deren Abgrenzung und Granularität ist subjektiv.

Im juristischen Kontext ermöglicht der Blick auf die einzelnen geltenden bzw. geplanten Gesetze bzw. Gesetzesbegründungen eine inhaltliche Ableitung des Begriffes, die sich als „kleinster gemeinsamer Nenner" festhalten lässt. Metadaten können grundsätzlich so verstanden werden, dass sie andere Daten beschreiben.[37] Sie können technische und ggf. inhaltliche Aussagen und Informationen über andere Daten enthalten. In welche Richtung diese Beschreibungen gehen, ist abhängig vom jeweiligen Kontext. Je nachdem, was in welchem Umfang beschrieben wird, können allein aus der Beschreibung wertvolle Informationen gewonnen werden. Der Begriff wird überall dort verwendet, wo zwischen verschiedenen Datenebenen unterschieden werden kann.[38]

Speziell im Zusammenhang mit der Datenverarbeitung in elektronischen Kommunikationsprozessen hat sich jedoch eine negative Bedeutungszuweisung etabliert. Dort werden Metadaten verstanden als alle in Verbindung mit dem Kommunikationsprozess stehenden Daten, die nicht der inhaltlichen

---

[35] *Dix/Schaar*, in: Roßnagel, § 15 TMG, Rn. 7; *Graulich*, S. 243; *Wenzel*, NZWiSt 2016, 85, 89.
[36] Vgl. *Waidner*, S. 16.
[37] So auch *Krüger/Möllers*, MMR 2016, 728, 728.
[38] Beispielsweise auch im Rahmen der Indexierung von digitalen Inhalten: *Schulz*, GRUR 2006, 470, 472; *Roßnagel/Wilke*, NJW 2006, 2145, 2145.

Ebene der Kommunikation zuzuordnen sind. Es handelt sich damit um die Daten, die technisch bedingt bei der Durchführung von Kommunikation, sei es durch Menschen oder durch Maschinen initiiert, anfallen. Die Betonung, dass die Daten nicht primär den Zweck haben, den Inhalt zu beschreiben, kann jedoch nicht darüber hinwegtäuschen, dass Metadaten trotzdem beschreibender Natur sind. Sie beschreiben jedenfalls die Umstände der Telekommunikation. Da sich daraus oft Rückschlüsse auf den Inhalt ergeben, sind sie gerade interessant für private Unternehmen ebenso wie für staatliche Behörden.

5. Juristische Begriffsbestimmung: Metadaten de lege ferenda

Durch gesetzgeberisches Tätigwerden auf EU-Ebene könnte der Begriff der Metadaten in naher Zukunft zumindest für den Bereich der elektronischen Kommunikation juristisch verfestigt werden. Ob sich dadurch Änderungen mit Blick auf die geltende Rechtslage ergeben, soll im Folgenden überprüft werden.

a. Definition im Vorschlag zur ePrivacy-Verordnung

Der „Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG"[39] (im Folgenden: ePrivacy-Verordnung) enthält eine Definition für „elektronische Kommunikationsmetadaten" in seinem Artikel 4 Abs. 3 lit. c:

> „Daten, die in einem elektronischen Kommunikationsnetz zu Zwecken der Übermittlung, der Verbreitung oder des Austauschs elektronischer Kommunikationsinhalte verarbeitet werden; dazu zählen die zur Verfolgung und Identifizierung des Ausgangs- und Zielpunkts einer Kommunikation verwendeten Daten, die im Zusammenhang mit der Bereitstellung elektronischer Kommunikationsdienste erzeugten Daten über den Standort des Geräts sowie Datum, Uhrzeit, Dauer und Art der Kommunikation"

Die Einordnung als Metadaten erfolgt demnach anhand einer technischen Zweckbestimmung. Sämtliche Daten, die zum Zweck der Übermittlung, Verbreitung oder des Austauschs elektronischer Kommunikationsinhalte in elektronischen Kommunikationsnetzwerken verarbeitet werden, sind von der Definition erfasst.

b. Übereinstimmung mit dem geltenden erarbeiteten Begriffsverständnis

Dieser Vorschlag stimmt im Ergebnis überein mit dem eben dargestellten, lediglich abgeleiteten Bedeutungsgehalt von Metadaten im Bereich elektronischer Kommunikation. Auch in ihm besitzt das beschreibende Element auf den ersten Blick keine entscheidende Funktion mehr. Stattdessen erfolgt die Zuordnung danach, dass die Daten anfallen, um elektronische Kommunikationsinhalte zu übermitteln, verbreiten oder auszutauschen. Ihre technische Bedeutung für die Vornahme von elektronischer Kommunikation ist also entscheidend.

Diese Art der Zuordnung setzt implizit die eben herausgearbeitete strikte Gegenüberstellung zu Inhaltsdaten voraus. Metadaten sind der Definition nach die Daten, die beim Vorgang der elektronischen Kommunikation verarbeitet werden. Zur Kommunikation auf inhaltlicher Ebene kommt es also durch die Verarbeitung von vom Inhalt losgelösten Daten. Letztere sind als Metadaten von den Inhaltsdaten zu unterscheiden.

---

[39] *Europäische Kommission*, COM(2017) 10 final, abrufbar unter: http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:52017PC0010.

Dass diese Gegenüberstellung der eigentliche Kernaspekt für die Bedeutungszuweisung von Metadaten nach der ePrivacy-Verordnung sein soll, wird zusätzlich beim Blick auf die übrigen neu einzuführenden Definitionen deutlich. Art. 4 Abs. 3 lit. a etabliert die Kategorie der „elektronischen Kommunikationsdaten". Diese setzen sich nicht nur aus den eben genannten Metadaten zusammen, die wie gezeigt in Art. 4 Abs. 3 lit. c definiert sind. Zusätzlich gehören dazu die „elektronischen Kommunikationsinhalte", die in Art. 4 Abs. 3 lit. b beschrieben werden.

Der Gegensatz zwischen diesen beiden Datenkategorien spiegelt sich auch in den getrennten Vorgaben bezüglich des rechtlichen Umgangs mit ihnen. Zwar ist in Art. 6 Abs. 1 eine einheitliche Grundregel bzgl. des erlaubten Umgangs mit der Gesamtheit der „elektronischen Kommunikationsdaten" enthalten. In den folgenden Absätzen sowie im folgenden Artikel bzgl. der Speicherung und Löschung spalten sich die Normen jedoch auf. Metadaten und Inhaltsdaten sind dementsprechend rechtlich differenziert zu behandeln.

Auch wenn damit im Kern eine negative Definition (Metadaten sind Daten elektronischer Kommunikation, die nicht Inhaltsdaten sind) gesetzlich verankert wird, die ihre begriffliche Zuweisung über eine Abgrenzung zu einem Gegenbegriff erhält, ändert sich nichts daran, dass diese Definition das Grundelement für Metadaten im ursprünglichen Wortsinne enthält. Es handelt sich immer noch um Daten, die ein beschreibendes Element aufweisen. Beschrieben wird zwar nicht unbedingt der Inhalt der Kommunikation, jedenfalls aber die näheren Umstände. Dass daraus spezifische Gefahren für die Privatsphäre der Kommunikationsteilnehmer resultieren, wird im Rahmen der Verordnung explizit betont. So könnten Rückschlüsse auf soziale Beziehungen, Aktivitäten und Gewohnheiten des täglichen Lebens sowie der allgemeinen Interessen und Vorlieben der Personen gezogen werden.[40]

c. Definitorische Parallele zu Verkehrs- und Nutzungsdaten

Die stärkere Anknüpfung an den Zweck bei der Zuordnung zur Begriffskategorie Metadaten sorgt im Übrigen für eine Parallele zu den Begriffen der Verkehrs- bzw. Nutzungsdaten, die für den Bereich der elektronischen Kommunikation in Deutschland etabliert sind. Bei beiden Kategorien handelt es sich ebenfalls um Daten, die zum Erreichen eines bestimmten Zweckes anfallen, nämlich dem Zweck der Erbringung eines TK-Dienstes oder dem Angebot eines Telemediendienstes.

6. Verhältnis Metadaten zu Verkehrs- und Nutzungsdaten

Mit dem Wissen um diese begrifflichen Hintergründe lässt sich die Ausgangsfrage beantworten. Metadaten der Telekommunikation und Verkehrs- bzw. Nutzungsdaten weisen nicht nur durch ihren zweckgerichteten Ansatz Parallelen in der Art der Definition auf, sondern sind auch inhaltlich verwandt. Im Gegensatz zu den auf spezielle Akteure und ihre Tätigkeiten zugeschnittenen Verkehrs- und Nutzungsdaten sind Metadaten allerdings in persönlich-sachlicher Hinsicht umfassender. Sie sind deshalb als Oberbegriff der Verkehrs- und Nutzungsdaten einzustufen, der die bisherige Teilung in Verkehrs- und Nutzungsdaten überwindet und weitere Daten einschließt, die weder den Verkehrs- noch Nutzungsdaten zuzuordnen sind.

Verkehrs- und Nutzungsdaten sind also spezielle Kategorien der Metadaten. Dabei kann ein- und dasselbe Metadatum sowohl Verkehrs- als auch Nutzungsdatum sein, wie z.B. eine IP-Adresse. Die mögliche Erfassung unter verschiedenen Begriffen ist lediglich Ausdruck einer rechtlichen Bewertung aus einem bestimmten Blickwinkel. Bei Verkehrsdaten ist es eine Perspektive, die sich speziell auf TK-

[40] Vgl. Vorschlag einer ePrivacy-Verordnung, COM(2017) 10 final, EwG 2.

Unternehmen und ihre Dienste richtet. Im Zusammenhang mit Nutzungsdaten stehen Telemediendiensteanbieter und ihre Tätigkeiten im Fokus der rechtlichen Bewertung.

Aus der Einstufung als Unterkategorie folgt, dass jedes Verkehrs- oder Nutzungsdatum zugleich ein Metadatum ist. Das Vorliegen der jeweiligen speziellen, gesetzlich festgelegten Merkmale sorgt letztlich dafür, die Begriffe voneinander zu unterscheiden und ihren rechtlichen Kontext entsprechend behandeln zu können. Handelt es sich um ein personenbezogenes Datum, das einem Nutzer die Nachfrage nach Telemediendiensten ermöglicht, handelt es sich bei diesem Metadatum um ein Nutzungsdatum. Handelt es sich hingegen um Daten, die bei der Erbringung eines TK-Dienstes erhoben, verarbeitet oder genutzt werden, sind diese Metadaten Verkehrsdaten. Gemeinsam ist ihnen, dass sie erhoben und verarbeitet werden, um elektronische Kommunikationsinhalte zu übertragen, verbreiten oder auszutauschen. Umgekehrt ist der Schluss allerdings nicht zwingend. Nicht jedes Metadatum lässt sich als Verkehrs- oder Nutzungsdatum einordnen.

Ein Beispiel für ein Metadatum das weder Verkehrs- noch Nutzungsdatum ist, ist die GPS-Koordinate des Aufnahmeorts eines von einem Smartphone übertragenen Digitalfotos. Diese Standortinformation kann sich vom Standort des mobilen Endgeräts zum Zeitpunkt der Übertragung unterscheiden, bspw. wenn ein Foto mit zeitlichem Abstand übertragen wird. Nur der Standort des mobilen Endgeräts zum Übertragungszeitpunkt wäre als Verkehrsdatum einzuordnen.

Folgt man der Tendenz des Vorschlages der neuen ePrivacy-Verordnung, so wird es zukünftig eher auf die Einordnung als Metadatum als auf die exakte Zugehörigkeit eines Datums zu Verkehrs- oder Nutzungsdaten ankommen. Hinzugefügt werden kann, dass der Begriff der Nutzungsdaten ein rein deutscher Begriff ist, der auf internationaler Ebene und auch im technischen Zusammenhang nicht verwendet wird (dazu bereits Punkt B. Teil IV).

Die Unterscheidung in Meta- und Inhaltsdaten ist daher grundsätzlich geeignet, um technisch sowie juristisch einem Datum eine grobe Bedeutung zuzumessen und gleichzeitig eine Vielzahl von Datenarten unterschiedlicher Dienste zu umfassen.

C. Wobei fallen die o.g. Daten an? Handelt es sich immer um Telekommunikationsereignisse von Personen oder ist auch eine maschinenbasierte Telekommunikation hiervon erfasst? Wie wäre das Gesamtaufkommen von TK-Daten diesen Klassen anteilig zuzuordnen?

Bei der Durchführung elektronischer Telekommunikation fallen zwangsläufig Metadaten an. Wie soeben ausgeführt (vgl. Frage B), handelt es sich bei Metadaten sowohl aus technischem als auch aus juristischem Blickwinkel um einen Oberbegriff. Rechtswissenschaftlich betrachtet sind insbesondere die Unterkategorien der Verkehrs- und Nutzungsdaten von Bedeutung. Aus technischer Sicht sind die Begriffe Verkehrs- und Nutzungsdaten dagegen kaum von Relevanz.

Da die hier zu beantwortenden Fragen auf technische Grundlagen abzielen, werden sie unter Bezugnahme auf den Begriff Metadaten beantwortet. Dieses Vorgehen empfiehlt sich auch aus juristischer Sicht, da sich so die komplizierte Zuordnung zu einer der beiden zuvor vorgestellten Unterkategorien erübrigt. Denn wie im ersten Teil (siehe Frage B, Teil VI, Abschn. 6) gezeigt, kann ein

Metadatum zwar als Verkehrs- oder Nutzungsdatum kategorisiert werden. Die Zuordnung ist jedoch nicht zwingend eindeutig und setzt stets eine Berücksichtigung aller Umstände des Einzelfalles voraus. Sie ist also auf dem abstrakten Level dieser Fragen nicht durchführbar.

Metadaten fallen an verschiedenen Stellen der elektronischen Kommunikation an. Grob kann man unterscheiden:

1. Metadaten bei der Erstellung der Kommunikationsinhalte (Bsp. GPS-Koordinate in Digitalfoto). Diese Daten fallen zunächst im Endgerät an und werden ggf. später übermittelt.

2. Metadaten durch Bereitstellung und Bereithaltung von Kommunikationsmöglichkeiten (Bsp. Zellinformation und Endgerätekennung bei Mobilfunk; Nutzungsdaten von Plattformen, bei denen sich Endgeräte automatisch einloggen und Präsenzinformation hinterlegen). Diese Daten fallen beim Dienstanbieter und im Endgerät an. Ausgewählte Informationen werden mitunter an Dritte weitergegeben (Bsp. Präsenzinformation an andere Teilnehmer, Abrechnungs- und Leitwegedaten bei Roaming).

3. Metadaten bei menschlich veranlassten Kommunikationsvorgängen (Bsp. Empfängerkennung beim Versand eine E-Mail). Daten dieser Art fallen bei den Endgeräten und den an der Vermittlung und Übertragung beteiligten Zwischenstationen an.

4. Metadaten bei automatisch veranlassten Datenübertragungen (Bsp. regelmäßige Synchronisation von örtlich verteilten Datenbanken zur Erhöhung der Ausfallsicherheit und Verbesserung der Zugriffsgeschwindigkeit; hierzu gehört auch die automatische, in der Regel vom Anbieter vorprogrammierte Aktualisierung von Inhalten, die dem Nutzer präsentiert werden unabhängig davon, ob er diese wahrnimmt, bspw. Online-Werbung). Daten dieser Art fallen beim den Kommunikationspartnern und den an der Vermittlung und Übertragung beteiligten Zwischenstationen an.

5. Metadaten, die im Kontext von Kommunikationsvorgängen automatisch zwischen Sender und Empfänger vereinbart werden bspw. um das Übertragungsformat festzulegen.[41] Hierbei ist es unerheblich, wer die Kommunikation veranlasst. Diese Daten fallen bei allen an der Kommunikation beteiligten Endgeräten an und sind in der Regel für Zwischenstationen sichtbar.

Aus dieser Darstellung wird zugleich deutlich, dass es nicht darauf ankommt, ob es sich um Telekommunikationsereignisse von Personen oder aber um maschinenbasierte Telekommunikation handelt. Maschinenbasierte Telekommunikation zeichnet sich dadurch aus, dass die im Rahmen der Kommunikation anfallenden Daten nicht direkt durch menschliches Verhalten, sondern durch Computerprozesse, Anwendungen, Dienste oder Sensoren erzeugt werden.[42] Diese Umschreibung deckt sich mit dem Schlagwort „Maschine-Maschine-Kommunikation", das eine Übertragung von Daten ohne im konkreten Einzelfall willentliches Zutun

[41] RFC 2703 (1999) „Information which is exchanged between the sender and receiver of a message by content negotiation in order to determine the variant which should be transferred".

[42] Vgl. insofern die Definition der "machine-generated data" in der *Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschluss der Regionen*, Aufbau einer europäischen Datenwirtschaft, COM 2017, 9 final, S. 9: "machine-generated data is created without the direct intervention of a human by computer processes, applications or services, or by sensors processing information received from equipment, software or machinery, whether virtual or real."

des Nutzers bezeichnet.[43] Demgegenüber sind Telekommunikationsereignisse von Personen zwangsläufig solche, in denen ein Mensch eine Übertragung von Daten initiiert. Metadaten fallen in beiden Konstellationen und damit unabhängig vom Entstehungsprozess an.

Eine anteilige Zuordnung der anfallenden Daten nach wissenschaftlichen Standards setzt voraus, dass repräsentativer Datenverkehr klassifiziert und gemessen wird. Die Klassifikation von Datenverkehr ist Gegenstand aktueller wissenschaftlicher Forschung in der Informatik.[44] Den Sachverständigen ist allerdings keine Untersuchung bekannt, die Datenverbindung nach ihrer Verursachung durch menschliches Verhalten bzw. maschinelle Abläufe einteilt. Eine entsprechende Studie durchzuführen, wäre mit erheblichen Schwierigkeiten verbunden. Moderne Klassifikationsverfahren bedienen sich der Methode des maschinellen Lernens, welche in der Anlernphase „wahre" (engl. „ground truth") Informationen zu einer Vielzahl an Beispiel-Datenflüssen benötigt. Diese zu erstellen bzw. zu sammeln, ist nicht trivial und wirft ethische sowie datenschutzrechtliche Fragen auf. Generell deuten Studien zur Datenverkehrsklassifikation in Teilnetzen des Internets darauf hin, dass die Ergebnisse weder im Zeitverlauf noch bezogen auf die Zusammensetzung der Datenströme stabil sind. Beides ist Ausdruck der erheblichen Dynamik bei der Verwendung von Internet-Protokollen und Protokollvarianten sowie der Heterogenität der Teilnetze.

Ohne empirische Daten sind lediglich grobe Schätzungen möglich. Aus heutiger Sicht gehen die Sachverständigen davon aus, dass der überwiegende Anteil der übertragenen Datenmenge zwischen Internet-Backbone und Endgeräten unmittelbar oder mittelbar mit menschlichem Verhalten in Zusammenhang steht. Diese Bezugsbasis schließt explizit Datenverkehr zur Synchronisation von Datenbeständen in weltweit verteilten Rechenzentren aus. Trotzdem ist der Anteil maschinell veranlasster Kommunikation nicht vernachlässigbar gering.

D. Welche Arten von Metadaten entstehen bei den verschiedenen Formen digitaler Telekommunikation und welche datenschutzrechtlichen Schlüsse lassen sich aus ihrer Analyse ziehen?

Grundsätzlich entstehen alle bereits besprochenen Arten von Metadaten bei digitaler Telekommunikation. Eine erschöpfende Aufzählung der Formen digitaler Kommunikation sowie der damit verbundenen kommunikationsbezogenen Metadaten ist unverhältnismäßig aufwändig und für die datenschutzrechtlichen Schlüsse unerheblich, da sich, wie im Rahmen von Frage E, Teil I genauer erläutert wird, die Personenbeziehbarkeit nicht pauschal an der Datenart oder Kommunikationsform feststellen lässt.

Als Beispiel hierfür sei das Metadatum einer dynamisch vergebenen TCP-Portnummer genannt, welches bei im Internet typischen TCP/IP-Verbindungen im Kopf des Segments und damit in den Metadaten der Transportschicht abgelegt ist (vgl. Frage B, Teil VI, Abschn. 1). Portnummern dienen zur Unterscheidung aller bestehenden TCP/IP-Verbindungen eines Endgeräts. Grundsätzlich werden Portnummern automatisch festgelegt und nach Verfügbarkeit vergeben. Die Vergaberegeln sind in der Regel in einem Teil des Betriebssystems programmiert. Trotzdem kann die

[43] *Graulich*, S. 242.
[44] *Dainotti/Pescapé/Claffy*, IEEE Network 2012, 35, 35ff.; *Richter/Chatzis/Smaragdakis/Feldmann/Willinger*, in: Mirkovic/Liu, S. 179ff.

Personenbeziehbarkeit aus mindestens zwei Gründen nicht pauschal verneint werden. Erstens lassen sich in der Zusammenschau der Vergabe von Portnummern Rückschlüsse auf das verwendete Betriebssystem und die Anzahl gleichzeitig laufender Verbindungen ziehen.[45] Dies kann unter bestimmten Umständen dazu führen, dass der Kommunikationspartner, etwa wenn er als Einziger ein ungewöhnliches Betriebssystem verwendet, mit Kenntnis der Portnummer identifizierbar ist. Zweitens können Kommunikationsereignisse über Portnummern verknüpft werden, die z.B. durch die in Heimnetzen übliche Network Address Translation (NAT) nicht allein aufgrund der IP-Adresse einzelnen Personen zugeordnet werden können. Dazu ist in der Regel die Zusammenschau von Informationen an mehreren Punkten im Netz erforderlich. Bei Geheimdiensten ist diese Fähigkeit nicht grundsätzlich auszuschließen. In beiden Fällen ist darüber hinaus möglich, dass mit Kenntnis der Portnummer im Ausschlussverfahren der Kreis der betroffenen Personen eingeschränkt werden kann, sodass mittelbar ein Personenbezug bei einem anderen Kommunikationsvorgang hergestellt werden kann. Dieses Beispiel veranschaulicht, dass unabhängig von der Form der digitalen Telekommunikation eine abschließende datenschutzrechtliche Bewertung einzelner Kommunikationsvorgänge oder einzelner Arten von Metadaten nicht möglich ist.

TCP-Portnummern sind nur ein Beispiel für übermittlungstechnische Metadaten bei TCP/IP, die Rückschlüsse auf die Endgeräte zulassen (sog. TCP-Fingerprinting). In der Literatur sind viele weitere Datenfelder dokumentiert.[46] Ähnliches gilt für die automatische Erzeugung von übermittlungstechnischen Metadaten auf anderen Schichten und bei anderen Formen der digitalen Telekommunikation, bspw. der Wahl von Übertragungsfrequenzen bei Funkstrecken. RFC 6562 (2012) verweist darüber hinaus auf zwei Beispiele dafür, wie strukturelle Metadaten im Sinne von RFC 4539 (2006) (vgl. dazu Frage B, Teil VI, Abschn. 2) Rückschlüsse auf den Inhalt selbst von verschlüsselter Sprachkommunikation erlauben, wenn diese per Voice-over-IP mit variabler Bitrate komprimiert wurde.

Da der Metadatenbegriff nicht zwischen Verkehrs-, Nutzungs- und teilweise Inhaltsdaten differenziert, sondern alle Datenarten einschließt, stellt der Umgang mit Metadaten potenziell eine größere Gefahr für die Privatsphäre der Kommunikationsteilnehmer dar als die Verarbeitung genau bestimmter Datenarten.

E. Welche ggf. feststehenden Indikatoren lassen eine Einordnung eines einzelnen (Meta)datums als „personenbezogen" zu und inwiefern sind, unabhängig von einzelnen Datensätzen, Personenbezüge in der Zusammenschau verschiedener, für sich betrachtet nicht personenbezogener Einzeldaten möglich?

I. Einordnung eines einzelnen (Meta)datums als personenbezogen

Mit der Qualifikation als Metadatum ist noch keine Aussage darüber getroffen, ob es sich um ein personenbezogenes Datum handelt. Metadaten der Kommunikation sind vielmehr eine heterogene

[45] Siehe https://www.cymru.com/jtk/misc/ephemeralports.html; auch RFC 6056 (2011).
[46] *Taleck*, in: Vigna/Jonsson/Kruegel, S. 192ff.

Gruppe von Daten, die lediglich die Gemeinsamkeit aufweisen, zum Zweck der Durchführung elektronischer Kommunikationsprozesse aus technischen Gründen anzufallen, ohne unbedingt den Inhalt der Kommunikation direkt wiederzugeben. Sie entstehen sowohl bei von Menschen initiierten Telekommunikationsprozessen als auch bei maschinenbasierter Telekommunikation.

Personenbezogene Daten sind gem. § 3 Abs. 1 BDSG Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener). Durch die Datenschutzgrundverordnung ändert sich der Wortlaut der Definition. Laut Art. 4 Nr. 1 DS-GVO sind personenbezogene Informationen alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Inhaltlich führt dies jedoch zu keiner Änderung. Das zentrale Begriffspaar „identifizierte oder identifizierbare" entspricht trotz des geänderten Wortlauts den traditionellen Begriffen „bestimmt oder bestimmbar".[47]

Sämtliche Metadaten, die Informationen über eine bestimmte oder bestimmbare natürliche Person enthalten, unterliegen also als personenbezogene Daten den datenschutzrechtlichen Restriktionen. Eine generelle Aussage, ob der Ursprung der Metadaten, also ihrer Entstehung aus einem menschlichen oder rein maschinellen Kommunikationsprozess, für einen Personenbezug spricht, lässt sich nicht tätigen. Es kommt stets darauf an, ob über das konkret betrachtete Datum der Betroffene bestimmbar ist. Eine Möglichkeit, die Bestimmbarkeit und damit die Personenbeziehbarkeit auszuschließen, ist die aktive Veränderung der Daten durch den Einsatz geeigneter Anonymisierungsverfahren.

Während die Grenze zwischen der Bestimmtheit und Bestimmbarkeit bzw. der der Identifikation und der Möglichkeit der Identifikation eher von theoretischem Interesse ist, ist die Grenze zwischen Bestimmbarkeit und Nichtbestimmbarkeit die praktisch relevante.[48] Auf die Möglichkeiten der Feststellung dieser Grenze zielt auch der erste Teil der Frage, indem sie nach feststehenden Indikatoren, also Hinweisen oder Anzeichen für die Einordung des Personenbezugs fragt.

1. Anzeichen für Identifizierbarkeit

Durch Art. 4 Nr. 1 Hs. 2 DS-GVO gibt ein Gesetz selbst Anhaltspunkte bezüglich der Ermittlung des vom Datenschutz erfassten Bereichs. Als identifizierbar wird demnach eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.

Indikatoren für die Identifizierbarkeit einer Person und damit den Personenbezug der Daten lassen sich aus dieser Auflistung entnehmen. Insbesondere der Name, aber auch Kennnummern oder Standortdaten indizieren die Möglichkeit der Identifikation individueller Personen. Der Name einer Person ist also nicht der einzig maßgebliche Indikator. Auch sonstige Zuordnungskriterien, mit denen „Singularität und Eindeutigkeit einer Person in den Kommunikations- und Interaktionsbeziehungen gewährleistet werden"[49], können diese Funktion einnehmen. Umgekehrt genügt jedoch allein das

[47] *Ernst*, in: Paal/Pauly, DS-GVO, Art. 4, Rn. 3; *Kühling/Klar*, ZD 2017, 24, 28; *Richter*, EuZW 2016, 909, 913; *Mantz/Spittka*, NJW 2016, 3579, 3583.
[48] *Dammann*, in: Simitis, § 3 BDSG, Rn. 23.
[49] *Karg*, ZD 2012, 255, 257.

Vorliegen dieser Indikatoren nicht für eine eindeutige Aussage über den Personenbezug.[50] **Ob für die Identifizierung ausreichende Informationen vorliegen, hängt vielmehr stets vom Kontext der jeweiligen Situation ab.**[51]

2. EuGH-Entscheidung im Fall Breyer: Identifizierung über Dritte

Verdeutlichen lässt sich dies an der kürzlich ergangenen Entscheidung des EuGH im Fall *Breyer*, in der es um die Einordnung einer dynamischen IP-Adresse ging. Da eine solche IP-Adresse eine einzigartige Kennung darstellt, die sich unstreitig nicht auf eine bestimmte natürliche Person bezieht[52], war die Klärung der Bestimmbarkeit der Person notwendig. In diesem Zusammenhang erfolgte zunächst die Klarstellung, dass es dafür nicht erforderlich ist, „dass die Information für sich genommen die Identifizierung einer betroffenen Person ermöglicht."[53] **Nur weil einem einzelnen Datum also nicht ohne Weiteres zu entnehmen ist, welche Person es betrifft, führt dies nicht zur Ablehnung des Personenbezugs dieses Datums.**

a. Mittel zur Identifizierung

Stattdessen sind dem EuGH zufolge „**alle Mittel zu berücksichtigen, die vernünftigerweise entweder vom für die Verarbeitung Verantwortlichen oder von einem Dritten eingesetzt werden könnten, um die betreffende Person zu bestimmen.**"[54] Es kommt für die Klärung der Bestimmbarkeit und somit des Personenbezugs stets zu einer Zusammenschau, die im zweiten Teil der hier bearbeiteten Frage angesprochen wird. Dieser Grundsatz, der sich auf die RL 95/46/EG stützt[55], verliert auch mit Geltung der DSGVO nicht an Bedeutung. So legt Erwägungsgrund 26 DSGVO fest:

„Die Grundsätze des Datenschutzes sollten für alle Informationen gelten, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. [...] 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 [...]."[56]

Dieser Maßstab bzgl. der Feststellung des Personenbezugs legt eine zweigeteilte Vorgehensweise nahe. In einem ersten Schritt ist zu klären, ob überhaupt jemand den Personenbezug herstellen kann. Ist es objektiv ausgeschlossen, dass der Betroffene bestimmt werden kann, fehlt es am Personenbezug.[57] Eine solche Situation, in der nicht einmal ein Dritter existiert, der den Personenbezug vornehmen kann, dürfte jedoch relativ selten sein. Gerade angesichts der vielfältigen Akteure im Rahmen der elektronischen Kommunikation und ihrer Mitwirkung am Kommunikationsprozess erscheint es unwahrscheinlich, dass es niemanden gibt, der den Personenbezug der Metadaten herstellen kann. Ganz im Gegenteil lässt die ständig steigende Vielfalt hochkomplexer Auswertungsmechanismen und deren einfache Verfügbarkeit faktisch die Anzahl derjenigen Stellen steigen, die in der Lage sind, zwischen gespeicherten Angaben und einer

---

[50] *Dammann*, in: Simitis, § 3 BDSG, Rn. 21.
[51] Vgl. *Art.-29-Datenschutzgruppe*, WP 136, S. 15, abrufbar unter: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_de.pdf.
[52] *EuGH*, Urt. v. 19.10.2016 – C-582/14, Rn. 38.
[53] *EuGH*, Urt. v. 19.10.2016 – C-582/14, Rn. 41.
[54] *EuGH*, Urt. v. 19.10.2016 – C-582/14, Rn. 42.
[55] Vgl. Datenschutz-RL 95/46/EG, EwG 26.
[56] VO 2016/679/EU, EwG 26.
[57] *Dammann*, in: Simitis, § 3 BDSG, Rn. 23.

natürlichen Person einen Bezug herzustellen.[58] In diesem Zusammenhang ist es gleichermaßen von Bedeutung, dass die Quantität der Daten ansteigt und die Nachfrage danach ebenso zunimmt. So erhält beispielsweise Google pro Jahr über 25.000 Anfragen von Ermittlungsbehörden, in denen das Unternehmen zur Herausgabe von Daten ihrer Nutzer aufgefordert wird.[59]

Umgekehrt ist allerdings darauf hinzuweisen, dass allein die Möglichkeit, dass ein Dritter mit seinem Zusatzwissen den Personenbezug herstellen kann, nicht ausreicht, um von einem personenbezogenen Datum auszugehen. Dies hat der EuGH im *Breyer*-Urteil klargestellt und damit die Streitfrage, ob der Personenbezug absolut oder relativ zu bestimmen ist,[60] zugunsten der relativen Theorie entschieden.[61] Denn obwohl es mit dem Internetzugangsanbieter einen Dritten gab, der die Zuordnung mit verhältnismäßig einfachen Mitteln vornehmen konnte, stellten die Richter nicht auf diese absolute Möglichkeit der Bestimmung des Personenbezugs ab.

Sofern die Möglichkeit der Bestimmbarkeit nicht objektiv ausgeschlossen ist, weil ein Dritter einen Personenbezug herstellen kann, kommt es laut EuGH auf die Mittel an, die zur Bestimmbarkeit genutzt werden können. Ganz konkret stellten die Richter die Frage ins Zentrum, ob für die verantwortliche Stelle vernünftige Mittel bestehen, um die für die Zuordnung notwendige Information vom Dritten zu erhalten.[62] Ihrer Ansicht nach kommt es also ausdrücklich nicht darauf an, dass sich „alle zur Identifizierung der betreffenden Person erforderlichen Informationen in den Händen [des für die Daten Verantwortlichen] befinden."[63]

b. Gesetzliches Verbot oder praktische Nichtdurchführbarkeit der Identifizierung

Was in diesem Zusammenhang „vernünftige Mittel" sind, wurde vom EuGH offengelassen. Es erfolgte lediglich eine negative Abgrenzung: **Mittel, die nicht vernünftigerweise eingesetzt werden** können und die deshalb bei der Bestimmung des Personenbezugs unberücksichtigt bleiben müssen, sind solche, deren Nutzung zur Identifizierung **gesetzlich verboten** ist oder mit denen die **Identifizierung praktisch nicht durchgeführt werden kann**.[64] Entweder existiert also ein gesetzliches Verbot oder praktische Gründe, die z.B. in einem „unverhältnismäßigen Aufwand an Zeit, Kosten oder Arbeitskraft"[65] begründet liegen können, die die Möglichkeit der Identifizierung einer Person ausschließen. Beide in Betracht kommenden Alternativen müssen geprüft werden, wenn bestimmt wird, ob eine Möglichkeit der Identifizierung einer Person besteht.

Da in diesem Fall keine Anzeichen bestanden, dass es einen unverhältnismäßigen Aufwand an Zeit, Kosten oder Arbeitskraft erfordern würde, die Zusatzinformationen vom Internetzugangsanbieter zu erhalten, stellte sich für den EuGH lediglich die Frage, ob ein gesetzliches Verbot der Erlangung der erforderlichen Informationen entgegenstand. Dass es an einem direkten Anspruch des Auskunftssuchenden gegenüber dem Internetzugangsanbieter mangelte, reichte dem EuGH nicht,

---

[58] *Karg*, MMR 2011, 341, 346.
[59] *US District Court for the Eastern District of Pennsylvania*, Urt. v. 3.2.2017, Misc. No. 16-960-M-01; 16-1061-M, S. 8.
[60] Dazu ausführlich: *Eckhardt*, CR 2016, 786, 786f.; *Dammann*, in: Simitis, § 3 BDSG, Rn. 24; *Gola/Klug/Körffer*, in: Gola/Schomerus, § 3 BDSG, Rn. 10
[61] *Kühling/Klar*, ZD 2017, 24, 28: „Verschärfter relativer Personenbezug". Ebenso: *Eckhardt*, ZUM 2016, 1029, 1030; *Kartheuser/Gilsdorf*, MMR-Aktuell 2016, 382533; *Mantz/Spittka*, NJW 2016, 3579, 3582; *Moos/Rothkegel*, MMR 2016, 842, 845.
[62] *EuGH*, Urt. v. 19.10.2016 – C-582/14, Rn. 45.
[63] *EuGH*, Urt. v. 19.10.2016 – C-582/14, Rn. 43.
[64] *EuGH*, Urt. v. 19.10.2016 – C-582/14, Rn. 46.
[65] *EuGH*, Urt. v. 19.10.2016 – C-582/14, Rn. 46.

um von einem gesetzlichen Verbot der Nutzung des Mittels – einer Auskunft vom Provider – auszugehen.[66] Ganz im Gegenteil bewerteten die Richter es als ausreichend, wenn eine indirekte Erlangung der für die Identifizierung erforderlichen Informationen möglich ist.

Sofern beispielsweise andere Möglichkeiten der Identifizierung bestehen, z.B. die Einschaltung einer staatlichen Behörde, die ihrerseits die Informationen erlangen könne und mit deren Hilfe die Bestimmung durchführbar sei, bestehe ein Mittel, dessen Nutzung nicht verboten sei und das deshalb als vernünftiges Mittel zur Identifizierung in Betracht komme.[67]

Der EuGH berücksichtigt also alternative Wege zur Identifizierung der Person, die z.B. in der Einschaltung von Zwischenstellen liegen können. Diese Betrachtung ist weitgehend und repräsentiert einen **umfassenden Ansatz hinsichtlich der Möglichkeiten der Identifizierung**.[68] Auch wenn bzgl. eines konkreten Datums der Personenbezug nur mittelbar über Dritte hergestellt werden kann, ist dieses Mittel als vernünftiges Mittel zu berücksichtigen. **Die Herstellung eines Personenbezugs „über's Eck" ist also ausreichend**.

c. Ergebnis

Auf dieser Basis konnte der EuGH den konkreten Fall im Ergebnis dahingehend entscheiden, dass es sich bei einer dynamischen IP-Adresse aus Sicht eines verarbeitenden Telemediendienstes um ein personenbezogenes Datum handelt, „wenn er über rechtliche Mittel verfügt, die es ihm erlauben, die betreffende Person anhand Zusatzinformation [eines Dritten] bestimmen zu lassen."[69]

Der Konditionalsatz im Ergebnis indiziert allerdings, dass eine endgültige Entscheidung damit noch nicht getroffen ist. Denn bzgl. der Existenz des notwendigen rechtlichen Mittels hielt sich der EuGH bewusst zurück, um nicht seine Kompetenzen zu überschreiten und nationalstaatliches Recht auszulegen und anzuwenden. Stattdessen verwies er zurück an das vorlegende Gericht, das zu klären hat, ob das erforderliche rechtliche Mittel für die benötigte Auskunft besteht. Falls das rechtliche Mittel für den Verantwortlichen nicht gegeben sein sollte, wäre die Erlangung des Zusatzwissens des Internetproviders gesetzlich verboten und somit aus der Bewertung des Personenbezugs auszuschließen. Sollte kein anderes Mittel bestehen, das vernünftigerweise zur Herbeiführung des Personenbezugs genutzt werden könnte, müsste konsequenterweise die Bestimmbarkeit und damit das Vorliegen eines personenbezogenen Datums abgelehnt werden.

3. Konsequenzen

Im Zusammenhang mit der endgültigen Klärung durch das nationale Gericht drängen sich weiterführende Fragestellungen auf, deren Beantwortung entscheidende Auswirkungen auf die praktische Umsetzung des *Breyer* Urteils haben wird.

a. Theoretische oder praktische Möglichkeit der Identifizierung?

Es wird zunächst zu klären sein, ob der indirekte Weg der Identifizierung tatsächlich eröffnet sein muss oder ob die theoretische Existenz dieses Weges ausreicht. Angesichts des Wortlauts des EuGH könnte davon ausgegangen werden, dass die theoretische Möglichkeit der Identifizierung bereits ausreicht.[70] Denn das Gericht bezieht sich nicht auf ein konkret bestehendes rechtliches Mittel, wie

---

[66] *EuGH*, Urt. v. 19.10.2016 – C-582/14, Rn. 47.
[67] *EuGH*, Urt. v. 19.10.2016 – C-582/14, Rn. 47.
[68] *Mantz/Spittka*, NJW 2016, 3579, 3582: „niedrige Grenze".
[69] *EuGH*, Urt. v. 19.10.2016 – C-582/14, Rn. 49.
[70] *Mantz/Spittka*, NJW 2016, 3579, 3582; Zweifelnd: *Eckhardt*, ZUM 2016, 1029, 1030.

z.B. Auskunftsansprüche, sondern auf rechtliche Mittel allgemein.[71] Zudem bestand im entschiedenen Fall auch kein Anzeichen dafür, dass ein Angriff auf das Telemedium vorlag, weshalb kein konkreter Auskunftsanspruch als rechtliches Mittel zur Identifizierung des Angreifers in Betracht kam.[72] In seiner Konsequenz würde das bedeuten, dass allein aus dem abstrakten Vorhandensein rechtlicher Mittel folgt, dass bzgl. des in Frage stehenden Datums von Personenbezug auszugehen ist.[73] Nur wenn bei Nutzung des Mittels die Grenze der Praktikabilität überschritten würde, könnte sich ein anderes Ergebnis ergeben.

Ginge man hingegen davon aus, dass ein konkretes rechtliches Mittel, das die Identifizierung ermöglicht, bestehen muss, würden sich differenzierte Ergebnisse bzgl. der gespeicherten Daten ergeben.[74] Nur die Daten von Nutzern, die bspw. im Verdacht stünden, eine Straftat begangen zu haben, wären dann als personenbezogen zu qualifizieren.[75] Innerhalb derselben Datenbank wären Daten derselben Kategorie also wahlweise personenbezogen oder nicht personenbezogen. Zudem könnten Daten durch Zusatzwissen Dritter zu personenbezogenen Daten werden.[76] Die damit einhergehende erhebliche Rechtsunsicherheit für den Betroffenen sowie den Verantwortlichen spricht dafür, die konkrete Sichtweise abzulehnen.[77]

b. EuGH Kriterien in der Praxis

Unabhängig davon, wie diese Entscheidung ausfallen wird, ist die Entscheidung des EuGH von großer praktischer Bedeutung. Denn der Gerichtshof hat generelle Kriterien für die Bestimmbarkeit bzgl. eines Datums vorgegeben. **Entscheidend kommt es darauf an, dass derjenige, der als Verantwortlicher ein Datum verarbeitet, in rechtlich zulässiger Weise und mit praktikablen Mitteln an die für die Bestimmbarkeit benötigten Zusatzinformationen herankommen kann, wobei er sich auch Dritter bedienen darf.**

Diese beiden Kriterien sind aus rechtlicher Sicht bedeutender als die eingangs angeführten Indikatoren (siehe Frage E, Teil I, Abschn. 1). Letztere sind nicht mehr als grobe Anhaltspunkte, da sich der Personenbezug immer nur unter Berücksichtigung sämtlicher Parameter im Einzelfall ergibt. **Feststehende Indikatoren für eine endgültige Bewertung des Personenbezugs können deshalb nicht aufgestellt werden.** Die Einordnung ist vielmehr kontextbezogen und hängt vor allem davon ab, wer mit den Daten umgeht, wie der Verantwortliche mit den Daten umgeht, welche ergänzenden Informationen bezüglich der Daten vorhanden sind und welche tatsächlichen und rechtlichen Möglichkeiten im Hinblick auf ergänzende Informationen bestehen.

Es ist daher nicht möglich, in negativer Hinsicht mit Hilfe eines feststehenden Indikators den Personenbezug eines Datums zu bestimmen, da diese Bewertung von den Umständen und dem Zusatzwissen im Einzelfall abhängt. Auch erfordern **Änderungen bzgl. der gesetzlichen oder technischen Bedingungen, die für die Bestimmbarkeit eines Datums relevant sind, eine ständige Neubewertung des relevanten Kontexts** (siehe Frage F, Teil II). Der Personenbezug kann lediglich unter Zuhilfenahme von Indikatoren positiv hergestellt werden, d.h. es ist möglich zu einem exakten Zeitpunkt eindeutig zu bestimmen, ob eine Personenbeziehbarkeit gegeben ist.

---

[71] Vgl. *EuGH,* Urt. v. 19.10.2016 – C-582/14, Rn. 47, Rn. 49.
[72] *Kühling, Z*D 2017, 24, 28.
[73] So *Nink*, CR 2016, 791, 794.
[74] So *Eckhardt*, CR 2016, 786, 788, der in dieser Differenzierung die Stärke der EuGH-Entscheidung sieht.
[75] So *Kartheuser/Gilsdorf*, MMR-Aktuell 2016, 382533
[76] So ähnlich auch *Weinhold*, ZD-Aktuell 2016, 05366.
[77] So auch *Richter*, EuZW 2016, 909, 913 unter Bezugnahme auf die Schlussanträge des Generalanwalts.

Vor diesem Hintergrund lohnt sich eine nähere Auseinandersetzung mit den beiden Kriterien des EuGH. Sofern ein Mittel gesetzlich verboten oder impraktikabel ist, soll es in der Zusammenschau zur Bestimmung des Personenbezugs nicht berücksichtigt werden.

aa. gesetzliche Verbote

Ein gesetzliches Verbot besteht in jedem Fall solange, wie die Zusatzinformation für den Dritten ein personenbezogenes Datum darstellt und er weder eine Einwilligung des Betroffenen für die Übermittlung der Zusatzinformation hat noch eine gesetzliche Ermächtigungsgrundlage besteht. Inwieweit das gesetzliche Verbot vor diesem Hintergrund als Ausschlusskriterium für die Bestimmbarkeit des Personenbezuges wirkt, lässt sich abstrakt kaum feststellen. Allerdings sind bestimmte Tendenzen feststellbar.

Zum einen liegt es nahe, dass der Raum für ein gesetzliches Verbot umso kleiner wird, je mehr Ermächtigungsgrundlagen für Datenabfragen geschaffen werden. Diese betreffen in erster Linie staatliche Stellen, da direkte Auskunftsansprüche für Private nur in besonderen Fällen vorgesehen sind.[78] Tendenziell werden Ermächtigungsgrundlagen in der jüngeren Gesetzgebung eher erweitert, was sich beispielsweise im Zusammenhang mit der Wiedereinführung der Vorratsdatenspeicherung zeigt. Dieses Gesetz verpflichtet zwar in erster Linie nur dazu, in größerem Umfang bestimmte TK-Daten für Auskunftsersuchen bereit zu halten. Es verleitet jedoch auch dazu, die Berechtigung zur Auskunft im Anschluss auf weitere Akteure und Anwendungsbereiche auszudehnen.[79] Indirekt vergrößert sich dadurch auch der Raum für Private, da sie über das Recht zur Akteneinsicht gem. § 406e Abs. 1 StPO unter Umständen von den Zusatzinformationen profitieren.[80] Je größer aber die Möglichkeiten sind, die erforderlichen Zusatzinformationen auf rechtlichem Wege zu erlangen, desto geringer wird die Wahrscheinlichkeit, dass das Mittel wegen eines gesetzlichen Verbots bei der Beurteilung der Bestimmbarkeit außen vor bleibt. Das Kriterium des gesetzlichen Verbots für die Bestimmbarkeit wird daher tendenziell an Bedeutung verlieren.

Zum anderen dürfte die Bedeutung der gesetzlichen Verbote insbesondere in grenzüberschreitenden Fallgestaltungen eher gering sein. Anfragen an Dritte mit dem benötigten Zusatzwissen sind gerade in Ländern erfolgversprechend, in denen Datenschutz einen anderen oder einen untergeordneten Stellenwert einnimmt. Solange nicht feststeht, dass es Dritten in fremden Territorien verboten ist, eine Anfrage bzgl. der Zusatzinformationen zu beantworten, kann auch nicht von einem gesetzlichen Verbot ausgegangen werden. Dies gilt auch, wenn die Gesetzeslage unklar ist, der konkrete Sachverhalt nicht vom Gesetz erfasst wird oder nationale Regelungen an territoriale Grenzen stoßen. **Unsicherheiten und Unklarheiten bzgl. der Rechtslage können nicht zu Lasten des Betroffenen gehen.** Im Zweifel kann sich der Verantwortliche in den erwähnten Konstellationen also nicht auf den Ausschlussgrund des gesetzlichen Verbots berufen.

Die genannte Zweifelsregelung gebietet nicht nur der Schutzzweck des Datenschutzrechts. Er lässt sich auch damit rechtfertigen, dass eine Anfrage regelmäßig eine Übermittlung des konkret

---

[78] Vgl. bspw. § 101 Abs. 2 iVm Abs. 9 UrhG.

[79] Vgl. den neu eingeführten Art. 15 Abs. 3 BayVSG (ursprünglich Art. 13 Abs. 3 BayVSG-E, Drucksache 17/10014), der eine Ausweitung der Nutzung von Vorratsdaten für nachrichtendienstliche Zwecke des Bayerischen Landesamtes für Verfassungsschutzes auch im Bereich des Fernmeldegeheimnisses enthält. Kritisch bzgl. der Gesetzesänderung: *Bäcker*, S. 12ff.

[80] *Moos/Rothkegel*, MMR 2016, 842, 846; Mahnend bzgl. der Gefahr einer Ausuferung des Datenschutzes *Eckhardt*, ZUM 2016, 1029, 1030: „Mit den Instrumenten der StPO wird sich letztlich jede Information einer Person zuordnen lassen können."

einzuordnenden Datums einschließt. Bei einer solchen Übermittlung sind die Gegebenheiten des Empfängers zu berücksichtigen. Da er aus seiner Perspektive mit verhältnismäßigem Aufwand den Betroffenen bestimmen kann, liegt eine datenschutzrechtlich relevante Übermittlung vor. Dies gilt unabhängig davon, dass die übermittelnde Stelle selbst dies nicht könnte.[81] Da zudem Folge-Übermittlungen einzubeziehen sind, kann auch das Zusatzwissen weiterer Empfänger veranschlagt werden, sofern Weiterübermittlungen nicht zuverlässig ausgeschlossen sind.[82]

Für die Entscheidung des EuGH im Fall *Breyer* nicht relevant war die Fragestellung, wie die **Situation zu bewerten ist, wenn trotz eines gesetzlichen Verbots der Personenbezug praktisch (aber rechtswidrig) hergestellt werden kann.** Argumentieren ließe sich damit, dass es in diesem Fall, weniger auf das gesetzliche Verbot, als auf die praktische Möglichkeit der Identifizierung ankommt. Steht fest, dass der Verantwortliche von der Möglichkeit rechtswidrig Gebrauch gemacht hat, kann er sich jedenfalls nicht auf den Ausschlussgrund des gesetzlichen Verbots berufen. Ein solcher Einwand wäre rechtsmissbräuchlich und widerspricht dem Schutzzweck des Datenschutzrechts. Besteht hingegen nur die praktische Möglichkeit einer rechtswidrigen Herstellung des Personenbezugs, empfiehlt sich ein differenzierter Ansatz. Unter Berücksichtigung der „faktischen Nähe zu den beim Dritten befindlichen Daten" oder der „Sensibilität der Daten" könnte das gesetzliche Verbot bei „hinreichend konkreten Anhaltspunkten für die Gefahr eines nicht rechtskonformen Zugriffs"[83] im Einzelfall als nicht wirksam bewertet werden. Folge wäre, dass der vom EuGH genannte Ausschlussgrund ausnahmsweise nicht anzuwenden wäre. Auf diesem Wege würde der Tatsache Rechnung getragen, dass eine Pönalisierung von Handlungen zwar den Befolgungsgrad erhöht, aber für sich genommen keine Garantie für rechtskonformes Verhalten bietet.[84] Somit wäre trotz der generellen Annahme eines legal handelnden Datenverarbeiters die Möglichkeit geschaffen, ein nicht ganz unwahrscheinliches illegales Handeln zu berücksichtigen.

bb. Praktikabilität

Besteht kein gesetzliches Verbot hinsichtlich der Nutzung des Mittels – der Erlangung des Zusatzwissens –, ist dieses als Mittel zur Identifizierung stets zu berücksichtigen, solange nicht die Grenze der Praktikabilität überschritten wird. Gerade in transnationalen Fallkonstellationen, wenn also das Zusatzwissen nur von einem Dritten im Ausland bereitgestellt werden kann, wird diese Grenze eine relevante Rolle spielen. Die Zusammenschau im internationalen Kontext erhöht die Wahrscheinlichkeit erheblich, dass Regelungs- und Durchsetzungslücken existieren und genutzt werden können. Beispielsweise besteht Gestaltungsspielraum bezüglich der Richtung der Weitergabe von für die Zusammenschau benötigten Informationen (Transfer des Zusatzwissens ins Inland oder Weitegabe der Daten ins Ausland). Mehrfache Weitergaben der Daten (auch in angereicherter oder veränderter Form) erweitern den Raum der Möglichkeiten auf die transitive Hülle aller Kombinationen von Datenweitergaben und Zusammenführungen. Hinzu kommt, dass die Zusammenschau und Informationsverwertung technisch in Räumen erfolgen kann, die sich weitgehend der Gesetzesdurchsetzung entziehen, bspw. durch automatische Analyse auf Satelliten, Schiffen in internationalen Gewässern oder Flugobjekten.

[81] *Gola/Klug/Körffer*, in: Gola/Schomerus, § 3 BDSG, Rn. 10; *Krüger/Maucher*, MMR 2011, 433, 437.
[82] *Dammann*, in: Simitis, § 3 BDSG, Rn. 34.
[83] *Kühling*, ZD 2017, 24, 28.
[84] *Dammann*, in: Simitis, § 3 BDSG, Rn. 28.

Der EuGH zieht die Grenze unter anderem dort, wo die Nutzung des Mittels einen unverhältnismäßigen Aufwand an Zeit, Kosten und Arbeitskräften erfordern würde.[85] Entscheidend sei, dass vor diesem Hintergrund das Risiko einer Identifizierung „de facto vernachlässigbar"[86] erscheine. Wann die Grenze erreicht ist, hängt stets von den Umständen im Einzelfall ab. Die beispielhafte Aufzählung unterstreicht allerdings, dass die Bewertung in erheblichem Maße von der organisatorischen, finanziellen und personellen Ausstattung des Verantwortlichen beeinflusst wird. Je geringer die Möglichkeiten des Verantwortlichen zur Identifizierung sind, desto eher dürfte die Grenze erreicht werden. Umgekehrt ist davon auszugehen, dass die Grenze der Praktikabilität für ein global agierendes IT-Unternehmen oder eine staatliche Behörde als Verantwortliche für den Datenumgang deutlich höher liegt.

II. Personenbezüge in der Zusammenschau verschiedener Einzeldaten

Wie unter Frage E, Teil I ausführlich erläutert, kann einerseits ein einzelnes, auch technisches Datum ausreichend sein, um den Bezug zu einer Person herzustellen. Dann ist ohne weiteres von einem personenbezogenen Datum auszugehen. Andererseits können auch mehrere einzelne Daten vorliegen, die an sich keine Identifizierung ermöglichen. Sofern aber der Verantwortliche durch eine Zusammenschau dieser Daten (oder sonstiger Daten, die er mit vernünftigen Mitteln erlangen kann) einen Personenbezug herstellen kann, handelt es sich ebenfalls um personenbezogene Daten. Im Ergebnis kommt es für den Personenbezug also weniger auf Einzeldaten oder Datensätze an, sondern auf die Möglichkeit der Identifizierbarkeit des Betroffenen.

F. Personenbeziehbarkeit und Aussagekraft von Metadaten aus technischer und juristischer Sicht: Wer kann diese Personenbeziehbarkeit mit ggf. welchen Schritten leisten? Welche unklaren Fälle gibt es, und welche maßgeblichen Kriterien entscheiden über die rechtliche Einstufung, so etwa im Falle der zum Teil so genannten „Maschinendaten"?

I. Personenbeziehbarkeit

Die Bewertung eines Datums als personenbezogen steht stets im Zusammenhang mit einem konkreten Datenumgang, also einer Erhebung, Verarbeitung oder Nutzung iSd § 3 Abs. 3 bis 5 BDSG. Für diesen konkreten Umgang gibt es zwangsläufig zumindest einen Verantwortlichen iSd § 3 Abs. 7 BDSG.[87] Es handelt sich um die Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt.

Kann diese verantwortliche Person das Datum auf eine konkrete Person beziehen, so liegt ein personenbezogenes Datum vor. Über die Verantwortlichkeit klärt sich also, auf wen es bei der Frage der Personenbeziehbarkeit ankommt. Dennoch sind auch andere Stellen und deren Zusatzwissen einzubeziehen. Dies hat der EuGH, wie oben dargelegt (vgl. Frage E, Teil I, Abschn. 2), ausdrücklich bestätigt. Dass dies nicht bedeutet, dass die Zusatzinformationen eines Dritten absolut mit in die Bewertung einfließen, sondern eine relative Sichtweise etabliert wurde, nach der es auf die Existenz

[85] *EuGH*, Urt. v. 19.10.2016 – C-582/14, Rn. 46.
[86] *EuGH*, Urt. v. 19.10.2016 – C-582/14, Rn. 46.
[87] *Dammann*, in: Simitis, § 3 BDSG, Rn. 224.

vernünftiger Mittel zur Erlangung der Zusatzinformationen ankommt, wurde ebenfalls bereits ausgeführt (vgl. Frage E, Teil I, Abschn. 2).

Dritter ist grundsätzlich jeder außerhalb der verantwortlichen Stelle.[88] Zu beachten ist, dass die Verantwortlichkeit innerhalb juristischer Personen und Behörden global gesehen wird. In der Regel entscheiden sie über die Zwecke des Datenumgangs und sind damit als verantwortliche Stelle zu qualifizieren.[89] Sofern die dort beschäftigten Personen (Arbeitnehmer, Beamte) für die verantwortliche Stelle handeln, liegt die Verantwortlichkeit weiterhin bei der übergeordneten Funktionseinheit.[90] Insofern lässt sich ein Personenbezug bei einem konkreten Datenumgang nicht mit dem Argument verneinen, dass eine praktisch handelnde Person den Betreffenden nicht identifizieren kann. Stattdessen ist das gesamte, innerhalb der verantwortlichen Stelle zu berücksichtigende Wissen bei der Bewertung einzubeziehen.

Es kommt auch nicht darauf an, ob Mensch oder Maschine die Daten erhebt und verarbeitet, sondern ob das Datum an sich die Identifizierung unter Berücksichtigung der o.g. Kriterien einer Person ermöglicht (siehe Frage C).

II. Unklare Fälle

Ausgehend vom dogmatischen Konstrukt kann es keine Unklarheiten bzgl. der Bestimmung personenbezogener Daten geben. Ein konkret zu bewertendes Datum ist entweder personenbezogen oder nicht. Dass die Frage der Bestimmbarkeit eines Datums nicht abstrakt gelöst werden kann und generelle Aussagen bzgl. vergleichbarer Datenkategorien nur schwer möglich sind, mag zwar aus praktischer Sicht für Unsicherheit sorgen.[91] Diese Situation ist allerdings die logische Konsequenz der erforderlichen Einzelfallbetrachtung.

Diese praktische Unsicherheit wurde durch das EuGH-Urteil im Fall *Breyer* zumindest teilweise reduziert. Wie erläutert, ist das Zusatzwissen eines Dritten der verantwortlichen Stelle zuzurechnen (siehe Frage E, Teil I, Abschn. 3b), solange ein vernünftiges Mittel existiert, über das sie direkt oder indirekt an das Zusatzwissen gelangen kann. Unberücksichtigt bleiben sollen bei der Einordnung die Mittel, deren Nutzung gesetzlich verboten ist oder deren Nutzung nicht praktikabel ist.

Aus praktischer Sicht bleibt trotz dieser Klarstellung vor allem aufgrund der Komplexität der jeweils in die Einzelfallbetrachtung einzubeziehenden Faktoren ein Maß an Unsicherheit bestehen. In diesem Zusammenhang spielt insbesondere der Faktor „Zeit" eine bedeutende Rolle. Denn das vorhandene Zusatzwissen ändert sich im Verlaufe der Zeit ebenso wie die Mittel, die eingesetzt werden können, um den Personenbezug herzustellen, und das Recht, das die Nutzung der Mittel reguliert.[92]

Klarzustellen ist, dass die Beurteilung eines Datums hinsichtlich seines Personenbezugs stets eine punktuelle Entscheidung in einem dynamischen Umfeld ist. Die gegenwärtigen gesetzlichen und technischen Rahmenbedingungen sind der Einzelfallbetrachtung zugrunde zulegen. Deshalb ist z.B. ein nach dem Stand der Technik verschlüsseltes Datum für einen Dritten, der das Datum - ohne Möglichkeit an den Schlüssel zu gelangen - erhält, selbst dann kein personenbezogenes Datum, wenn davon ausgegangen werden kann, dass in mittelfristiger Zukunft die Verschlüsselung verhältnismäßig

---

[88] Vgl. § 3 Abs. 8 S. 2 BDSG.
[89] *Art.-29-Datenschutzgruppe*, WP 169 vom 16.2.2010, S. 19.
[90] *Dammann*, in: Simitis, § 3 BDSG, Rn. 234.
[91] Vgl. *Dammann*, in: Simitis, § 3 BDSG, Rn. 38.
[92] *Dammann*, in: Simitis, § 3 BDSG, Rn. 30.

einfach aufgebrochen werden kann. **Umgekehrt bedeutet dies aber, dass Änderungen bzgl. der gesetzlichen oder technischen Bedingungen, die für die Bestimmbarkeit eines Datums relevant sind, eine Neubewertung erforderlich machen.** Zukünftig können Daten auf völlig anderen, schwer vorhersehbaren Wegen gewonnen werden. Als Beispiele seien Fortschritte in der Kryptoanalyse, die forensische Analyse von Endgeräten oder die Auswertung von in Cloud-Speichern abgelegten Sicherungskopien genannt. Das Risiko, an einer Entscheidung festgehalten zu haben, die durch die rechtliche und technische Entwicklung überholt wurde, liegt bei der verantwortlichen Stelle.[93]

Von einer vergleichbaren Risikoverteilung ist mit Blick auf das zu berücksichtigende Zusatzwissen auszugehen. Angesichts der stetigen Steigerung der Datenmengen, der Ausdehnung von Speicherverpflichtungen und der Verbesserung der Analysemöglichkeiten ist in zeitlicher Hinsicht eine Tendenz zur Möglichkeit der Bestimmbarkeit von Daten anzunehmen.[94] Je größer das für die Bestimmbarkeit erforderliche eigene Wissen des Verantwortlichen bzw. das Zusatzwissen, an das ein Verantwortlicher mit vernünftigen Mitteln herankommen kann, wird, desto weniger Raum bleibt, um die Bestimmbarkeit abzulehnen. Auch in diesem Zusammenhang gilt, dass die praktische Unsicherheit bzgl. der Einschätzung hinsichtlich des Personenbezugs, die aufgrund der Dynamik der Bewertungsfaktoren bestehen, dem Risikobereich des Verantwortlichen zuzuordnen ist.

III. „Maschinendaten"

Die rechtliche Einstufung der Daten erfolgt unabhängig davon, wie die Daten entstanden sind. Wie unter Frage C dargestellt, fallen Metadaten sowohl bei maschinenbasierter Telekommunikation als auch bei Telekommunikationsereignissen von Personen an. Die maßgeblichen Kriterien, die bei der Bewertung des Personenbeziehbarkeit im Einzelfall zu berücksichtigen sind, stimmen für beide Auslöser von Telekommunikation überein. Die Personenbeziehbarkeit von „Maschinendaten" wird folglich in gleicher Art und Weise beurteilt wie bei sonstigen Metadaten.

G. Kurzzusammenfassung

Aus den Antworten auf die Fragen an die Sachverständigen ergeben sich zusammenfassend folgende Schlussfolgerungen:

- Die Begriffe Verkehrs- und Nutzungsdatum stellen Unterkategorien des Metadatenbegriffes dar. Sie sind speziell in den Zusammenhängen Telemedien und Telekommunikation gebräuchlich. Den Sachverständigen ist kein Verkehrs- und Nutzungsdatum bekannt, das nicht zugleich als Metadatum bezeichnet werden kann.
- Metadaten sind verkürzt zusammengefasst „Daten über Daten". Sie können sowohl personenbezogen als auch nicht personenbezogen sein. Der Begriff der Metadaten ist bislang jedoch kein juristisch anerkannter Begriff. Dies könnte sich durch zukünftige Gesetze (vgl. Vorschlag der ePrivacy-Verordnung) ändern.
- Im Bereich der elektronischen Kommunikation hat sich der Metadatenbegriff als Gegenpol zu Inhaltsdaten entwickelt. Metadaten sind beschreibender und ergänzender Natur. Aus ihnen können oft Rückschlüsse auf den Inhalt der Kommunikation gezogen werden.
- Mit der Qualifikation als Metadatum ist noch keine Aussage darüber getroffen, ob es sich um ein personenbezogenes Datum handelt oder nicht.

---

[93] So auch *Dammann*, in: Simitis, § 3 BDSG, Rn. 38.

[94] Vgl. dazu für den speziellen Fall von DNA-Proben: *Wellbrock*, MedR 2003, 77, 79.

- Bei welcher Gelegenheit bzw. welcher Verarbeitungsart – durch Menschen oder Maschinen – die Daten anfallen, spielt technisch wie juristisch keine Rolle. Entscheidend für die datenschutzrechtliche Relevanz ist allein der Personenbezug.
- Eine Unterteilung in verschiedene Arten von Metadaten ist für die datenschutzrechtlichen Schlüsse unerheblich, da sich die Personenbeziehbarkeit nicht pauschal an der Datenart oder Kommunikationsform feststellen lässt (siehe Frage D).
- Da der Metadatenbegriff nicht zwischen den Datenarten differenziert, kann aus der Verarbeitung von Metadaten im Allgemeinen eine größere Gefahr für die Privatsphäre der Kommunikationsteilnehmer resultieren.
- Nur weil einem einzelnen Datum nicht ohne Weiteres zu entnehmen ist, welche Person es betrifft, führt dies nicht zur Ablehnung des Personenbezugs dieses Datums.
- Stattdessen sind dem EuGH zufolge „alle Mittel zu berücksichtigen, die vernünftigerweise entweder vom für die Verarbeitung Verantwortlichen oder von einem Dritten eingesetzt werden könnten, um die betreffende Person zu bestimmen."[95]
- Mittel, die nicht vernünftigerweise eingesetzt werden können und die deshalb bei der Bestimmung des Personenbezugs unberücksichtigt bleiben müssen, sind solche, deren Nutzung zur Identifizierung gesetzlich verboten sind oder mit denen die Identifizierung praktisch nicht durchgeführt werden kann.
- Entweder existiert also ein gesetzliches Verbot oder es bestehen praktische Gründe, die die Möglichkeit der Identifizierung einer Person ausschließen. Praktische Gründe können z.B. in einem „unverhältnismäßigen Aufwand an Zeit, Kosten oder Arbeitskraft"[96] begründet liegen.
- Auch wenn bzgl. eines konkreten Datums der Personenbezug nur mittelbar über Dritte hergestellt werden kann, ist dieses Mittel als vernünftiges Mittel zu berücksichtigen. Die Herstellung des Personenbezugs „über's Eck" ist also ausreichend.
- Der Personenbezug kann nur im Einzelfall und unter Berücksichtigung von Zusatzwissen sowie der Möglichkeit, sich das Zusatzwissen zu beschaffen, beurteilt werden (siehe Frage E, Teil I).
- Die theoretische Möglichkeit der Identifizierung reicht nach Ansicht der Sachverständigen aus, um von Personenbeziehbarkeit auszugehen (siehe Frage E, Teil I, Abschn. 3a).
- Personenbezug kann unter Zuhilfenahme von Indikatoren positiv hergestellt werden, d.h. es ist möglich zu einem exakten Zeitpunkt eindeutig zu bestimmen, ob eine Personenbeziehbarkeit gegeben ist.
- Im Gegensatz dazu ist es nicht möglich, in negativer Hinsicht mit Hilfe eines feststehenden Indikators den Personenbezug eines Datums zu bestimmen. Die Ablehnung der Personenbeziehbarkeit ist nur nach sorgfältiger Prüfung des Einzelfalls unter Berücksichtigung sämtlicher Umstände sowie insbesondere des Zusatzwissens möglich. Eine Möglichkeit, die Personenbeziehbarkeit auszuschließen, ist die aktive Veränderung der Daten durch den Einsatz geeigneter Anonymisierungsverfahren.
- Änderungen bzgl. der gesetzlichen oder technischen Bedingungen, die für die Bestimmbarkeit eines Datums relevant sind, machen eine Neubewertung des Personenbezuges notwendig.

[95] *EuGH*, Urt. v. 19.10.2016 – C-582/14, Rn. 42.
[96] *EuGH*, Urt. v. 19.10.2016 – C-582/14, Rn. 46.

H. Literaturverzeichnis

Artikel-29-Datenschutzgruppe	Stellungnahme 4/2007 zum Begriff „personenbezogene Daten" vom 20.6.2007, WP 136.
Artikel-29-Datenschutzgruppe	Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher" und „Auftragsverarbeiter" vom 16.2.2010, WP 169.
Bäcker, Matthias	Stellungnahme zu dem Entwurf für ein Bayerisches Verfassungsschutzgesetz vom 25.4.2016.
Böhme, Rainer	Vorlesungsfolienskript „Rechnernetze und Internettechnik", Innsbruck 2015.
Dainotti, Alberto; Pescapé, Antonio; Claffy, Kimberly, C.	Issues and Future Directions in Traffic Classification, IEEE Network 2012 (1), 35–40.
Dix, Alexander; Kipker, Dennis-Kenji; Schaar, Peter	Schnellschuss gegen die Grundrechte - Plädoyer für eine ausführliche öffentliche Debatte in Sachen Vorratsdatenspeicherung, ZD 2015, 300-305.
Eckhardt, Jens	Anmerkung zu EuGH, Urteil vom 19.10.2016 – C-582/14, ZUM 2016, 1029-1030.
Eckhardt, Jens	Anwendungsbereich des Datenschutzrechts – Geklärt durch den EuGH?, CR 2016, 786-790.
Geppert, Martin; Schütz, Raimund	Beck'scher TKG-Kommentar, 4. Auflage, München 2013.
Gersdorf, Hubertus	Telekommunikationsrechtliche Einordnung von OTT-Diensten am Beispiel von GMail, K&R 2016, 91-101.
Gola, Peter; Schomerus, Rudolf	Bundesdatenschutzgesetz, 12. überarbeitete und ergänzte Auflage, München 2015.
Graf, Jürgen-Peter	Beck'scher Online-Kommentar StPO mit RiStBV und MiStra, 27. Edition, München 2017.
Graulich, Kurt	Nachrichtendienstliche Fernmeldeaufklärung mit Selektoren in einer transnationalen Kooperation – Prüfung und Bewertung von NSA-Selektoren nach Maßgabe des Beweisbeschlusses BND-26.
Grünwald, Andreas; Nüßing, Christoph	Kommunikation over the Top – Regulierung für Skype, WhatsApp oder Gmail?, MMR 2016, 91-97.
Karg, Moritz	Die Rechtsfigur des personenbezogenen Datums - Ein Anachronismus des Datenschutzes?, ZD 2012, 255-260.

Karg, Moritz	Speicherung dynamischer IP-Adressen – Anmerkung zu BGH, Urteil vom 13.1.2011 - III ZR 146/10, MMR 2011, 341-346.
Krüger, Jochen; Möllers, Frederik	Metadaten in Justiz und Verwaltung - Neue juristische Problemkategorie im Rahmen der elektronischen Aktenführung?, MMR 2016, 728-731.
Krüger, Stefan; Maucher, Svenja-Ariane	Ist die IP-Adresse wirklich ein personenbezogenes Datum? – Ein falscher Trend mit großen Auswirkungen auf die Praxis, MMR 2011, 433-439.
Kühling, Jürgen; Klar, Manuel	Speicherung von IP-Adressen beim Besuch einer Internetseite – Anmerkungen zu EuGH, Urteil vom 19.10.2016 – C-582/14, ZD 2017, 24-29.
Kühling, Jürgen; Schall, Tobias	WhatsApp, Skype & Co.: OTT-Kommunikationsdienste im Spiegel des geltenden Telekommunikationsrechts. "Level playing field" de lege lata oder de lege ferenda?, CR 2015, 641-655.
Mantz, Reto; Spittka, Jan	Speicherung von IP-Adressen beim Besuch einer Website – Anmerkung zu EuGH, Urteil vom 19.10.2016 – C-582/14, NJW 2016, 3579-3583.
Mirkovic, Jelena; Liu, Yong	Passive and Active Measurement, Band 8995 der Reihe Lecture Notes in Computer Science, Berlin 2015.
Moos, Flemming; Rothkegel, Tobias	Speicherung von IP-Adressen beim Besuch einer Internetseite – Anmerkungen zu EuGH, Urteil vom 19.10.2016 – C-582/14, MMR 2016, 842-847.
Nink, Judith	Speicherung dynamischer IP-Adressen durch Mediendienstanbieter – Anmerkungen zu EuGH, Urteil vom 19.10.2016 – C-582/14, CR 2016, 791-795.
Ohlenburg, Anna	Der neue Telekommunikationsdatenschutz – Eine Darstellung von Teil 7 Abschnitt 2 TKG, MMR 2004, 431-440.
Ohlenburg, Anna	Die neue EU-Datenschutzrichtlinie 2002/58/EG – Auswirkungen und Neuerungen für elektronische Kommunikation, MMR 2003, 82-86.
Paal, Boris; Pauly, Daniel	Datenschutz-Grundverordnung, München 2017.
Richter, Heiko	Speicherung von IP-Adressen beim Besuch einer Website – Anmerkung zu EuGH, Urteil vom 19.10.2016 – C-582/14, EuZW 2016, 909-914.
Roßnagel, Alexander	Beck'scher Kommentar zum Recht der Telemediendienste, München 2013.
Roßnagel, Alexander; Wilke, Daniel	Die rechtliche Bedeutung gescannter Dokumente, NJW 2006, 2145-2150.

Schellenberg, Ulrich	Wie die bürgerliche Freiheit im digitalen Fegefeuer verbrennen könnte, ZRP 2014, 24-26.
Schumacher, Pascal	OTT-Dienste und Telekommunikationsrecht – Einordnung der neuen Dienste im Kontext der TK-Regulierung, K&R 2015, 771-776.
Simitis, Spiros	Bundesdatenschutzgesetz, 8., neu bearbeitete Auflage, Baden-Baden 2014.
Spindler, Gerald; Schuster, Fabian	Recht der elektronischen Medien, 3. Auflage, München 2015.
Vigna, Giovanni; Jonsson, Erland; Kruegel, Christopher	Recent Advances in Intrusion Detection, Band 2820 der Reihe Lecture Notes in Computer Science, Berlin 2003.
Waidner, Michael	Stellungnahme zur Anhörung des NSA-Untersuchungsausschusses am 26. Juni 2014.
Wellbrock, Rita	Datenschutzrechtliche Aspekte des Aufbaus von Biobanken für Forschungszwecke, Medizinrecht 2003, 77-82.
Wenzel, Henning	Rechtliche Grundlagen der IT-Forensik, NZWiSt 2016, 85-93.