Zur rechtlichen Beurteilung von Verkehrs-, Nutzungs- und Metadaten

von

Kurt Graulich

Sachverständigengutachten zum Beweisbeschluss SV-19b

vom 15. Dezember 2016 des

1. Untersuchungsausschusses des Deutschen Bundestages in der

18. Wahlperiode

Beweisthema:

(1) (a) und b)) Wie bzw. auf welche unterschiedliche Art und Weise wird der Begriff der Verkehrs- und Nutzungsdaten wissenschaftlich im technischen und juristischen Kontext gebraucht? (c)) Wie ist dieser vom Begriff der Metadaten abzugrenzen?

(2) (a) und b)) Wobei fallen diese o.g. Daten an? (c) Handelt es sich immer um Telekommunikationsereignisse von Personen? (d)) Ist auch eine maschinenbasierte Telekommunikation hiervon erfasst? (e)) Wie wäre das Gesamtaufkommen von TK-Daten diesen Klassen anteilig zuzuordnen?

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

(a) Zunächst soll aus technischer sowie aus juristischer Sicht der Begriff Metadaten geklärt werden.

(b) Dazu soll insbesondere geklärt werden, welche ggfs. feststehenden Indikatoren eine Einordnung eines einzelnen Datums als „personenbezogen"

zulassen und inwiefern, unabhängig von einzelnen Datensätzen, Personenbezügen in der Zusammenschau verschiedener, für sich betrachtet nicht personenbezogener Einzeldaten möglich sind.

(c) In einem zweiten Schritt werden die Personenbeziehbarkeit und die Aussagekraft von Metadaten aus technischer und juristischer Sicht bewertet. 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"?

(d) Welche technischen und juristischen Aussagen bzw. Bewertungen können anhand der Betrachtung eines einzelnen Datums getroffen werden?

Gliederung:

bb) Polizeirecht (§ 20m Abs. 2 BKAG)

cc) Recht der Nachrichtendienste (§ 8a Abs. 2 Satz 1 Nr. 5 BVerfSchG)

c) Abgrenzung von Verkehrs-, Nutzung- und Metadaten

2. Zur Entstehung von Verkehrs- und Nutzungsdaten

a) Was sind und wobei entstehen Verkehrsdaten?

aa) Was sind Verkehrsdaten?

aaa) Kennungen (§ 96 Abs. 1 Satz 1 Nr. 1, § 98 und § 113 Abs. 2 Satz 1 Nr. 1 TKG)

bbb) Verbindungsdauer und übermittelte Datenmengen (§ 96 Abs. 1 Satz 1 Nr. 2 TKG)

ccc) Telekommunikationsdienst (§ 96 Abs. 1 Satz 1 Nr. 3 und § 113b Abs. 2 Satz 1 Nr. 3 TKG)

ddd) Endpunkte von festgeschalteten Verbindungen (§ 96 Abs. 1 Satz 1 Nr. 4 TKG)

eee) Sonstige zum Aufbau und der Aufrechterhaltung der Verbindung notwendige Verkehrsdaten (§ 96 Abs. 1 Satz 1 Nr. 5 TKG)

fff) Pflicht zur Speicherung von Verkehrsdaten bei mobilen Telefondiensten (§ 113b Abs. 2 Satz 1 Nr. 4 TKG)

ggg) Pflicht zur Speicherung von Verkehrsdaten bei Internet-Telefondiensten (§ 113b Abs. 2 Satz 1 Nr. 5 TKG)

hhh) Erweiterte Pflicht zur Speicherung von Verkehrsdaten im Falle der Übermittlung einer Kurz-, Multimedia- oder ähnlichen Nachricht (§ 113b Abs. 2 Satz 2 TKG)

bb) Wie entstehen Verkehrsdaten?

b) Was sind und wobei entstehen Nutzungsdaten?

c) Zur Frage der notwendigen Ursächlichkeit von TK-Ereignissen von Personen bei der Entstehung solcher Daten

d) Zur etwaigen Erfassung maschinenbasierter Telekommunikation an der Entstehung von Verkehrs- bzw. Nutzungs- und Metadaten.

bb) Wer kann die Personenbeziehbarkeit und ggf. mit welchen Schritten leisten?

d) Welche juristischen Aussagen und Bewertungen können anhand einzelner Daten getroffen werden?

Gutachten

I. Auslegung des Gutachtenauftrags

Der Untersuchungsausschuss hat nebeneinander ein technisches und ein juristisches Gutachten zum Beweisthema bestellt. Der Kompetenz des Beauftragten geschuldet, werden vorliegend die juristischen Aspekte behandelt. Dem Beweisthema wurde durch den Sachverständigen eine Gliederung - von (1) bis (3) - eingefügt, die nicht Bestandteil des Beweisbeschlusses im Untersuchungsausschusses war. Sie versteht sich nicht als inhaltliche Gewichtung, sondern dient nur der besseren Strukturierung bei Beantwortung der einzelnen gutachtlichen Fragen.

II. Beantwortung der gutachtlichen Einzelfragen

Das Rechtsgutachten geht von der Normativität der zu untersuchenden Begriffe – Verkehrs-, Nutzungs- und Metadaten - aus, d.h. es werden ihre rechtliche Verwendung sowie ihr jeweiliger gesetzlicher Ausgangspunkt betrachtet; hierbei liegt der Schwerpunkt auf dem Recht des Bundes und supranationalen sowie internationalrechtlichen Regelungen. Nicht Gegenstand dieser Untersuchung ist die technische und naturwissenschaftliche Dimension der Begriffe; dazu ist ein gesondertes Gutachten bestellt worden, auf das hier pauschal verwiesen wird. Ebenso wenig wird die Begriffspraxis außerhalb des rechtlichen Rahmens ausgewertet, also umgangssprachliche, mediale und milieuübliche Verständigungsgebräuche in sozialen Netzwerken usw.; die Auseinandersetzung mit ihr dient nur der Abgrenzung zur rechtlichen Bedeutung.

1. Zum rechtlichen Gebrauch der Begriffe Verkehrs-, Nutzungs- und Metadaten

Gemäß Beweisfrage (1) ist zu klären, wie bzw. auf welche unterschiedliche Art und Weise der Begriff der Verkehrs- (a)) und Nutzungsdaten (b)) wissenschaftlich im technischen und juristischen Kontext gebraucht wird und wie dieser vom Begriff der Metadaten abzugrenzen ist. Um eine Doppelung bei den Ausführungen zu vermeiden, erfolgen Inhaltsbestimmung und

begriffliche Abgrenzung von Metadaten unter 3. a); wo durch den Beweisbeschluss gezielt nach der Klärung des Begriffs gefragt wird.

a) Verkehrsdaten

Verkehrsdaten sind solche Daten, die bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet oder genutzt werden. Es handelt sich hierbei etwa um Beginn, Ende und Dauer eines Internetzugangs, aber auch die IP-Adresse des Nutzers oder der besuchten Websites[1]. Normative Vorgaben über Verkehrsdaten der Telekommunikation finden sich in verschiedenen nationalen, supranationalen und internationalen Regelungen. In der rechtlichen Systematik steht das Telekommunikationsrecht am Anfang aller Regelungen über die Verkehrsdaten (aa)). Insbesondere das Strafrecht und Strafverfahrensrecht (bb)) setzen die Bestimmungen des Telekommunikationsrechts voraus. Hinzu kommen Eingriffsregelungen im Polizeirecht (cc)) sowie dem Recht der Nachrichtendienste (dd)).

aa) Telekommunikationsrecht

Mit jedem Telekommunikationsvorgang fallen Verkehrsdaten an. Bei der früher vorherrschenden analogen Übertragung gingen diese Daten mit der Beendigung der Verbindung verloren. Demgegenüber erzeugt die digitale Vermittlungstechnik für jede Kommunikation einen Datensatz, der zumindest kurzfristig gespeichert wird[2].

aaa) Europäisches Unions-Recht

Ausgangspunkt für die nationalen Regelungen im Telekommunikationsrecht in den Mitgliedsländern der Europäischen Union sind die einschlägigen supranationalen Regelungen. Das europäische Datenschutzrecht hat die „Verkehrsdaten" als Bestandteil des Telekommunikationsvorgangs von vornherein erfasst und in sein Schutzkonzept einbezogen. Nach den Begründungserwägungen zur Datenschurzrichtlinie für elektronische

---

[1] Köhler/Arndt/Fetzer, Recht des Internet, 7. Auflage Rn. 928

[2] BT-Drs. 16/8434, Erfahrungsbericht über die praktische Umsetzung der §§ 100g, 100h der Strafprozessordnung S. 28

Kommunikation[3] kann eine Nachricht alle Informationen über Namen, Nummern oder Adressen einschließen, die der Absender einer Nachricht oder der Nutzer einer Verbindung für die Zwecke der Übermittlung der Nachricht bereitstellt. Der Begriff „Verkehrsdaten" kann alle Formen einschließen, in die diese Informationen durch das Netz, über das die Nachricht übertragen wird, für die Zwecke der Übermittlung umgewandelt werden. Verkehrsdaten können sich unter anderem auf die Leitwege, die Dauer, den Zeitpunkt oder die Datenmenge einer Nachricht, das verwendete Protokoll, den Standort des Endgeräts des Absenders oder Empfängers, das Netz, von dem die Nachricht ausgeht bzw. an das es gesendet wird, oder den Beginn, das Ende oder die Dauer einer Verbindung beziehen. Sie können auch das Format betreffen, in dem die Nachricht über das Netz weitergeleitet wird[4]. Vorliegend enthält Art. 2 lit. b) der Datenschutzrichtlinie für den elektronischen Verkehr (Datenschutz-RL) eine Definition. Danach sind „Verkehrsdaten" Daten, die zum Zwecke der Weiterleitung einer Nachricht an ein elektronisches Kommunikationsnetz oder zum Zwecke der Fakturierung dieses Vorgangs verarbeitet werden.

bbb) Deutsches Telekommunikationsrecht

Im deutschen Telekommunikationsrecht wird der Begriff „Verkehrsdaten" in § 3 Nr. 30 TKG definiert. Danach handelt es sich um Daten, die bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet oder genutzt werden. Unionsrechtlich setzt die Regelung Art. 2 lit. b) Datenschutz-RL um[5]. Nationalrechtlich geht die Definition auf die inzwischen aufgehobene Regelung in § 2 Nr. 4 TDSV zurück[6]. Der Begriff entspricht nach dem Willen des Gesetzgebers dem seinerzeit noch synonym verwendeten Begriff „Verbindungsdaten"[7].

Das TKG kennt in seiner bestehenden Fassung zum einen auf vertraglicher Grundlage gespeicherte (§ 96 TKG) und zum anderen – nach erneuter Einführung der Vorratsspeicherung – gesetzlich verpflichtend gespeicherte Verkehrsdaten (§ 113b TKG).

---

[3] RICHTLINIE 2002/58/EG DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation)

[4] Erwägungsgrund Nr. 15

[5] Fetzer in Arndt/Fetzer/Scherer/Graulich, TKG 2. Aufl., § 3 Rn. 113

[6] Telekommunikations-Datenschutzverordnung, aufgehoben mit Wirkung vom 26.06.2004 durch das Gesetz vom 22.06.2004 (BGBl. I S. 1190)

[7] BT-Drs. 15/2316 S. 58; vgl. m.w.N. zur Begriffsgeschichte Graulich in Arndt/Fetzer/Scherer/Graulich TKG 2. Aufl. § Rn. 9 ff.

a1) Zu geschäftlichen Zwecken nach § 96 TKG gespeicherte Verkehrsdaten

Eine Reihe von Verkehrsdaten werden vom Gesetzgeber in § 96 Abs. 1 TKG benannt, und zwar im Zusammenhang mit der Bestimmung einer restriktiven Verwendung dieser Daten. Der Diensteanbieter darf die dort aufgeführten Verkehrsdaten nämlich nur erheben, soweit dies für die im 2. Abschnitt des 7. Teil des TKG genannten Zwecke erforderlich ist[8]. Nach der Umschreibung dieser Zwecke in § 91 Abs. 1 Satz 1 TKG regelt der 2. Abschnitt den Schutz personenbezogener Daten der Teilnehmer und Nutzer von Telekommunikation bei der Erhebung und Verwendung dieser Daten durch Unternehmen und Personen, die geschäftsmäßig Telekommunikationsdienste in Telekommunikationsnetzen, einschließlich Telekommunikationsnetzen, die Datenerfassungs- und Identifizierungsgeräte unterstützen, erbringen oder an deren Erbringung mitwirken.

Die danach – bei der Ausfüllung des vertraglichen Verhältnisses zwischen Kunden und TK-Dienstleister – zu erhebenden Daten werden in § 96 Abs. 1 Satz 1 TKG aufgeführt. Dazu zählen (Nr. 1.) die Nummer oder Kennung der beteiligten Anschlüsse oder der Endeinrichtung, personenbezogene Berechtigungskennungen, bei Verwendung von Kundenkarten auch die Kartennummer, bei mobilen Anschlüssen auch die Standortdaten, (Nr. 2.) den Beginn und das Ende der jeweiligen Verbindung nach Datum und Uhrzeit und, soweit die Entgelte davon abhängen, die übermittelten Datenmengen, (Nr. 3.) den vom Nutzer in Anspruch genommenen Telekommunikationsdienst, (4.) die Endpunkte von festgeschalteten Verbindungen, ihren Beginn und ihr Ende nach Datum und Uhrzeit und, soweit die Entgelte davon abhängen, die übermittelten Datenmengen sowie (Nr. 5.) sonstige zum Aufbau und zur Aufrechterhaltung der Telekommunikation sowie zur Entgeltabrechnung notwendige Verkehrsdaten.

b1) Gesetzlich verpflichtend nach § 113b TKG gespeicherte Verkehrsdaten

[8] Lutz in Arndt/Fetzer/Scherer, TKG 2. Aufl. § 96 Rn. 4

Die Vorschrift des § 113b TKG dient – nach der Bezugnahme in der Begründung des Gesetzesentwurfs - als Kernregelung der Vorratsspeicherung von Verkehrsdaten nach den Vorgaben der Entscheidungen des Bundesverfassungsgerichts[9] und des Gerichtshofs der Europäischen Union[10], indem sie die Adressaten sowie die Grundvoraussetzungen der Speicherpflichten bestimmt, die zu speichernden Datenkategorien sowie die Speicherfrist festlegt und Vorgaben macht, wie die Speicherung der Daten und deren Löschung zu erfolgen haben[11]. In § 113b TKG[12] wird die Speicherung von genau bezeichneten Verkehrsdaten angeordnet[13]; es ist nicht erkennbar,

---

[9] Das Bundesverfassungsgericht hat mit Urteil vom 2. März 2010 (BVerfGE 125, 260) die §§ 113a und 113b TKG und auch § 100g Absatz 1 Satz 1 StPO, soweit danach Verkehrsdaten nach § 113a TKG erhoben werden durften, wegen Verstoßes gegen Artikel 10 Absatz 1 des Grundgesetzes (GG) für nichtig erklärt.

[10] Der Gerichtshof der Europäischen Union hat am 8. April 2014 die Richtlinie 2006/24/EG für ungültig erklärt (verbundene Rechtssachen C-293/12 und C594/12, EuZW 2014, 459), weil sie die Grundrechte aus den Artikeln 7 und 8 der Grundrechtecharta der Europäischen Union in unverhältnismäßigem Umfang einschränkte.

[11] BT-Drs. 18/5088 S. 37

[12] Fassung aufgrund des Gesetzes zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten vom 10.12.2015 (BGBl. I S. 2218), in Kraft getreten am 18.12.2015.

[13] § 113b Pflichten zur Speicherung von Verkehrsdaten
(1) Die in § 113a Absatz 1 Genannten sind verpflichtet, Daten wie folgt im Inland zu speichern:
1. Daten nach den Absätzen 2 und 3 für zehn Wochen,
2. Standortdaten nach Absatz 4 für vier Wochen.
(2) Die Erbringer öffentlich zugänglicher Telefondienste speichern
1. die Rufnummer oder eine andere Kennung des anrufenden und des angerufenen Anschlusses sowie bei Um- oder Weiterschaltungen jedes weiteren beteiligten Anschlusses,
2. Datum und Uhrzeit von Beginn und Ende der Verbindung unter Angabe der zugrunde liegenden Zeitzone,
3. Angaben zu dem genutzten Dienst, wenn im Rahmen des Telefondienstes unterschiedliche Dienste genutzt werden können,
4. im Fall mobiler Telefondienste ferner
a) die internationale Kennung mobiler Teilnehmer für den anrufenden und den angerufenen Anschluss,
b) die internationale Kennung des anrufenden und des angerufenen Endgerätes,
c) Datum und Uhrzeit der ersten Aktivierung des Dienstes unter Angabe der zugrunde liegenden Zeitzone, wenn Dienste im Voraus bezahlt wurden,
5. im Fall von Internet-Telefondiensten auch die Internetprotokoll-Adressen des anrufenden und des angerufenen Anschlusses und zugewiesene Benutzerkennungen.
Satz 1 gilt entsprechend
1. bei der Übermittlung einer Kurz-, Multimedia- oder ähnlichen Nachricht; hierbei treten an die Stelle der Angaben nach Satz 1 Nummer 2 die Zeitpunkte der Versendung und des Empfangs der Nachricht;
2. für unbeantwortete oder wegen eines Eingriffs des Netzwerkmanagements erfolglose Anrufe, soweit der Erbringer öffentlich zugänglicher Telefondienste die in Satz 1 genannten Verkehrsdaten für die in § 96 Absatz 1 Satz 2 genannten Zwecke speichert oder protokolliert.
(3) Die Erbringer öffentlich zugänglicher Internetzugangsdienste speichern
1. die dem Teilnehmer für eine Internetnutzung zugewiesene Internetprotokoll-Adresse,

warum in der Gesetzesbegründung mitunter der Begriff Verbindungsdaten anstelle von Verkehrsdaten benutzt wird[14]. Hinsichtlich der Speicherdauer wird differenziert. Während die Verbindungsdaten für zehn Wochen zu speichern sind, ist die Speicherung der besonders sensiblen Standortdaten auf vier Wochen beschränkt.

bb) Strafrecht und Strafverfahrensrecht

Im Strafrecht und Strafverfahrensrecht finden sich Regelungen über Verkehrsdaten in der Cybercrime Convention des Europäischen Konventionsrechts (aaa)) und dem nationalen Recht der Bundesrepublik (bbb)).

aaa) Europäisches Konventions-Recht

Nach Art. 1 lit. d) der Cybercrime Convention des Europarates vom 23. November 2001, die sich mit Computerkriminalität beschäftigt, sind „Verkehrsdaten" alle Computerdaten in Zusammenhang mit einer Kommunikation unter Nutzung eines Computersystems, die von einem

---

2. eine eindeutige Kennung des Anschlusses, über den die Internetnutzung erfolgt, sowie eine zugewiesene Benutzerkennung,
3. Datum und Uhrzeit von Beginn und Ende der Internetnutzung unter der zugewiesenen Internetprotokoll-Adresse unter Angabe der zugrunde liegenden Zeitzone.
(4) Im Fall der Nutzung mobiler Telefondienste sind die Bezeichnungen der Funkzellen zu speichern, die durch den anrufenden und den angerufenen Anschluss bei Beginn der Verbindung genutzt wurden. Bei öffentlich zugänglichen Internetzugangsdiensten ist im Fall der mobilen Nutzung die Bezeichnung der bei Beginn der Internetverbindung genutzten Funkzelle zu speichern. Zusätzlich sind die Daten vorzuhalten, aus denen sich die geografische Lage und die Hauptstrahlrichtungen der die jeweilige Funkzelle versorgenden Funkantennen ergeben.
(5) Der Inhalt der Kommunikation, Daten über aufgerufene Internetseiten und Daten von Diensten der elektronischen Post dürfen auf Grund dieser Vorschrift nicht gespeichert werden.
(6) Daten, die den in § 99 Absatz 2 genannten Verbindungen zugrunde liegen, dürfen auf Grund dieser Vorschrift nicht gespeichert werden. Dies gilt entsprechend für Telefonverbindungen, die von den in § 99 Absatz 2 genannten Stellen ausgehen. § 99 Absatz 2 Satz 2 bis 7 gilt entsprechend.
(7) Die Speicherung der Daten hat so zu erfolgen, dass Auskunftsersuchen der berechtigten Stellen unverzüglich beantwortet werden können.
(8) Der nach § 113a Absatz 1 Verpflichtete hat die auf Grund des Absatzes 1 gespeicherten Daten unverzüglich, spätestens jedoch binnen einer Woche nach Ablauf der Speicherfristen nach Absatz 1, irreversibel zu löschen oder die irreversible Löschung sicherzustellen.
Vgl. im Einzelnen unten 3.

[14] BT-Drs. 18/5088 S. 27 u. 38

Computersystem, das Teil der Kommunikationskette war, erzeugt wurden und aus denen der Ursprung, das Ziel, der Leitweg, die Uhrzeit, das Datum, der Umfang oder die Dauer der Kommunikation oder die Art des für die Kommunikation benutzten Dienstes hervorgeht[15]. Nach Art. 16 Abs. 1 der Konvention trifft jede Vertragspartei die erforderlichen gesetzgeberischen und anderen Maßnahmen, damit ihre zuständigen Behörden die umgehende Sicherung bestimmter Computerdaten einschließlich Verkehrsdaten, die mittels eines Computersystems gespeichert wurden, anordnen oder in ähnlicher Weise bewirken können, insbesondere wenn Gründe zu der Annahme bestehen, dass bei diesen Computerdaten eine besondere Gefahr des Verlusts oder der Veränderung besteht.

bbb) Deutsches Strafrecht und Strafverfahrensrecht

Im nationalen Recht der Bundesrepublik sind Verkehrsdaten Gegenstand von Regelungen im Strafverfahrensrecht, insbesondere als Recht der Strafverfolgung (a1)) sowie – zumindest der Sache nach – im materiellen Strafrecht des StGB (b1)).

a1) Strafprozessordnung

Der ursprünglich in § 100g StPO verwendete Begriff der Erhebung von Verbindungsdaten[16] ist im Zuge der Angleichung an den telekommunikationsrechtlichen Sprachgebrauch in der Europäischen Union sowie dem TKG durch den Begriff Verkehrsdaten abgelöst worden. Mit beiden Begriffen sind dieselben Arten von Daten gemeint[17]. Die aktuelle Fassung von § 100g StPO geht auf den zweiten nationalgesetzlichen Anlauf zur Regelung der Vorratsdatenspeicherung - „Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten"[18] – zurück und steht in einem engen Wechselspiel mit den seinerzeit neu eingeführten §§ 113a ff. TKG beim ersten Versuch einer Normierung der Vorratsdatenspeicherung.

---

[15] Council of Europe, Sammlung der Verträge Nr. 185

[16] Der Begriff „Verbindungsdaten" kommt ursprünglich aus dem FernmeldeanlagenG, an Stelle von dessen § 12 FAG mit Wirkung vom 01.01.2002 die §§ 100g, 100h StPO in der damals geltenden Fassung getreten sind (BGBl. I 2001 S. 3879); vgl. dazu im Einzelnen Gercke in Roggan/Kutscha (Hrsg.), Handbuch zum Recht der inneren Sicherheit, 2. Aufl., 2006 S. 159 ff.

[17] BT-Drs. BT-Drs. 16/8434, Erfahrungsbericht über die praktische Umsetzung der §§ 100g, 100h der Strafprozessordnung S. 28

[18] Gesetz vom 10.12.2015 – BGBl. I 2015 S. 2218

Für die Erhebung der Daten zum Zweck der Verfolgung von besonders schweren Straftaten sieht der seinerzeit neu formulierte § 100g StPO nach Eingriffsintensität abgestufte Befugnisse vor. Dabei geht es jeweils um die bei den Erbringern öffentlich zugänglicher Telekommunikationsdienste vorhandenen Verkehrsdaten. Diese Daten haben zwei unterschiedliche Entstehungsgründe, nämlich einmal die Speicherung zu geschäftlichen Zwecken (§ 100g Absatz 1 StPO) und zum anderen die gesetzliche Verpflichtung zur Speicherung – im Rahmen der Vorratsdatenspeicherung - nach Maßgabe der §§ 113a ff. TKG (§ 100g Absatz 2 StPO)[19]. Während in Absatz 1 die Erhebung von Verkehrsdaten geregelt wird, die aus geschäftlichen Gründen bei den Erbringern öffentlich zugänglicher Telekommunikationsdienste gespeichert werden, legt Absatz 2 fest, unter welchen Voraussetzungen die nunmehr durch die neue Speicherpflicht in § 113b TKG gespeicherten Daten erhoben werden dürfen[20]. Diese Differenzierung hatte das Bundesverfassungsgericht ausdrücklich verlangt[21].

aa1) Erhebung von Verkehrsdaten, die zu geschäftlichen Zwecken gespeichert sind (§ 100g Abs. 1 Satz 1 StPO)

§ 100g Absatz 1 StPO findet ausschließlich auf die Erhebung von Verkehrsdaten Anwendung, welche die Erbringer öffentlich zugänglicher Telekommunikationsdienste nach dem abschließenden Katalog in § 96 Absatz 1 TKG zu geschäftlichen Zwecken speichern dürfen[22]. Die Voraussetzungen dafür sind Verdacht auf eine Straftat von „auch im Einzelfall erheblicher Bedeutung" (Nr. 1) oder die Begehung einer Straftat mittels Telekommunikation (Nr. 2). Das Bundesverfassungsgericht hatte in seinem Urteil über die Vorratsdatenspeicherung die Vorschrift des § 100g StPO nicht beanstandet, soweit die Verkehrsdaten, welche die Telekommunikationsunternehmen nach Maßgabe der §§ 96 ff. TKG zu

---

[19] BT-Drs. 18/5088 S. 2

[20] BT-Drs. 18/5088 S. 27

[21] BVerfGE 125, 260 <328>: „Die Verwendung der durch eine anlasslos systematische Speicherung praktisch aller Telekommunikationsverkehrsdaten gewonnenen Datenbestände unterliegt dementsprechend besonders hohen Anforderungen. Insbesondere ist diese nicht in gleichem Umfang verfassungsrechtlich zulässig wie die Verwendung von Telekommunikationsverkehrsdaten, die die Erbringer öffentlich zugänglicher Telekommunikationsdienste in Abhängigkeit von den jeweiligen betrieblichen und vertraglichen Umständen – von den Kunden teilweise beeinflussbar – nach § 96 TKG speichern dürfen. Angesichts der Unausweichlichkeit, Vollständigkeit und damit gesteigerten Aussagekraft der über sechs Monate systematisch vorsorglich erhobenen Verkehrsdaten hat ihr Abruf ein ungleich größeres Gewicht."

[22] BT-Drs. 18/5088 S. 31

geschäftlichen Zwecken speichern, im Strafverfahren erhoben werden sollen. Insofern konnte der Gesetzgeber sich frei fühlen, die Regelung in § 100g Abs. 1 StPO beizubehalten[23]. Wegen des begrifflichen Verständnisses von Verkehrsdaten verweist § 100g Abs. 1 Satz 1 StPO auf § 96 Abs. 1 TKG.

In der höchstrichterlichen Rechtsprechung ist als Anwendungsfall von § 100g Abs. 1 StPO das IP-Tracking[24] - d.h. die Erhebung der IP-Adresse, unter der ein Betroffener auf bestimmte Angebote oder Dokumente über das Internet zugreift - zur Ausspähung von Tätergruppen durch Sicherheitsbehörden zu finden. Beim "IP-Tracking" findet ein Telekommunikationsvorgang statt, denn bei jedem Öffnen einer von der Tätergruppierung heruntergeladenen, manipulierten Datei wird ein Telekommunikationsvorgang zum Server des Bundeskriminalamts ausgelöst, weil die manipulierte Datei (unbemerkt von der Tätergruppierung) ihre Inhalte ergänzen will und deshalb versucht, diese nachzuladen. Bei diesem Vorgang wird - soweit die Gruppierung keine statische IP-Adresse nutzt - eine dynamische IP-Adresse von deren Diensteanbieter vergeben. Die IP-Adresse wird ebenso wie Datum, Uhrzeit und Dauer der jeweiligen Verbindung sowohl beim Diensteanbieter erhoben als auch bei der mit dem Nachladen verbundenen Kontaktaufnahme auf dem Server des Bundeskriminalamts protokolliert[25].

bb1) Erhebung von verpflichtend gespeicherten Verkehrsdaten

---

[23] BT-Drs. 18/5088 S. 31

[24] Nach dem Sachverhalt ging es dem BKA darum die IP-Adressen einer Tätergruppe festzustellen. Dazu sollten auf einem vom Bundeskriminalamt mit der von der Tätergruppierung "E. B. " genutzten Spähsoftware "Havex RAT" (auch bekannt unter dem Namen "Dragonfly") infizierten Rechner Dateien gespeichert werden, die für die unbekannten Täter interessant erscheinen und deshalb von diesen voraussichtlich ausgeleitet, mithin heruntergeladen, werden. Die Dokumente werden zuvor mit einem Lesebestätigungsdienst präpariert, der beim Abruf bzw. beim Öffnen des Dokuments automatisch die eigene IP-Adresse der Tätergruppierung an die Seite des "Ausgespähten" zurückübermittelt. Hierzu wird das Dokument mit einem funktionslosen, 1x1-Pixel kleinen, transparenten Bild versehen, das nicht direkt in dem Office-Dokument integriert ist, sondern beim späteren Öffnen der Datei durch die allgemeine Office-Funktion "Bild einfügen" automatisch nachgeladen wird. Um das Nachladen zu ermöglichen, ist die Übermittlung der eigenen IP-Adresse der Tätergruppierung notwendig. Über die Erhebung der IP-Adresse und den Zeitpunkt des Zugriffs hinaus werden durch den Einsatz des Lesebestätigungsdienstes keine weiteren Daten erhoben; insbesondere wird das von der Maßnahme betroffene IT-System nicht durchsucht.5Das Einbetten von unsichtbaren Bildern zum Zwecke der Feststellung, wann von welcher IP-Adresse auf Internetseiten zugegriffen wird oder eine E-Mail geöffnet wird, wird von vielen Providern, Herstellern von Betriebs- und Softwaresystemen standardmäßig angeboten und von vielen Webdienste-Anbietern und Webseitenbetreibern zu kommerziellen Zwecken, insbesondere für personalisierte Werbung, genutzt, ohne dass der Anwender davon erfährt (Beispiele: ReadNotify, Google Analytics) (BGH, Beschluss vom 23. September 2014 – 1 BGs 210/14 –, Rn. 5, juris). Der BGH hat die beantragte Anordnung nach § 100g StPO erlassen.

[25] BGH, Beschluss vom 23. September 2014 – 1 BGs 210/14 –, Rn. 11, juris

(§ 100g Abs. 2 StPO)

Auch die Erhebung der verpflichtend gespeicherten Verkehrsdaten – im Rahmen der Vorratsdatenspeicherung - ist eng begrenzt. Ein Abruf dieser Daten ist nur zur Verfolgung der in § 100g Absatz 2 StPO aufgeführten besonders schweren Straftaten zulässig, die auch im Einzelfall besonders schwer wiegen müssen. Im Hinblick auf die hohe Grundrechtsrelevanz des Abrufs verpflichtend gespeicherter Daten ist der Katalog des § 100g Absatz 2 StPO im Vergleich zu dem nach der vorhergehenden Regelung (Straftaten von erheblicher Bedeutung) deutlich reduziert[26]. Die Qualifizierung einer Straftat als schwer muss nach der Rechtsprechung des BVerfG aber in der Strafnorm – insbesondere etwa durch deren Strafrahmen – einen objektivierten Ausdruck finden[27]. Eine Generalklausel oder lediglich die Verweisung auf Straftaten von erheblicher Bedeutung reichen hingegen nicht aus[28]. Außerdem wird damit dem Umstand Rechnung getragen, dass der EuGH die Speicherung von Verkehrsdaten nur für zulässig gehalten hat, soweit die Bekämpfung schwerer Kriminalität in Rede steht[29]. Der Katalog enthält Straftaten, die der Bekämpfung des Terrorismus oder dem Schutz höchstpersönlicher Rechtsgüter, insbesondere Leib, Leben, Freiheit und sexueller Selbstbestimmung, dienen. Außerdem sind besonders schwere Straftaten umfasst, bei denen die gespeicherten Verkehrsdaten nach kriminalistischer Erfahrung besonders wertvolle Dienste leisten können. Darüber hinaus ist festgelegt, dass die Strafverfolgungsbehörden Verkehrsdaten in Bezug auf alle nach § 53 StPO zeugnisverweigerungsberechtigten Personen nicht erheben dürfen. Zufallsfunde unterliegen einem Verwertungsverbot. Für den Abruf der Daten ist ein umfassender Richtervorbehalt vorgesehen; eine Eilkompetenz der Staatsanwaltschaft besteht nicht. Zudem ist die Datenerhebung als offene Maßnahme ausgestaltet. Die betroffenen Personen sind grundsätzlich vor dem Abruf der Daten zu benachrichtigen. Die Benachrichtigung kann ausnahmsweise zurückgestellt werden; dies erfordert jedoch eine richterliche Entscheidung.[30].

cc1) Erhebung von Standortdaten (§ 100g Abs. 1 Satz 3 und Abs. 2

---

[26] BT-Drs. 18/5088 S. 32

[27] BVerfGE 109, 279 <343 ff., insbesondere 347 f.>

[28] BVerfGE 125, 260 <328 f.>

[29] Der Gerichtshof der Europäischen Union hat objektive Kriterien gefordert, die den Eingriff in Artikel 7 und 8 der Charta der Grundrechte auf Straftaten beschränken, die im Hinblick auf die betroffenen Grundrechte als hinreichend schwer angesehen werden können, um den Eingriff zu rechtfertigen (Urteil Digital Rights, C-294/13 und C-594/12, Rn. 60).

[30] BT-Drs. 18/5088 S. 24

StPO)

Eine zusätzliche Einschränkung – aus Verhältnismäßigkeitsgründen – betrifft die Erhebung von Standortdaten im Zusammenhang mit derjenigen von Verkehrsdaten nach § 100g StPO. Die Erhebung von gespeicherten Standortdaten ist besonders sensibel, weil aus ihnen Bewegungsprofile erstellt werden können[31]. Standortdaten für Verkehrsdaten, die zu geschäftlichen Zwecken gespeichert wurden, dürfen nur unter den Voraussetzungen des § 100g Abs. 1 Satz 3 StPO erhoben werden. Die Erhebung von Standortdaten in diesem Fall ist nur für künftig anfallende Verkehrsdaten oder in Echtzeit und nur im Fall des Satzes 1 Nr. 1 zulässig, soweit sie für die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten erforderlich ist. Damit wird bezüglich der besonders sensiblen Standortdaten, die grundsätzlich die Erstellung von Bewegungsprofilen ermöglichen, differenziert: Nicht gespeicherte Standortdaten stehen den Behörden nach wie vor im gleichen Umfang wie vor der Neufassung zur Verfügung; auf gespeicherte Standortdaten ist der Zugriff nur noch unter den Bedingungen des § 110g Abs. 2 StPO möglich[32].

dd1) Funkzellenabfrage (§ 100g Abs. 3 StPO)

Außerdem sind durch § 100g Abs. 3 StPO die Anforderungen an die Abfrage der in einer Funkzelle angefallenen Verkehrsdaten (Funkzellenabfrage) präzisiert worden, um zu gewährleisten, dass auch bei diesen Datenerhebungen die Verhältnismäßigkeit gewahrt ist[33]. Bei Funkzellenabfragen handelt es sich nicht um Standortdatenerhebungen; vielmehr werden bei einer solchen Abfrage alle Verkehrsdaten erhoben, die in einer bestimmten Funkzelle angefallen sind, um festzustellen, welche Mobilgeräte zu einer bestimmten Zeit der betreffenden Funkzelle zuzuordnen waren. Das Gesetz führt eine Legaldefinition der Funkzellenabfrage ein und nennt ihre Voraussetzungen. Auf diese Weise wird eine normenklare Ermächtigungsgrundlage für Funkzellenabfragen geschaffen[34].

Funkzellenabfragen, bei denen auf die nach § 96 Absatz 1 TKG gespeicherten Daten zugegriffen werden soll, beruhen auf der Grundlage von Absatz 3 Satz 1. Die Voraussetzungen des Absatzes 1 Satz 1 Nummer 1 müssen vorliegen (Nr. 1). Zudem muss die Erhebung der Daten in einem angemessenen

---

[31] BT-Drs. 18/5088 S. 24

[32] BT-Drs. 18/5088 S. 27, 31, 32

[33] BT-Drs. 18/5088 S. 2

[34] BT-Drs. 18/5088 S. 32

Verhältnis zur Bedeutung der Sache stehen (Nr. 2). Schließlich muss die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise aussichtslos oder wesentlich erschwert sein (Nr. 3)[35].

Durch Funkzellenabfragen werden unvermeidbar Verkehrsdaten Dritter, namentlich solcher Personen erhoben, die – ohne Beschuldigte oder Nachrichtenmittler zu sein – in der abgefragten Funkzelle mit ihrem Mobiltelefon kommuniziert haben. Die Maßnahme kann daher im Einzelfall aus Verhältnismäßigkeitsgründen zeitlich und örtlich weiter zu begrenzen sein oder muss unterbleiben, wenn eine solche Begrenzung nicht möglich ist und das Ausmaß, in dem Dritte betroffen sind, als unangemessen erscheint[36]. Gleichwohl soll dem Grundsatz der Verhältnismäßigkeit durch eine Präzisierung der Anforderungen für die Anordnung einer Funkzellenabfrage besonders Rechnung getragen werden, um von vornherein zu verhindern, dass Verkehrsdaten Unbeteiligter über das zur Strafverfolgung unerlässliche Maß hinaus erhoben werden und dabei bei den Strafverfolgungsbehörden Bewegungsprofile erstellt werden könnten[37].

Funkzellenabfragen, bei denen auf die nach § 113b TKG verpflichtend gespeicherten Daten zugegriffen werden soll, erfolgen auf der Grundlage von § 100g Abs. 3 Satz 2 StPO in Verbindung mit Abs. 2[38].

b1) Strafgesetzbuch (§§ 202d, 206 StGB)

Der zweite legislatorische Anlauf zur Regelung der Vorratsdatenspeicherung - „Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten"[39] – hat den neuen Straftatbestand der Datenhehlerei (§ 202d StGB) hervorgebracht. Danach soll sich strafbar machen, wer nicht öffentlich zugängliche Daten, die ein anderer durch eine rechtswidrige Tat erlangt hat, sich oder einem anderen verschafft, einem anderen überlässt, verbreitet oder sonst zugänglich macht, um sich oder einen Dritten zu bereichern oder einen anderen zu schädigen[40]. Die Tat wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bedroht, wobei die Strafe nicht schwerer sein darf als die für die Vortat angedrohte Strafe. Nach seiner Entstehungsgeschichte steht die Norm in Zusammenhang mit der Vorratsspeicherung von Verkehrsdaten, erwähnt den Begriff aber nicht

---

[35] BT-Drs. 18/5088 S. 32
[36] Bundestagsdrucksache 16/5846, S. 55
[37] BT-Drs. 18/5088 S. 24
[38] BT-Drs. 18/5088 S. 33
[39] Gesetz vom 10.12.2015 – BGBl. I 2015 S. 2218
[40] BT-Drs. 18/5088 S. 28

ausdrücklich[41]. Der Gesetzgeber begründet die Einführung des strafrechtlichen Schutzes nach § 202d StGB als gegenläufige Reaktion auf die Effektivierung der Strafverfolgungsmaßnahmen beim Umgang mit Telekommunikationsdaten. Dem Anliegen, in einer immer stärker von Informations- und Kommunikationstechnologie geprägten Gesellschaft effektive Strafverfolgung zu ermöglichen, stehe die Notwendigkeit gegenüber, den strafrechtlichen Schutz von Informationssystemen und der in ihnen gespeicherten Daten vor Angriffen und Ausspähungen ausreichend zu gewährleisten. Dieser Schutz müsse sich auch gegen Tathandlungen richten, mit denen ausgespähte, abgefangene oder in anderer Weise rechtswidrig erlangte Daten gehandelt würden und damit die durch die Vortat erfolgte Beeinträchtigung der formellen Verfügungsbefugnis des Berechtigten über seine Daten fortgesetzt und vertieft werde[42].

Der neu eingeführte Straftatbestand der Datenhehlerei schützt das formelle Datengeheimnis, das durch die Vortat bereits verletzt worden ist, vor einer Aufrechterhaltung und Vertiefung dieser Verletzung. Bereits mit der Erlangung der Daten durch den Vortäter sind die formelle Verfügungsbefugnis desjenigen, der aufgrund seines Rechts an dem gedanklichen Inhalt über eine Weitergabe und Übermittlung der Daten entscheidet[43], und damit das Interesse an der Aufrechterhaltung des Herrschaftsverhältnisses über eine Information[44] beeinträchtigt worden. Dem Berechtigten wird mit der Vortat die ihm zustehende Entscheidung, wem seine Daten zugänglich sein sollen, aus der Hand genommen. Diese Rechtsgutsverletzung wird aufrechterhalten und vertieft, wenn sich im Anschluss daran ein Dritter die gestohlenen Daten verschafft und damit die Daten weiterverbreitet werden. Mit dem Datenhehler erhält eine weitere Person die Möglichkeit, über die Zugänglichmachung der Daten anstelle des Berechtigten zu entscheiden. Zugleich kann es für den Berechtigten schwieriger werden, seine Daten nachzuverfolgen und die alleinige Verfügungsbefugnis über sie zurückzugewinnen[45].

Auch ohne begriffliche Nennung werden die Verkehrsdaten dem strafrechtlichen Schutz des Fernmeldegeheimnisses unterstellt. Denn nach § 206 Abs. 5 Satz 2 StGB unterliegen dem Fernmeldegeheimnis der Inhalt der Telekommunikation und ihre näheren Umstände, insbesondere die Tatsache, ob jemand an einem Telekommunikationsvorgang beteiligt ist oder war. Und nach § 206 Abs. 5 Satz 3 StGB erstreckt sich das Fernmeldegeheimnis auch auf die näheren Umstände erfolgloser Verbindungsversuche. Damit werden die

---

[41] BT-Drs. 18/5088 S. 28

[42] BT-Drs. 18/5088 S. 2 ff.

[43] Münchener Kommentar/Graf, 2. Auflage, § 202a Rz. 2

[44] Leipziger Kommentar/Hilgendorf, 12. Auflage, § 202a Rz. 6

[45] BT-Drs. 18/5088 S. 26

rechtswidrige Lieferung von Telekommunikationsverkehrsdaten und deren Auswertung strafrechtlich geschützt[46].

cc) Polizeirecht (§ 20m Abs. 1 BKAG)

Das Bundeskriminalamt kann nach § 20m Abs. 1 BKAG ohne Wissen des Betroffenen Verkehrsdaten (§ 96 Abs. 1 und § 113a TKG) erheben zu (Nr. 1.) den entsprechend § 17 oder § 18 BPolG Verantwortlichen zur Abwehr einer dringenden Gefahr für den Bestand oder die Sicherheit des Staates oder für Leib, Leben oder Freiheit einer Person oder Sachen von bedeutendem Wert, deren Erhaltung im öffentlichen Interesse geboten ist, (Nr. 2.) der Person, bei der bestimmte Tatsachen die Annahme rechtfertigen, dass sie Straftaten gemäß § 4a Abs. 1 Satz 2 BKAG vorbereitet, (Nr. 3.) der Person, bei der bestimmte Tatsachen die Annahme rechtfertigen, dass sie für eine Person nach Nr. 1 bestimmte oder von dieser herrührende Mitteilungen entgegennimmt oder weitergibt, oder (Nr. 4.) der Person, bei der bestimmte Tatsachen die Annahme rechtfertigen, dass eine Person nach Nr. 1 deren Telekommunikationsanschluss oder Endgerät benutzen wird. Im Unterschied zu Inhaltsdaten, die sich auf den eigentlichen Gesprächsinhalt bzw. Nachrichteninhalt – beispielsweise eines Telefonats, des E-Mail-Verkehrs oder eines Skypee-Chats – beziehen, umfassen die Verkehrsdaten weitere Informationen über Ort, Zeit sowie die Art und Weise der Kommunikation[47]. Um den Begriff der Verkehrsdaten zu definieren, verweist Abs. 1 auf § 96 Abs. 1 und § 113a TKG[48]. Die Gesetzesbegründung führt ergänzend § 3 Nr. 30 TKG auf und definiert Verkehrsdaten als alle Daten, die nach § 96 Abs. 1l und § 3 Nr. 30 TKG bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet oder genutzt werden[49].

dd) Recht der Nachrichtendienste (§ 8a Abs. 2 Saz 1 Nr. 4 BVerfSchG)

Das BfV darf nach § 8a Abs. 2 Nr. 4 BVerfSchG im Einzelfall Auskunft einholen bei denjenigen, die geschäftsmäßig Telekommunikationsdienste erbringen oder daran mitwirken, zu Verkehrsdaten nach § 96 Abs. 1 Nr. 1 bis 4 des Telekommunikationsgesetzes und sonstigen zum Aufbau und zur Aufrechterhaltung der Telekommunikation notwendigen Verkehrsdaten. Mitumfasst sind Standortdaten für den Fall der „Stand-by-Daten", weil einem

---

[46] LG Bonn, Urteil vom 30. November 2010 – 23 KLs 10/10 –, Rn. 426 und 444, juris

[47] Ralf P. Schenke in Schenke/Graulich/Ruthig, Sicherheitsrecht, § 20m BKAG Rn. 1

[48] Ralf P. Schenke in Schenke/Graulich/Ruthig, Sicherheitsrecht, § 20m BKAG Rn. 14

[49] BT-Drs. 16/10121 S. 33

Mobilfunknetz zum Zweck des Aufbaus einer Telekommunikation zu einem Mobiltelefon dessen Standort – zumindest grob – bekannt sein muss[50]. Die Angabe zu einem aktiv geschalteten Mobiltelefon kann also unabhängig vom Verbindungsaufbau erfolgen[51].

b) Nutzungsdaten

Der Begriff der Nutzungsdaten gehört im Ausgangspunkt zum Telemedienrecht (aa)). Auf diese Daten sind aber Eingriffsbefugnisse der Polizei (bb)) und der Nachrichtendienste gerichtet (cc)).

aa) Telemedienrecht (§ 15 TMG)

Der Begriff „Nutzungsdaten" entstammt dem Telemediengesetz[52], dessen einschlägige datenschutzrechtliche Vorschriften wiederum auf die entsprechenden Regelungen des Teledienstedatenschutzgesetzes (TDDSG)[53]

---

[50] Mallmann in Schenke/Graulich/Ruthig, Sicherheitsrecht, § 8a BVerfSchG Rn. 14

[51] BT-Drs. 16/2921 S. 14

[52] Telemediengesetz vom 26. Februar 2007 (BGBl. I S. 179), das zuletzt durch Artikel 1 des Gesetzes vom 21. Juli 2016 (BGBl. I S. 1766) geändert worden ist

[53] Das TDDSG trat als Teil des Informations- und Kommunikationsdienste-Gesetzes (IuKDG) vom 22. Juli 1997 (BGBl. I S. 1870) zusammen mit dem Teledienstegesetz und dem Signaturgesetz in Kraft. Es trat am 1. März 2007 infolge des Erlasses des TMG (Art. 5 G vom 26. Februar 2007, BGBl. I S. 179, 185) außer Kraft
Die Regelung über die Nutzungsdaten im TDDSG befand sich in § 6 und lautete:
(1) Der Diensteanbieter darf personenbezogene Daten eines Nutzers ohne dessen Einwilligung nur erheben, verarbeiten und nutzen, soweit dies erforderlich ist, um die Inanspruchnahme von Telediensten zu ermöglichen und abzurechnen (Nutzungsdaten). Nutzungsdaten sind 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.
(2) Der Diensteanbieter darf Nutzungsdaten eines Nutzers über die Inanspruchnahme verschiedener Teledienste zusammenführen, soweit dies für Abrechnungszwecke mit dem Nutzer erforderlich ist.
(3) Der Dienstsanbieter darf für Zwecke der Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung der Teledienste Nutzungsprofile bei Verwendung von Pseudonymen erstellen, sofern der Nutzer dem nicht widerspricht. Der Diensteanbieter hat den Nutzer auf sein Widerspruchsrecht im Rahmen der Unterrichtung nach § 4 Abs. 1 hinzuweisen. Diese Nutzungsprofile dürfen nicht mit Daten über den Träger des Pseudonyms zusammengeführt werden.
(4) Der Diensteanbieter darf Nutzungsdaten über das Ende des Nutzungsvorgangs hinaus verarbeiten und nutzen, soweit sie für Zwecke der Abrechnung mit dem Nutzer erforderlich

sowie des Staatsvertrages über Mediendienste (kurz Mediendienste-Staatsvertrag oder MDStV)[54] zurückgehen[55]. Die datenschutzrechtlichen Vorschriften des TMG unterscheiden bei Erhebung und Verwendung zwischen drei Datenarten, nämlich Bestandsdaten (§ 14 Abs. 1 TMG), Nutzungsdaten (§ 15 Abs. 1 TMG) und Abrechnungsdaten (§ 15 Abs. 4 TMG)[56], die in einem funktionellen Zusammenhang stehen.

Der Begriff der Bestandsdaten in § 14 Abs. 1 TMG entspricht weitgehend dem der Bestandsdaten in § 3 Nr. 3 TKG. Er umfasst sämtliche Daten die für die Begründung, inhaltlichen Ausgestaltung oder Änderung eines Vertragsverhältnisses zwischen Diensteanbieter und Nutzer über die Nutzung von Telemedien erforderlich sind. Sie dürfen ohne Einwilligung des Nutzers nur erhoben und verwendet werden, soweit dies für die Durchführung des Vertragsverhältnisses auch tatsächlich erforderlich ist[57].

---

sind (Abrechnungsdaten). Zur Erfüllung bestehender gesetzlicher, satzungsmäßiger oder vertraglicher Aufbewahrungsfristen darf der Diensteanbieter die Daten sperren.
(5) Der Diensteanbieter darf an andere Diensteanbieter oder Dritte Abrechnungsdaten übermitteln, soweit dies zur Ermittlung des Entgelts und zur Abrechnung mit dem Nutzer erforderlich ist. Hat der Dienstsanbieter mit einem Dritten einen Vertrag über den Einzug des Entgelts geschlossen, so darf er diesem Dritten Abrechnungsdaten übermitteln, soweit es für diesen Zweck erforderlich ist. Handelt es sich dabei um Daten, die beim Diensteanbieter auch dem Fernmeldegeheimnis unterliegen, ist der Dritte zur Wahrung des Fernmeldegeheimnisses zu verpflichten. Zum Zwecke der Marktforschung anderer Diensteanbieter dürfen anonymisierte Nutzungsdaten übermittelt werden. Nach Maßgabe der hierfür geltenden Bestimmungen darf der Diensteanbieter Auskunft an Strafverfolgungsbehörden und Gerichte für Zwecke der Strafverfolgung erteilen.
(6) Die Abrechnung über die Inanspruchnahme von Telediensten darf Anbieter, Zeitpunkt, Dauer, Art, Inhalt und Häufigkeit bestimmter von einem Nutzer in Anspruch genommener Teledienste nicht erkennen lassen, es sei denn, der Nutzer verlangt einen Einzelnachweis.
(7) Der Diensteahbieter darf Abrechnungsdaten, die für die Erstellung von Einzelnachweisen über die Inanspruchnahme bestimmter Angebote auf Verlangen des Nutzers verarbeitet werden, höchstens bis zum Ablauf des sechsten Monats nach Versendung der Rechnung speichern. Werden gegen die Entgeltforderung innerhalb dieser Frist Einwendungen erhoben oder diese trotz Zahlungsaufforderung nicht beglichen, dürfen die Abrechnungsdaten aufbewahrt werden, bis die Einwendungen abschließend geklärt sind oder die Entgeltforderung beglichen ist.
(8) Liegen dem Diensteanbieter zu dokumentierende tatsächliche Anhaltspunkte vor, dass seine Dienste von bestimmten Nutzern in der Absicht in Anspruch genommen werden, das Entgelt nicht oder nicht vollständig zu entrichten, darf er die personenbezogenen Daten dieser Nutzer über das Ende des Nutzungsvorgangs sowie die in Absatz 7 genannte Speicherfrist hinaus nur verarbeiten und nutzen, soweit dies zur Durchsetzung seiner Ansprüche gegenüber dem Nutzer erforderlich ist. Der Diensteanbieter hat die Daten unverzüglich zu löschen, wenn die Voraussetzungen nach Satz 1 nicht mehr vorliegen oder die Daten für die Rechtsverfolgung nicht mehr benötigt werden. Der betroffene Nutzer ist zu unterrichten, sobald dies ohne Gefährdung des mit der Maßnahme verfolgten Zweckes möglich ist.

[54] Z.B. Niedersachsen durch Gesetz vom 19. Juni 1997 (NdsGVBl. 1997, S.280)

[55] M.w.N. BT-Drs. 16/3078 S. 12

[56] Köhler/Arndt/Fetzer, Recht des Internet, 7. Aufl. Rn. 930

[57] Köhler/Arndt/Fetzer, Recht des Internet, 7. Aufl. Rn. 931

Nach der Definition in § 15 Abs. 1 TMG[58] darf der Diensteanbieter personenbezogene Daten eines Nutzers nur erheben und verwenden, soweit dies erforderlich ist, um die Inanspruchnahme von Telemedien zu ermöglichen und abzurechnen (Nutzungsdaten). Nutzungsdaten sind

---

[58] 15 Nutzungsdaten
(1) 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). Nutzungsdaten sind insbesondere
1. Merkmale zur Identifikation des Nutzers,
2. Angaben über Beginn und Ende sowie des Umfangs der jeweiligen Nutzung und
3. Angaben über die vom Nutzer in Anspruch genommenen Telemedien.
(2) Der Diensteanbieter darf Nutzungsdaten eines Nutzers über die Inanspruchnahme verschiedener Telemedien zusammenführen, soweit dies für Abrechnungszwecke mit dem Nutzer erforderlich ist.
(3) Der Diensteanbieter darf für Zwecke der Werbung, der Marktforschung oder zur bedarfsgerechten Gestaltung der Telemedien Nutzungsprofile bei Verwendung von Pseudonymen erstellen, sofern der Nutzer dem nicht widerspricht. Der Diensteanbieter hat den Nutzer auf sein Widerspruchsrecht im Rahmen der Unterrichtung nach § 13 Abs. 1 hinzuweisen. Diese Nutzungsprofile dürfen nicht mit Daten über den Träger des Pseudonyms zusammengeführt werden.
(4) Der Diensteanbieter darf Nutzungsdaten über das Ende des Nutzungsvorgangs hinaus verwenden, soweit sie für Zwecke der Abrechnung mit dem Nutzer erforderlich sind (Abrechnungsdaten). Zur Erfüllung bestehender gesetzlicher, satzungsmäßiger oder vertraglicher Aufbewahrungsfristen darf der Diensteanbieter die Daten sperren.
(5) Der Diensteanbieter darf an andere Diensteanbieter oder Dritte Abrechnungsdaten übermitteln, soweit dies zur Ermittlung des Entgelts und zur Abrechnung mit dem Nutzer erforderlich ist. Hat der Diensteanbieter mit einem Dritten einen Vertrag über den Einzug des Entgelts geschlossen, so darf er diesem Dritten Abrechnungsdaten übermitteln, soweit es für diesen Zweck erforderlich ist. Zum Zwecke der Marktforschung anderer Diensteanbieter dürfen anonymisierte Nutzungsdaten übermittelt werden. § 14 Abs. 2 findet entsprechende Anwendung.
(6) Die Abrechnung über die Inanspruchnahme von Telemedien darf Anbieter, Zeitpunkt, Dauer, Art, Inhalt und Häufigkeit bestimmter von einem Nutzer in Anspruch genommener Telemedien nicht erkennen lassen, es sei denn, der Nutzer verlangt einen Einzelnachweis.
(7) Der Diensteanbieter darf Abrechnungsdaten, die für die Erstellung von Einzelnachweisen über die Inanspruchnahme bestimmter Angebote auf Verlangen des Nutzers verarbeitet werden, höchstens bis zum Ablauf des sechsten Monats nach Versendung der Rechnung speichern. Werden gegen die Entgeltforderung innerhalb dieser Frist Einwendungen erhoben oder diese trotz Zahlungsaufforderung nicht beglichen, dürfen die Abrechnungsdaten weiter gespeichert werden, bis die Einwendungen abschließend geklärt sind oder die Entgeltforderung beglichen ist.
(8) Liegen dem Diensteanbieter zu dokumentierende tatsächliche Anhaltspunkte vor, dass seine Dienste von bestimmten Nutzern in der Absicht in Anspruch genommen werden, das Entgelt nicht oder nicht vollständig zu entrichten, darf er die personenbezogenen Daten dieser Nutzer über das Ende des Nutzungsvorgangs sowie die in Absatz 7 genannte Speicherfrist hinaus nur verwenden, soweit dies für Zwecke der Rechtsverfolgung erforderlich ist. Der Diensteanbieter hat die Daten unverzüglich zu löschen, wenn die Voraussetzungen nach Satz 1 nicht mehr vorliegen oder die Daten für die Rechtsverfolgung nicht mehr benötigt werden. Der betroffene Nutzer ist zu unterrichten, sobald dies ohne Gefährdung des mit der Maßnahme verfolgten Zweckes möglich ist.

insbesondere (Nr. 1.) Merkmale zur Identifikation des Nutzers, (Nr. 2.) Angaben über Beginn und Ende sowie des Umfangs der jeweiligen Nutzung und (Nr. 3.) Angaben über die vom Nutzer in Anspruch genommenen Telemedien. Der Umgang mit Nutzungsdaten ist in § 15 Abs. 2 bis 3 TMG geregelt. Nutzungsdaten, die nicht zur Abrechnung von Telemedien benötigt werden, sind grundsätzlich mit dem Ende einer Nutzung zu löschen. Daten, die zur Abrechnung benötigt werden (sog. Abrechnungsdaten, § 15 Abs. 4 TMG), dürfen höchstens bis zum Ablauf von 6 Monaten nach Versendung der Rechnung gespeichert werden (§ 15 Abs. 7 TMG)[59].

Eine besondere Regelung enthält § 15a TMG für den Fall unrechtmäßiger Übermittlung oder Kenntniserlangung von Bestands- oder Nutzungsdaten: „Stellt der Diensteanbieter fest, dass bei ihm gespeicherte Bestands- oder Nutzungsdaten unrechtmäßig übermittelt worden oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind, und drohen schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen des betroffenen Nutzers, gilt § 42a BDSG entsprechend."[60] § 15a TMG enthält eine Informationspflicht für nicht-öffentliche Stellen und ihnen datenschutzrechtlich gleichgestellte öffentlich-rechtliche Wettbewerbsunternehmen. Sonstige öffentliche Stellen werden nicht einbezogen. Die Informationspflicht besteht, wenn bestimmte besonders sensible personenbezogene Daten Dritten unrechtmäßig zur Kenntnis gelangen und schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der Betroffenen drohen[61]. Zu den geschützten besonders sensiblen personenbezogenen Daten aus dem Verfügungsbereich der verantwortlichen Stelle gehören solche, die einem Berufsgeheimnis unterliegen, personenbezogene Daten, die sich auf strafbare Handlungen oder Ordnungswidrigkeiten oder den Verdacht strafbarer Handlungen oder Ordnungswidrigkeiten beziehen, und personenbezogene Daten zu Bank- oder Kreditkartenkonten[62]. Die Vorschrift des § 42a BDSG soll demnach bereichsspezifisch für den fehlerhaften Umgang mit Nutzungsdaten und Bestandsdaten nach dem TMG gelten[63].

Der Begriff Nutzungsdaten wurde mit § 15 TMG durch das Gesetz zur Vereinheitlichung von Vorschriften über bestimmte elektronische Informations- und Kommunikationsdienste (Elektronischer-

---

[59] Köhler/Arndt/Fetzer, Recht des Internet, 7. Aufl. Rn. 933 ff.

[60] § 15a TMG in der Fassung d. Gesetzes zur Änderung datenschutzrechtlicher Vorschriften vom 14. August 2009, BGBl. I 2009 S. 2814

[61] Die Vorschrift knüpft an einen Vorschlag der Kommission der Europäischen Gemeinschaften zur Änderung der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der Elektronischen Kommunikation /(KOM(2007)698 endg.) und Regelungen im Recht der Vereinigten Staaten von Amerika an (BT-Drs. 16/12011 S. 34).

[62] BT-Drs. 16712011 S. 34

[63] BT-Drs. 16/12011 S. 36

Geschäftsverkehr-Vereinheitlichungsgesetz – EIGVG)[64] eingeführt. Bereits in der Stellungnahme des Bundesrates zum Gesetzesentwurf der Bundesregierung wurde klargemacht, dass die Erhebung von Bestands- und Nutzungsdaten, die nicht – wie bei der Telekommunikationsüberwachung – im Rahmen des eigentlichen Übertragungsvorgangs stattfinde, ein Eingriff in das Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) sei. Ein Eingriff in Art. 10 GG liege hingegen auch bei der Erhebung von Nutzungsdaten nicht vor. Das Fernmeldegeheimnis nach Art. 10 GG schütze den durch Netzbetreiber vermittelten Fernmeldeverkehr und umfasse sowohl den Inhalt als auch die Umstände desselben. Das Fernmeldegeheimnis beziehe sich nur auf den eigentlichen Übertragungsvorgang. Der Schutzbereich werde durch den Herrschaftsbereich des Betreibers des Fernmeldenetzes umgrenzt. Der Grundrechtsschutz des Art. 10 GG ende daher am Endgerät des Telekommunikationsteilnehmers und gelte nicht im Verhältnis der Kommunikationspartner untereinander. Die Nutzer eines Telemediendienstes und der Diensteanbieter stünden zueinander im Verhältnis von Kommunikationspartnern. Soweit die Nutzungsdaten daher nach Abschluss der dem Telemediendienst zu Grund liegenden Telekommunikation beim Diensteanbieter gespeichert würden, seien sie nicht vom Schutzbereich des Art. 10 GG umfasst.[65]

Bezogen auf Internetkommunikation hat das Bundesverfassungsgericht etwa Maildienste, Chatdienste und nichtöffentliche Diskussionsforen als vom Schutzbereich des Art. 10 Abs. 1 GG erfasst angesehen[66].

Die datenschutzrechtliche Verantwortlichkeit nach dem Telemediengesetz hat das Bundesverwaltungsgericht zu einer – noch nicht entschiedenen - Vorlage an den EuGH[67] gebracht. Gegenstand ist ein Vorabentscheidungsersuchen zur Klärung der datenschutzrechtlichen Verantwortlichkeit für die beim Aufruf einer Facebook-Fanpage erhobenen Nutzerdaten:

1. Ist Art. 2 Buchst. d) EGRL 46/95 dahin auszulegen, dass er Haftung und Verantwortlichkeit für Datenschutzverstöße abschließend und erschöpfend regelt oder verbleibt im Rahmen der "geeigneten Maßnahmen" nach Art. 24 EGRL 46/95 und der "wirksame[n] Eingriffsbefugnisse" nach Art. 28 Abs. 3 Spiegelstrich 2 EGRL 46/95 in mehrstufigen Informationsanbieterverhältnissen Raum für eine Verantwortlichkeit einer Stelle, die nicht im Sinne des Art. 2 Buchst. d) EGRL 46/95 für die Datenverarbeitung verantwortlich ist, bei der Auswahl eines Betreibers für sein Informationsangebot?

---

[64] Gesetz vom 26.02.2007 – BGBl. I 2007 S. 179

[65] BT-Drs. 16/3078 S. 18

[66] BGH, Urteil vom 26. November 2015 – I ZR 3/14 –, Rn. 52, juris unter Hinweis auf BVerfGE 120, 274, 340; vgl. auch BVerfGE 113, 348, 383

[67] BVerwG, EuGH-Vorlage vom 25. Februar 2016 – 1 C 28/14 –, juris

2. Folgt aus der Pflicht der Mitgliedstaaten nach Art. 17 Abs. 2 EGRL 46/95, bei der Datenverarbeitung im Auftrag vorzuschreiben, dass der für die Verarbeitung Verantwortliche einen "Auftragsverarbeiter auszuwählen hat, der hinsichtlich der für die Verarbeitung zu treffenden technischen Sicherheitsmaßnahmen und organisatorischen Vorkehrungen ausreichend Gewähr bietet", im Umkehrschluss, dass bei anderen Nutzungsverhältnissen, die nicht mit einer Datenverarbeitung im Auftrag im Sinne des Art. 2 Buchst. e) EGRL 46/95 verbunden sind, keine Pflicht zur sorgfältigen Auswahl besteht und auch nach nationalem Recht nicht begründet werden kann?

3. Ist in Fällen, in denen ein außerhalb der Europäischen Union ansässiger Mutterkonzern in verschiedenen Mitgliedstaaten rechtlich selbständige Niederlassungen (Tochtergesellschaften) unterhält, nach Art. 4, Art. 28 Abs. 6 EGRL 46/95 die Kontrollstelle eines Mitgliedstaates zur Ausübung der nach Art. 28 Abs. 3 EGRL 46/95 übertragenen Befugnisse gegen die im eigenen Hoheitsgebiet gelegene Niederlassung auch dann befugt, wenn diese Niederlassung allein für die Förderung des Verkaufs von Werbung und sonstige Marketingmaßnahmen mit Ausrichtung auf die Einwohner dieses Mitgliedstaates zuständig ist, während der in einem anderen Mitgliedstaat gelegenen selbständigen Niederlassung (Tochtergesellschaft) nach der konzerninternen Aufgabenverteilung die ausschließliche Verantwortung für die Erhebung und Verarbeitung personenbezogener Daten im gesamten Gebiet der Europäischen Union und damit auch in dem anderen Mitgliedstaat obliegt, wenn tatsächlich die Entscheidung über die Datenverarbeitung durch den Mutterkonzern getroffen wird?

4. Sind Art. 4 Abs. 1 Buchst. a), Art. 28 Abs. 3 EGRL 46/95 dahin auszulegen, dass in Fällen, in denen der für die Verarbeitung Verantwortliche eine Niederlassung im Hoheitsgebiet eines Mitgliedstaates besitzt und eine weitere, rechtlich selbständige Niederlassung in dem Hoheitsgebiet eines anderen Mitgliedstaates besteht, die u.a. für den Verkauf von Werbeflächen zuständig ist und deren Tätigkeit auf die Einwohner dieses Staates ausgerichtet ist, die in diesem anderen Mitgliedstaat zuständige Kontrollstelle Maßnahmen und Anordnungen zur Durchsetzung des Datenschutzrechts auch gegen die nach der konzerninternen Aufgaben- und Verantwortungsverteilung für die Datenverarbeitung nicht verantwortliche weitere Niederlassung richten kann oder sind Maßnahmen und Anordnungen dann nur durch die Kontrollbehörde des Mitgliedstaates möglich, in dessen Hoheitsgebiet die konzernintern verantwortliche Stelle ihren Sitz hat?

5. Sind Art. 4 Abs. 1 Buchst. a), Art. 28 Abs. 3 und 6 EGRL 46/95 dahin auszulegen, dass in Fällen, in denen die Kontrollbehörde eines Mitgliedstaates eine in ihrem Hoheitsgebiet tätige Person oder Stelle nach Art. 28 Abs. 3 EGRL 46/95 wegen der nicht sorgfältigen Auswahl eines in den Datenverarbeitungsprozess eingebundenen Dritten in Anspruch nimmt, weil

dieser Dritte gegen Datenschutzrecht verstoße, die tätig werdende Kontrollbehörde an die datenschutzrechtliche Beurteilung der Kontrollbehörde des anderen Mitgliedstaates, in dem der für die Datenverarbeitung verantwortliche Dritte seine Niederlassung hat, in dem Sinne gebunden ist, dass sie keine hiervon abweichende rechtliche Beurteilung vornehmen darf, oder darf die tätig werdende Kontrollstelle die Rechtmäßigkeit der Datenverarbeitung durch den in einem anderen Mitgliedstaat niedergelassenen Dritten als Vorfrage des eigenen Tätigwerdens selbständig auf seine Rechtmäßigkeit prüfen?

6. Soweit der tätig werdenden Kontrollstelle eine selbständige Überprüfung eröffnet ist: Ist Art. 28 Abs. 6 Satz 2 EGRL 46/95 dahin auszulegen, dass diese Kontrollstelle die ihr nach Art. 28 Abs. 3 EGRL 46/95 übertragenen wirksamen Einwirkungsbefugnisse gegen eine in ihrem Hoheitsgebiet niedergelassene Person oder Stelle wegen der Mitverantwortung für die Datenschutzverstöße des in einem anderen Mitgliedstaat niedergelassenen Dritten nur und erst dann ausüben darf, wenn sie zuvor die Kontrollstelle dieses anderen Mitgliedstaates um die Ausübung ihrer Befugnisse ersucht hat?

bb) Polizeirecht (§ 20m Abs. 2 BKAG)

Nach § 20m Abs. 2 BKAG kann das BKA unter den Voraussetzungen des Abs. 1 von denjenigen, die geschäftsmäßig eigene oder fremde Telemedien zur Nutzung bereithalten oder den Zugang zur Nutzung vermitteln, Auskunft über Nutzungsdaten (§ 15 Abs. 1 TMG) verlangen. Die Auskunft kann auch über zukünftige Nutzungsdaten angeordnet werden. Die Daten sind unverzüglich sowie auf dem vom Bundeskriminalamt bestimmten Weg durch den Diensteanbieter zu übermitteln. Zur Auskunft verpflichtet ist, wer geschäftsmäßig eigene oder fremde Telemedien zur Nutzung bereithält oder den Zugang zur Nutzung vermittelt (Telemedienunternehmen)[68]. Nach der Gesetzesbegründung gehören hierzu insbesondere Internetauktionshäuser oder Internettauschbörsen, Anbieter von Videos auf Abruf oder Suchmaschinen im Internet[69].

cc) Recht der Nachrichtendienste (§ 8a Abs. 2 Satz 1 Nr. 5 BVerfSchG)

Nach Maßgabe von § 8a Abs. 2 Satz 1 Nr. 5 BVerfSchG darf das BfV bei denjenigen, die geschäftsmäßig Teledienste erbringen oder daran mitwirken,

[68] Ralf P. Schenke in Schenke/Graulich/Ruthig, Sicherheitsrecht, § 20m BKAG Rn. 21
[69] BT-Drs. 16/10121 S. 33

Auskunft einholen über die dort genannten Angaben zur Nutzeridentifikation, Nutzung und in Anspruch genommene Teledienste. Diese Nutzungsdaten entsprechen den in § 15 Abs. 1 TMG konkret aufgeführten Datenarten[70]. Sie sind auf diese beschränkt[71].

c) Abgrenzung von Verkehrs-, Nutzung- und Metadaten

Der Beweisbeschluss möchte unter 1. c) wissen, wie die Begriffe Verkehrsdaten und Nutzungsdaten vom Begriff der Metadaten abzugrenzen sei. Es geht also um die Klärung des Verhältnisses dieser drei Begriffe zueinander. Das ist hinsichtlich der beiden ersten Begriffe bereits an dieser Stelle möglich.

Der Begriff Verkehrsdaten entstammt dem Telekommunikationsrecht und umfasst nach § 96 Abs. 1 Satz 1 TKG (Nr. 1.) die Nummer oder Kennung der beteiligten Anschlüsse oder der Endeinrichtung, personenbezogene Berechtigungskennungen, bei Verwendung von Kundenkarten auch die Kartennummer, bei mobilen Anschlüssen auch die Standortdaten, (Nr. 2.) den Beginn und das Ende der jeweiligen Verbindung nach Datum und Uhrzeit und, soweit die Entgelte davon abhängen, die übermittelten Datenmengen, (Nr. 3.) den vom Nutzer in Anspruch genommenen Telekommunikationsdienst, (Nr. 4.) die Endpunkte von festgeschalteten Verbindungen, ihren Beginn und ihr Ende nach Datum und Uhrzeit und, soweit die Entgelte davon abhängen, die übermittelten Datenmengen und (Nr. 5.) sonstige zum Aufbau und zur Aufrechterhaltung der Telekommunikation sowie zur Entgeltabrechnung notwendige Verkehrsdaten. Sie werden vom Gesetz selbst nicht als personenbezogene Daten bezeichnet, aber nach dem inzwischen allgemeinen Rechtsverständnis als solche angesehen (vgl. 3. b)).

Der Begriff Nutzungsdaten entstammt dem Telemedienrecht. Nach § 15 Abs. 1 TMG handelt es sich – von Gesetzes wegen - um personenbezogene Daten des Nutzers eines Telemediendienstes, und zwar insbesondere (Nr. 1.) Merkmale zur Identifikation des Nutzers, (Nr. 2.) Angaben über Beginn und Ende sowie des Umfangs der jeweiligen Nutzung und (Nr. 3.) Angaben über die vom Nutzer in Anspruch genommenen Telemedien.

Die vollständige Beantwortung der Frage setzt eine genaue Untersuchung des Begriffs „Metadaten" voraus, die aber erst an nachgeordneter Stelle

---

[70] Mallmann in Schenke/Graulich/Ruthig, Sicherheitsrecht, § 8a BVerfSchG Rn. 15

[71] BT-Drs. 16/2921 S. 15

unternommen wird. Der Beweisbeschluss gibt nämlich unter 3. a) auf, den Begriff „Metadaten" juristisch zu klären[72].

[72] Zur Vermeidung von Redundanz wird daher auf den Prüfungsabschnitt (3. a) ff)) verwiesen.

2. Zur Entstehung von Verkehrs- und Nutzungsdaten

Gemäß Beweisfrage (2)) ist zu klären, wobei diese o.g. Daten anfallen. Diese Frage zwingt hintergründig zur gesonderten Untersuchung von Verkehrsdaten (a)) und Nutzungsdaten (b)). Der Begriff Verkehrsdaten gehört zu den Telekommunikationsdiensten und derjenige der Nutzungsdaten zu den Telemediendiensten, die beide wiederum Unterfälle der elektronischen Informations- und Kommunikationsdienste (IuK-Dienste) sind[73]. Für den Ort und Entstehungszusammenhang dieser Daten kommt es also darauf an, worunter die entsprechende Dienstleistung einzuordnen ist. Weiter ist zu klären, (c)) ob es sich immer um Telekommunikationsereignisse von Personen handelt oder (d)) ob auch eine maschinenbasierte Telekommunikation hiervon erfasst ist und (e)) wie das Gesamtaufkommen von TK-Daten diesen Klassen anteilig zuzuordnen wäre.

a) Was sind und wobei entstehen Verkehrsdaten?

Im ersten Abschnitt der Antwort auf Beweisfrage 2 geht es darum, welche Arten von Verkehrsdaten bei den verschiedenen Formen digitaler Telekommunikation entstehen. (aa)). In einem zweiten Schritt soll untersucht werden, wie diese typischerweise entstehen (bb)).

aa) Was sind Verkehrsdaten?

Auflistungen von Verkehrsdaten finden sich hinsichtlich der zu geschäftlichen Zwecken gespeicherten in § 96 TKG und hinsichtlich der gesetzlich verpflichtend gespeicherten in § 113b TKG. Hinzu kommt die Spezialregelung über Standortdaten in § 98 TKG. Es ist im Rahmen des vorliegenden Gutachtens nicht möglich, sämtliche gesetzlich geregelten Fälle des Umgangs mit Verkehrsdaten im TKG darzustellen und zu erörtern. Aber eine grundlegende Einführung in die Fälle der vertraglich geregelten Umgangspflichten sowie der gesetzlich verpflichtenden Fälle – i.R. der Vorratsdatenspeicherung – wird nachfolgend unternommen.

aaa) Kennungen (§ 96 Abs. 1 Satz 1 Nr. 1, § 98 und § 113 Abs. 2 Satz 1

[73] BT-Drs. 16/3078 S. 13

Nr. 1 TKG)

Nach § 96 Abs. 1 Satz 1 Nr. 1. TKG darf der TK-Diensteanbieter die Nummer oder Kennung der beteiligten Anschlüsse oder der Endeinrichtung, personenbezogene Berechtigungskennungen, bei Verwendung von Kundenkarten auch die Kartennummer, bei mobilen Anschlüssen auch die Standortdaten speichern. § 96 Abs. 1 Satz 1 Nr. 1 TKG bezieht sich nur auf die Nummer i.S.d. § 3 Nr. 13 TKG[74] der beteiligten Anschlüsse oder der Endeinrichtung. Hierdurch fallen auch IP-Adressen unter den Begriff er Verkehrsdaten, soweit sie zum Aufbau, zur Aufrechterhaltung der Telekommunikation oder zur Entgeltabrechnung notwendig sind. erfasst werden damit insbesondere die IP-Adressen bei VoIP-Verbindungen[75]. Das Bundesverfassungsgericht hat im Rahmen seiner Entscheidung über die Vorratsdatenspeicherung IP-Adressen als Verkehrsdaten eingeordnet[76]. In einer weiteren Entscheidung hat das Bundesverfassungsgericht ausgeführt, dass § 113 Abs. 1 Satz 1 TKG bei verfassungskonformer Auslegung keine Rechtsgrundlage für die Zuordnung von dynamischen IP-Adressen bietet[77].

Außerdem werden von § 96 Abs. 1 Nr. 1 TKG personenbezogene Berechtigungskennungen – z.B. PIN und TAN -, bei Verwendung von Kundenkarten[78] auch die Kartennummer sowie bei mobilen Anschlüssen die Standortdaten i.S.d. § 3 Nr. 19 TKG[79] erfasst. Zu den Verkehrsdaten gehören damit auch die Positionsdaten eines Endgeräts, und zwar unabhängig davon, ob das Gerät genutzt wird. In Bezug auf die Verwendung von Standortdaten für die Erbringung von Diensten mit Zusatznutzen enthält das TKG jedoch in § 98 TKG eine Sondervorschrift, die in ihrem Anwendungsbereich einer Verwendung von Standortdaten nach § 96 TKG vorgeht[80]. § 113b Abs. 2 Satz 1 Nr. 1 TKG Nummer 1 stellt sicher, dass bei der Vorratsdatenspeicherung – auch im Falle von Um- oder Weiterschaltungen eines Anrufs – die im Bereich der Telefonie zur Identifizierung der Kommunikationsteilnehmer

---

[74] Nach § 3 Nr. 13 TKG sind „"Nummern" Zeichenfolgen, die in Telekommunikationsnetzen Zwecken der Adressierung dienen"

[75] Lutz in Arndt/Fetzer/Scherer/Graulich TKG, 2. Aufl. § 96 Rn. 6

[76] BVerfG, v. 02.03.2010, MMR 2010, 356

[77] BVerfG, v. 24.01.2012, NJW 2012, 1419

[78] Nach § 3 Nr. 11 TKG sind „"Kundenkarten" Karten, mit deren Hilfe Telekommunikationsverbindungen hergestellt und personenbezogene Daten erhoben werden können"

[79] Nach § 3 Nr. 19 TKG sind „"Standortdaten" Daten, die in einem Telekommunikationsnetz oder von einem Telekommunikationsdienst erhoben oder verwendet werden und die den Standort des Endgeräts eines Endnutzers eines öffentlich zugänglichen Telekommunikationsdienstes angeben"

[80] Lutz in Arndt/Fetzer/Scherer/Graulich, TKG 2. Aufl., § 96 Rn. 9

erforderlichen Rufnummern oder anderen Anschlusskennungen verfügbar sind[81].

bbb) Verbindungsdauer und übermittelte Datenmengen (§ 96 Abs. 1 Satz 1 Nr. 2 TKG)

Nach § 96 Abs. 1 Satz 1 Nr. 2 TKG darf der TK-Anbieter den Beginn und das Ende der jeweiligen Verbindung nach Datum und Uhrzeit und, soweit die Entgelte davon abhängen, die übermittelten Datenmengen speichern. Unzulässig ist nach der Rechtsprechung die Erhebung von Datenvolumen und Verbindungsdauer, wenn die Abrechnung der Dienste volumen- und zeitunabhängig erfolgt, mithin eine Flatrate vereinbart worden ist[82].

ccc) Telekommunikationsdienst (§ 96 Abs. 1 Satz 1 Nr. 3 und § 113b Abs. 2 Satz 1 Nr. 3 TKG)

Nach § 96 Abs. 1 Satz 1 Nr. 3 TKG darf der TK-Dienstleister den vom Nutzer in Anspruch genommenen Telekommunikationsdienst[83] speichern. Die Regelung betrifft die Art des vom Nutzer in Anspruch genommenen TK-Dienstes i.S.d. § 3 Nr. 24 TKG, also im Wesentlichen, ob es sich um Sprachtelefonie, Datenübertragung, Faxdienst oder andere Dienste handelt[84]. § 113b Abs. 2 Satz 1 Nr. 3 TKG betrifft bei der Vorratsdatenspeicherung die Fallgestaltung, dass im Rahmen des Telefondienstes weitere Dienste in Anspruch genommen werden können. In diesem Fall ist auch die Angabe zu speichern, welcher Dienst bei dem jeweiligen Telekommunikationsvorgang genutzt wurde (im ISDN etwa Sprach-, Telefax- oder Datenübertragung; im Mobiltelefondienst etwa die Versendung von Kurzmitteilungen [SMS] oder von Multimediadaten [MMS])[85].

ddd) Endpunkte von festgeschalteten Verbindungen (§ 96 Abs. 1 Satz

---

[81] BT-Drs. 18/5088 S. 34

[82] M.w.N. Lutz in Arndt/Fetzer/Scherer/Graulich, TKG 2. Aufl., § 96 Rn. 10

[83] Nach § 3 Nr. 24 sind "Telekommunikationsdienste" in der Regel gegen Entgelt erbrachte Dienste, die ganz oder überwiegend in der Übertragung von Signalen über Telekommunikationsnetze bestehen, einschließlich Übertragungsdienste in Rundfunknetzen

[84] Lutz in Arndt/Fetzer/Scherer/Graulich, TKG 2. Aufl. § 96 Rn. 12

[85] BT-Drs. 18/5088 S. 38

1 Nr. 4 TKG)

Nach § 96 Abs. 1 Satz 1 Nr. 4 TKG darf der TK-Dienstleister die Endpunkte von festgeschalteten Verbindungen, ihren Beginn und ihr Ende nach Datum und Uhrzeit und, soweit die Entgelte davon abhängen, die übermittelten Datenmengen speichern. Kennzeichnend für solche Verbindungen ist, dass sie nicht kurzfristig auf- und wieder abgebaut werden, sondern über eine bestimmte Zeitspanne aufrechterhalten werden. Hiervon können auch DSL- oder Kabelmodemverbindungen betroffen sein, sofern sie nicht zeitabhängig, sondern volumentarifiert oder Flatrate-basiert sind. Entscheidend ist allein, ob dem Teilnehmer die Verbindung permanent zur Verfügung steht[86].

eee) Sonstige zum Aufbau und der Aufrechterhaltung der Verbindung notwendige Verkehrsdaten (§ 96 Abs. 1 Satz 1 Nr. 5 TKG)

Nach § 96 Abs. 1 Satz 1 Nr. 5 TKG darf der T-Dienstleister sonstige zum Aufbau und zur Aufrechterhaltung der Telekommunikation sowie zur Entgeltabrechnung notwendige Verkehrsdaten speichern. Mit dieser zukunftsoffenen, flexiblen Regelung wird die Erhebung und Verwendung auch solcher Daten ermöglicht, die sich aus neuen Technologien ergeben.

fff) Pflicht zur Speicherung von Verkehrsdaten bei mobilen Telefondiensten (§ 113b Abs. 2 Satz 1 Nr. 4 TKG)

Im Falle der Vorratsdatenspeicherung beschreibt § 113b Abs. 2 Satz 1 Nr. 4 TKG besondere Speichervorgaben für den Bereich der Mobilfunktelefonie. Nach Buchst. a sind die internationalen Kennungen für mobile Teilnehmer für den anrufenden und den angerufenen Anschluss zu speichern (so genannte IMSI). Nach Buchst. b sind die internationalen Kennungen der anrufenden und der angerufenen Endgeräte zu speichern (so genannte IMEI). Nach Buchst. c ist bei der Inanspruchnahme im Voraus bezahlter anonymer Telefondienste der Zeitpunkt der ersten Aktivierung des Dienstes zu speichern. Sofern die Aktivierung einer solchen sogenannten Prepaidkarte mittels Anrufs beim TK-Diensteerbringer erfolgt, werden diese Daten bereits durch die Nr. 1, 2 und 4 Buchst. a und b erfasst, so dass auf der Grundlage

[86] Lutz in Arndt/Fetzer/Scherer/Graulich, TKG 2. Aufl, § 96 Rn. 13

dieses Aktivierungsverfahrens Buchst. c zu keiner zusätzlichen Datenspeicherung führt. Soweit die Aktivierung des Dienstes auf eine Weise erfolgt, bei der Verkehrsdaten weder erzeugt noch verarbeitet werden, wie dies etwa der Fall sein kann, wenn die Freischaltung durch eine sofortige Onlineanmeldung bei Vertragsschluss von einem Mitarbeiter des Erbringers öffentlich zugänglicher Telekommunikationsdienste erfolgt, begründet dies nach Maßgabe von Abs. 1 Satz 1 keine Speicherpflicht[87].

ggg) Pflicht zur Speicherung von Verkehrsdaten bei Internet-Telefondiensten (§ 113b Abs. 2 Satz 1 Nr. 5 TKG)

§ 113b Abs. 2 Satz 1 Nr. 5 TKG regelt bei der Vorratsdatenspeicherung für den Bereich der Internettelefonie die Pflicht zur Speicherung der Internetprotokoll-Adressen des anrufenden und des angerufenen Anschlusses, um eine Bestimmung des Anschlusses zu ermöglichen, der Ziel oder Ursprung eines Internettelefonats war. Bei Internet-Telefondiensten sind auch die zugewiesenen Benutzerkennungen zu speichern[88].

hhh) Erweiterte Pflicht zur Speicherung von Verkehrsdaten im Falle der Übermittlung einer Kurz-, Multimedia- oder ähnlichen Nachricht (§ 113b Abs. 2 Satz 2 TKG)

Nach § 113b Abs. 2 Satz 2 TKG gelten im Falle der Vorratsdatenspeicherung für die TK-Dienstleister die erweiterten Pflichten bei für Verkehrsdaten im Falle von zwei Gruppen (Nr. 1 und 2) in qualifizierter Weise. Satz 1 gilt entsprechend demnach entsprechend (Nr. 1.) bei der Übermittlung einer Kurz-, Multimedia- oder ähnlichen Nachricht; hierbei treten an die Stelle der Angaben nach Satz 1 Nr. 2 die Zeitpunkte der Versendung und des Empfangs der Nachricht; (Nr. 2.) für unbeantwortete oder wegen eines Eingriffs des Netzwerkmanagements erfolglose Anrufe, soweit der Erbringer öffentlich zugänglicher Telefondienste die in Satz 1 genannten Verkehrsdaten für die in § 96 Absatz 1 Satz 2 genannten Zwecke speichert oder protokolliert.

bb) Wie entstehen Verkehrsdaten?

---

[87] BT-Drs. 18/5088 S. 38 ff.

[88] BT-Drs. 18/5088 S. 39

Die Frage – „wobei diese Daten anfallen" - ist hinsichtlich der Verkehrsdaten eindeutig zu beantworten. Nach § 3 Nr. 30 TKG handelt es sich bei „Verkehrsdaten" um Daten, die bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet oder genutzt werden.[89]. Für jede Kommunikationsbeziehung wird im digitalen Netz ein Datensatz erzeugt, der der rechnergesteuerten Herstellung und Aufrechterhaltung der Verbindung dient. Diese Daten werden überschrieben und damit gelöscht, wenn die Verbindung von einem herkömmlichen analogen Anschluss hergestellt worden ist. Ist sie hingegen von einem Anschluss aufgebaut worden, bei dem die Digitalisierung der Sprachsignale bereits im Endgerät des Teilnehmers erfolgt, werden die Verbindungsdaten bis zur Rechnungserstellung gespeichert[90]. Nach § 3 Nr. 24 TKG sind "Telekommunikationsdienste" in der Regel gegen Entgelt erbrachte Dienste, die ganz oder überwiegend in der Übertragung von Signalen über Telekommunikationsnetze bestehen, einschließlich Übertragungsdienste in Rundfunknetzen. Das Erfordernis, dass der Dienst „in der Regel gegen Entgelt erbracht wird", muss nach einer typisierenden Betrachtung geprüft werden: Ausreichend ist demnach, dass der Dienst gewöhnlich gegen Entgelt erbracht wird, selbst wenn er im Einzelfall unentgeltlich ist. Ausdrückliche Beispiele für Telekommunikationsdienste sind demnach Übertagungsdienste in

[89] Unionsrechtlich setzt die Regelung Art. 2 lit. b) Datenschutz-RL um (Fetzer in Arndt/Fetzer/Scherer/Graulich, TKG 2. Aufl., § 3 Rn. 113). Nationalrechtlich geht die Definition auf die inzwischen aufgehobene Regelung in § 2 Nr. 4 TDSV zurück (Telekommunikations-Datenschutzverordnung, aufgehoben mit Wirkung vom 26.06.2004 durch das Gesetz vom 22.06.2004 (BGBl. I S. 1190)).

[90] BVerfG, Urteil vom 12. März 2003 – 1 BvR 330/96 –, Rn. 71, juris

Rundfunknetzen, Sprachtelefonie und E-Mail-Übertragungsdienste[91]. Art und Inhalt der übertragenen Informationen sind unerheblich[92].

b) Was sind und wobei entstehen Nutzungsdaten?

Schwieriger ist die Beantwortung hinsichtlich der Nutzungsdaten, denn sie verschränken sich in einem gewissen Maße mit den Verkehrsdaten. Der Begriff „Nutzungsdaten" entstammt dem Telemediengesetz[93], und zwar insbesondere § 15 TMG. Aufgrund der Regelbeispiele in § 15 Abs. 1 Satz 2 TMG sind Nutzungsdaten insbesondere (Nr. 1.) Merkmale zur Identifikation des Nutzers, (Nr. 2.) Angaben über Beginn und Ende sowie des Umfangs der jeweiligen Nutzung und (Nr. 3.) Angaben über die vom Nutzer in Anspruch genommenen Telemedien. Nach der Legaldefinition in § 15 Abs. 1 Satz 1 TMG darf der Diensteanbieter personenbezogene Daten eines Nutzers nur erheben und verwenden, soweit dies erforderlich ist, um die Inanspruchnahme von Telemedien zu ermöglichen und abzurechnen (Nutzungsdaten).

Für die Entstehung von Nutzungsdaten ausschlaggebend ist somit, ob sie bei der Inanspruchnahme von Telemedien erhoben werden. Der Begriff der Telemedien ergibt sich wiederum aus der Legaldefinition in § 1 Abs. 1 Satz 1 TMG: Dieses Gesetz gilt nach § 1 Abs. 1 TMG für alle elektronischen Informations- und Kommunikationsdienste, soweit sie nicht Telekommunikationsdienste nach § 3 Nr. 24 TKG, die ganz in der Übertragung von Signalen über Telekommunikationsnetze bestehen, telekommunikationsgestützte Dienste nach § 3 Nr. 25 TKG oder Rundfunk

---

[91] Fetzer in Arndt/Fetzer/Scherer/Graulich, TKG, 2. Aufl., § 3 Rn. 104. Für die Einordnung von Sprachtelefonie und E-Mail-Übertragungsdiensten als Telekommunikationsdienste spricht auch Erwägungsgrund 10 der Datenschutzrichtlinie: Danach umfasst die Begriffsbestimmung für Dienste der Informationsgesellschaft in Artikel 1 der Richtlinie 98/34/EG des Europäischen Parlaments und des Rates vom 22. Juni 1998 über ein Informationsverfahren auf dem Gebiet der Normen und technischen Vorschriften und der Vorschriften für die Dienste der Informationsgesellschaft einen weiten Bereich von wirtschaftlichen Tätigkeiten, die online erfolgen. Die meisten dieser Tätigkeiten werden vom Geltungsbereich der vorliegenden Rahmen-RL nicht erfasst, weil sie nicht ganz oder überwiegend in der Übertragung von Signalen über elektronische Kommunikationsnetze bestehen. Sprachtelefonie und E-Mail-Übertragungsdienste hingegen werden von dieser Richtlinie erfasst. Dasselbe Unternehmen, beispielsweise ein Internet-Diensteanbieter, kann sowohl elektronische Kommunikationsdienste, wie den Zugang zum Internet, als auch nicht unter diese Richtlinie fallende Dienste, wie die Bereitstellung von Internet gestützten Inhalten, anbieten (RICHTLINIE 2002/21/EG DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 7. März 2002 über einen gemeinsamen Rechtsrahmen für elektronische Kommunikationsnetze und -dienste (Rahmenrichtlinie), Erwägungsgrund 10,).

[92] Fetzer in Arndt/Fetzer/Scherer/Graulich, TKG, 2. Aufl., § 3 Rn. 102

[93] Telemediengesetz vom 26. Februar 2007 (BGBl. I S. 179), das zuletzt durch Artikel 1 des Gesetzes vom 21. Juli 2016 (BGBl. I S. 1766) geändert worden ist

nach § 2 des Rundfunkstaatsvertrages sind (Telemedien). Das TMG gilt für alle Anbieter einschließlich der öffentlichen Stellen unabhängig davon, ob für die Nutzung ein Entgelt erhoben wird.

Die Beantwortung der Frage, ob es sich bei einem Dienst um einen Telemediendienst oder einen Telekommunikationsdienst handelt, hängt entscheidend davon ab, ob bei einer elektronischen Leistung ausschließlich eine technische Übertragung erbracht wird – dann handelt es sich um einen Telekommunikationsdienst -, oder ob nur überwiegend eine technische Übertragung erbracht wird – dann handelt es sich sowohl um einen Telekommunikationsdienst als auch um einen Telemediendienst[94]. Telekommunikationsdienst, die ganz in der Übertragung von Signalen über Telekommunikationsnetze bestehen, sind keine Telemediendienste, sondern beurteilen sich ausschließlich nach dem TKG. Davon zu unterscheiden sind die Telekommunikationsdienste, die überwiegend in der Übertragung von Signalen über Telekommunikationsnetze bestehen, also neben der Übertragungsleistung noch eine inhaltliche Dienstleistung anbieten, wie der Internet-Zugang und die E-Mail-Übertragung. Diese sind zugleich Telemediendienste und fallen damit mit Ausnahme der Vorschriften zum Datenschutz auch unter das TMG. Die bloße Internet-Telefonie (Voice over Internet Protocol – VoIP) fällt nicht unter die Telemediendienste. Während die Bereitstellung eines Internetz-Zugangs oder eines E-Mail-Dienstes eine besondere Dienstleistung darstellt, weist das Telefonieren über das Internet keinen äußerlich erkennbaren Unterschied zu herkömmlichen leitungsgebundenen Telefonie auf und ist daher ausschließlich dem TKG zuzuordnen. Unter Telemediendienste fallen alle übrigen Informations- und Kommunikationsdienste, die also nicht ausschließlich Telekommunikationsdienste oder Rundfunk sind. Bei Telemedien handelt es sich beispielsweise um Online-Angebote von Waren/Dienstleistungen mit unmittelbarer Bestellmöglichkeit, Video auf Abruf, soweit es sich nicht nach Form und Inhalt um einen Fernsehdienst im Sinne der Richtlinie 89/552/EWG (Richtlinie Fernsehen ohne Grenzen) handelt, aber auch Online-Dienste, die Instrumente zur Datensuche[95].

c) Zur Frage der notwendigen Ursächlichkeit von TK-Ereignissen von Personen bei der Entstehung solcher Daten

Nach Beweisfrage 2 b) soll geklärt werden, ob es sich bei der Entstehung von Verkehrs-, Nutzungs- und Metadaten immer um

---

[94] Fetzer in Arndt/Fetzer/Scherer/Graulich, TKG 2. Aufl, § 3 Rn. 103

[95] BT-Drs. 16/3078 S. 13

Telekommunikationsereignisse von Personen handelt. Aus der rechtlichen Sicht ist diese Frage zu verneinen. Die gesetzlichen Anforderungen an die Entstehung solcher Daten verlangen nicht, dass Personen miteinander kommunizieren.

Kriterium für Verkehrsdaten ist nach § 3 Nr. 30 TKG, dass sie bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet oder genutzt werden; auf die Natur der Teilnehmer kommt es nicht an. Nutzungsdaten dürfen nach § 15 Abs. 1 Satz 1 TMG erhoben und verwendet werden, soweit dies erforderlich ist, „um die Inanspruchnahme von Telemedien zu ermöglichen und abzurechnen"; auch insoweit kommt es auf die Natur der Nutzer nicht an.

d) Zur etwaigen Erfassung maschinenbasierter Telekommunikation an der Entstehung von Verkehrs- bzw. Nutzungs- und Metadaten.

Die Beweisfrage 2 c) möchte weiterhin wissen, ob auch eine maschinenbasierte Telekommunikation „hiervon" erfasst ist. Im Rahmen dieses rechtlichen Gutachtens wird nicht erwogen, welche Rolle „maschinenbasierte Telekommunikation" im IT-Bereich insgesamt spielt. Der Begriff der „Verkehrsdaten" in § 3 Nr. 30 TKG gilt auch für die Telekommunikation von Maschinen. Und der Schutz des Art. 10 Abs. 1 GG erfasst jegliche Art und Form von Telekommunikation; es macht keinen Sinn, das Eingreifen des Schutzbereichs davon abhängig zu machen, ob ein Mensch speziell die Entstehung eines Verkehrsdatums auslöst oder ob dieses – prozessbeding – im Verlauf eines Kommunikationsvorgangs entsteht, der lediglich ursprünglich von einem Menschen angestoßen worden ist.

Dieses Verständnis wird ferner durch das Zusammenwirken von Art. 10 Abs. 1 GG und § 88 TKG gestützt. Soweit Art. 10 Abs. 1 GG unmittelbar nur vor staatlichen Eingriffen schützt, ergibt sich daraus nämlich auch ein Schutzauftrag des Staates gegenüber Grundrechtsträgern, die als Private Zugriffsmöglichkeiten auf die Telekommunikation haben. Dabei ist der Schutz des Fernmeldegeheimnisses durch § 88 TKG als einfachgesetzliche Ausprägung des verfassungsrechtlichen Schutzes anzusehen[96] mit dem Ziel, die Teilnehmer der Fernkommunikation vor Kenntnisnahme und Unterdrückung durch die Anbieter der Telekommunikation zu schützen[97]. Nach § 88 Abs. 1 TKG schützt das Fernmeldegeheimnis den Inhalt der Telekommunikation und ihre näheren Umstände, insbesondere die Tatsache, ob jemand an einem Telekommunikationsvorgang beteiligt ist oder war, und

[96] BT-Drucks. 13/3608, S. 53

[97] Schnabel, MMR 2008, 281, 283

es erstreckt sich auch auf die näheren Umstände erfolgloser Verbindungsversuche[98]. Der Schutz ist technologieneutral und umfasst auch die Kommunikation durch Computer oder sonstige Endeinrichtungen[99].

Umgekehrt wird eine natürliche oder juristische Person auch rechtlich verantwortlich gemacht für Aktionen von Rechnern, die ihnen zugeordnet werden können. Die zeigt die umfangreiche wettbewerbsrechtliche Judikatur zum sog. filesharing, dessen Operationen weitgehend auf Rechnerkommunikation veruhen. Die Kommunikation zwischen Client und Server (sog. eDonkey-Server) findet in diesen Fällen typischerweise wie folgt statt: Der Client übermittelt die Informationen über seine freigegebenen Dateien an einen Server, der diese indiziert. Der Client möchte eine Datei suchen und übermittelt einen Teil eines Dateinamens an einen oder mehrere Server. Die angefragten Server durchsuchen in ihren Indices und schicken die entsprechenden eD2K-Links zurück. Der Client fragt regelmäßig alle bekannten Server ab, welche Clients die Dateien freigeben, die er herunterladen möchte. Die Server schauen in ihren Indices nach und senden IP-Adressen und Ports dieser Clients zurück. Die Server verwalten also nur einen Index der freigegebenen Dateien und der dazugehörigen Client-Adressen[100].

Deutlich wird der Übergang von „Menschen-" und „Maschinenkommunikation" beim Einsatz von IP-Adressen. Die IP-Adresse ist ein numerisches Adressformat, welches die Kommunikation vernetzter Geräte - Server oder Privatcomputer - im Internet ermöglicht. Bei Abruf einer Seite wird dem Server, auf dem die Seite gespeichert ist, die Adresse des abrufenden Computers mitgeteilt, so dass die Daten über das Internet von dem einen an den anderen Rechner geleitet werden können. Für die Verbindung von Privatanwendern mit dem Internet können feste (statische) IP-Adressen vergeben werden. IP-Adressen – im seitherigen IPv4 Protokoll - dienen der Adressierung eines Rechners und besitzen daher weder aus sich heraus noch im Zusammenhang mit anderen Nutzungsdaten in Bezug auf die Nutzung einer Internetpräsenz einen unmittelbaren Bezug zu einer natürlichen Person. Eine statische IP-Adresse wird als stets personenbezogenes Datum betrachtet – sofern sie einer natürlichen und nicht einer juristischen Person zugeordnet ist -, da grundsätzlich für jedermann die Zuordnung der statischen IP-Adresse zu ihrem Inhaber möglich ist und sie

---

[98] BVerfG MMR 2008, 315, 316 m.w.N.

[99] LG Hamburg, Urteil vom 12. März 2010 – 308 O 640/08 –, Rn. 46, juris

[100] OLG Düsseldorf, Urteil vom 15. Oktober 2008 – I-20 U 196/07 –, Rn. 3, juris; vgl. auch den Unterlassungsausspruch im Beschluss des LG Hamburg vom 15.7.2005, Aktenzeichen: 308 O 378/05

„personenbeziehbar" ist. Allerdings offenbart eine IP-Adresse nicht unmittelbar die Person „dahinter"[101].

e) Zur etwaigen Zuordnung des Gesamtaufkommens von TK-Daten an den Verkehrs-, Nutzungs- und Metadaten

Beweisfrage 2 d) möchte wissen, wie das Gesamtaufkommen von TK-Daten diesen Klassen anteilig zuzuordnen wäre. Dabei handelt es sich nicht um eine rechtliche, sondern um eine tatsächliche Frage, zu der dem Rechtssachverständigen keine Informationen vorliegen.

[101] Graulich in Arndt/Fetzer/Scherer/Graulich, TKG 2 Aufl. § 88 Rn. 37

3. Welche Verkehrsdaten (Metadaten) entstehen bei der digitalen Telekommunikation, und welche datenschutzrechtlichen Schlüsse lassen sich daraus ziehen?

Beweisfrage 3 möchte wissen, welche Arten von Metadaten bei den verschiedenen Formen digitaler Telekommunikation entstehen und welche datenschutzrechtlichen Schlüsse sich aus ihrer Analyse ziehen lassen. Die Antwort auf die Frage wird anhand der vier Untergliederungen entwickelt, die der Beweisbeschluss vorgibt, nämlich zum Begriff der Metadaten (a)), den Arten von Verkehrsdaten bei digitaler Telekommunikation (b)), den Möglichkeiten datenschutzrechtlicher Schlussfolgerungen daraus (c)) und welche juristischen Aussagen und Bewertungen anhand einzelner der Daten getroffen werden können (d)).

a) Zur Bedeutung und Verwendung des Begriffs Metadaten

Beweisfrage 3. a) möchte wissen, wie von Verkehrs- und Nutzungsdaten der Begriff der Metadaten abzugrenzen ist. Dazu ist zu untersuchen, inwieweit der Begriff Metadaten überhaupt zur deutschen Rechtssprache gehört. Zunächst wird hierzu nach seiner Verwendung in Gesetzen (aa)) geforscht, sodann nach seinem Vorkommen in der verfügbaren Rechtsprechung (bb)). Schließlich soll – lediglich beispielhaft und ohne Anspruch auf Vollständigkeit – ein Blick auf seine Verbreitung beim Regierungshandeln und in der Verwaltung (cc)), im allgemeinen wissenschaftlichen Gebrauch (dd)) und in der medialen Umgangssprache (ee)) geworfen werden.

aa) Verwendung des Begriffs in der Gesetzessprache

Der Begriff Metadaten wird in den die Sicherheit betreffenden Gesetzen – mit einer nachfolgend zu erwähnenden spezifischen Ausnahme - nicht verwendet. Er kommt nicht im Strafrecht und Strafprozessrecht vor und ist weder Gegenstand von Regelungen der Polizei- oder Nachrichtendienstgesetze des Bundes noch von solchen des normierten Telekommunikations- oder Medienrechts. Er wird auch nicht in der Verordnung über die technische und organisatorische Umsetzung von Maßnahmen zur Überwachung der Telekommunikation

(Telekommunikations-Überwachungsverordnung - TKÜV)[102] verwendet, die im Wesentlichen der technischen Umsetzung der Überwachungsmaßnahmen im Bereich der Telekommunikation dient; erst in der untergesetzlichen Technische Richtlinie zur Umsetzung gesetzlicher Maßnahmen zur Überwachung der Telekommunikation, Erteilung von Auskünften (TR TKÜV)[103] taucht der Begriff häufig auf[104].

Der Begriff Metadaten wird hingegen verbreitet in Gesetzen benutzt, welche die Organisation von Verwaltung oder verwaltungsnahen Einrichtungen betreffen. Nach § 12 Abs. 3 ZensG 2011[105] stellt das Statistische Bundesamt das Metadatensystem für den Zensus bereit. In der Begründung zum Regierungsentwurf dieses Gesetzes findet sich auch eine ausführliche Umschreibung des Begriffs im dort gemeinten Sinn: „Metadaten sind alle Angaben, die den Inhalt der Daten und ihr Zustandekommen beschreiben und dadurch erst aus der statistischen Wertgröße (die nackte Zahl) eine interpretierbare Information machen. Sie enthalten beispielsweise Informationen über die Erhebungsmethode, die verwendeten Formate oder die Qualität statistischer Informationen. Metadaten fallen in allen Arbeitsschritten bei der Vorbereitung und Durchführung des Zensus an und beinhalten sowohl semantische Metadaten (Definitionen, Nomenklaturen, Klassifikationen, Methodenbeschreibungen, etc.) als auch technische Metadaten (Dateiformate, Versionsnummern, usw."[106]

Teil eines wesentlich größeren Planungs- und Regelungszusammenhangs ist das E-Government-Gesetz. Es gehört in den durch die Föderalismus-Reform geänderten Verfassungsvorschriften von Art. 91c ff.GG, die Anstoß für den „Staatsvertrag über die Errichtung des IT-Planungsrats und über die Grundlagen der Zusammenarbeit beim Einsatz der Informationstechnologie

---

[102] Telekommunikations-Überwachungsverordnung vom 3. November 2005 (BGBl. I S. 3136), die zuletzt durch Artikel 4 des Gesetzes vom 25. Dezember 2008 (BGBl. I S. 3083) geändert worden ist

[103] Ausgabe 6.3 Stand: 06. April 2016, Bearbeiter und Herausgeber: Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen Postfach 80 01, 55003 Mainz, Notifiziert gemäß der Richtlinie (EU) 2015/1535 des Europäischen Parlaments und des Rates vom 9. September 2015 über ein Informationsverfahren auf dem Gebiet der technischen Vorschriften und der Vorschriften für die Dienste der Informationsgesellschaft (ABl. L 241 vom 17.9.2015, S. 1).

[104] In der Grundsätzlichen Verfahrensbeschreibung (S. 121) in der TR TKÜV heißt es beispielsweise: „Zur Administrierung der Anfrage bei der berechtigten Stelle gehört die Eingabe aller für den warrant request notwendigen Metadaten sowie die elektronische Kopie der Anordnung. Die Metadaten enthalten die Informationen der Anordnung zu den verschiedenen Kennungen und Zeiträumen zur eigentlichen elektronischen Weiterverarbeitung."

[105] § 12 Gesetz über den registergestützten Zensus im Jahre 2011 in der Fassung vom 8.7.2009, BGBl. I 2009, 1781

[106] BT-Drs. 16/12219 S. 40

in den Verwaltungen von Bund und Ländern" waren. In § 12 Abs. 1 EGovG[107] wird der Begriff Metadaten daher ebenfalls zu Standardisierungszwecken verwendet: „Stellen Behörden über öffentlich zugängliche Netze Daten zur Verfügung, an denen ein Nutzungsinteresse, insbesondere ein Weiterverwendungsinteresse im Sinne des Informationsweiterverwendungsgesetzes, zu erwarten ist, so sind grundsätzlich maschinenlesbare Formate zu verwenden. Ein Format ist maschinenlesbar, wenn die enthaltenen Daten durch Software automatisiert ausgelesen und verarbeitet werden können. Die Daten sollen mit Metadaten versehen werden." Das E-GovernmentG befasst sich nämlich u.a. mit der Datenbereitstellung in maschinenlesbarer Form und will das Auffinden dieser Daten durch die Erschließung anhand einheitlicher und abgestimmter Metadaten erleichtern. Dazu zählen nach der Gesetzesbegründung u.a. Kontakt-Informationen, Veröffentlichungs- und Änderungsdaten, Beschreibungen, Verweise zu Nutzungsbestimmungen, geographische und zeitliche Granularitäten und Abdeckungen[108].

Verbreitet wird der Begriff Metadaten im Recht der Geodaten verwendet. Nach § 1 Abs. 2 BGeoRG[109] sollen die geodatenhaltenden Stellen des Bundes sicherstellen, dass die qualitativen und technischen Vorgaben für die von ihnen erhobenen oder erstellten geotopographischen Referenzdaten und die dazugehörigen Metadaten sowie für geodätische Referenzsysteme und -netze eingehalten werden, so dass ein einfacher Austausch und eine breite Nutzung nach Absatz 1 Satz 2 gewährleistet sind. Dem entsprechend regelt die GeoNutzVO die Voraussetzungen, unter denen Geodaten und Geodatendienste, einschließlich zugehöriger Metadaten, nach § 11 Absatz 1 und 2 des Geodatenzugangsgesetzes von den geodatenhaltenden Stellen nach § 2 Absatz 1 in Verbindung mit § 3 Absatz 8 des Geodatenzugangsgesetzes zur Verfügung gestellt werden[110]. Nach § 1 Geodatenzugangsgesetz ist es das Ziel des Gesetzes, dem Aufbau einer nationalen Geodateninfrastruktur zu dienen. Es schafft u.a. den rechtlichen Rahmen für den Zugang zu Geodaten, Geodatendiensten und Metadaten von geodatenhaltenden Stellen sowie die Nutzung dieser Daten und Dienste, insbesondere für Maßnahmen, die

---

[107] Gesetz zur Förderung der elektronischen Verwaltung (E-Government-Gesetz) vom 25.07.2013, BGBl. I 2013, 2749

[108] BT-Drs. 17/11473 S. 44. Die Gesetzesbegründung verweist auch darauf, dass im Rahmen des Modernisierungsprojektes Open Government der Bundesregierung und des Steuerungsprojektes des IT-Planungsrates „Förderung des Open Government" Empfehlungen für einheitliche Metadaten erarbeitet würden.

[109] Gesetz über die geodätischen Referenzsysteme, -netze und geotopographischen Referenzdaten des Bundes
Bundesgeoreferenzdatengesetz i.d.F. vom 10.05.2012, BGBl I 2012, 1081

[110] Vgl. § 1 Verordnung zur Festlegung der Nutzungsbestimmungen für die Bereitstellung von Geodaten des Bundes vom 19. März 2013 (BGBl. I S. 547) (GeoNutzV)

Auswirkungen auf die Umwelt haben können[111]. Ursprünglich ist das Geodatenzugangsgesetz durch die am 15 Mai 2007 in Kraft getretene Richtlinie 2007/2/EG des Europäischen Parlaments und des Rates zur Schaffung einer Geodateninfrastruktur in der Europäischen Gemeinschaft (INSPIRE-Richtlinie) veranlasst worden[112]. Spätere Änderungen haben es aber zusätzlich in den Dienst von Open-Data-Initiativen und E-Government-Aktivitäten gestellt

Die eingangs erwähnte Ausnahme findet sich im Gesetz zum Schutz vor Gefährdung der Sicherheit der Bundesrepublik Deutschland durch das Verbreiten von hochwertigen Erdfernerkundungsdaten (Satellitendatensicherheitsgesetz)[113]. Als Grund für das Gesetz wurden sicherheits- und außenpolitische Interessen der Bundesrepublik Deutschland beim Verbreiten von Erdfernerkundungsdaten angegeben, die mit Hilfe seinerzeit in Deutschland neu entwickelter leistungsfähiger Erdfernerkundungssatelliten erzeugt und vermarktet werden konnten[114]. In § 18 Abs. 1 des Gesetzes werden die Datenanbieter nicht nur verpflichtet, die Identität des Anfragenden genau zu überprüfen und festzuhalten (Nr. 2), sondern auch die Metadaten der Daten, insbesondere das Zielgebiet, den Zeitpunkt der Erzeugung der Daten, den Sensorbetriebsmodus und die Parameter der Verarbeitung der Daten aufzuzeichnen (Nr. 8). Metadaten werden in diesem Zusammenhang als die zentralen Informationen eines Datensatzes bezeichnet. Vorschaubilder bzw. Miniaturansichten und Metadaten seien ein wichtiges Hilfsmittel für den potenziellen Kunden, um vor einer Anfrage (Bestellung) einen Eindruck von Daten und deren Eignung für eine bestimmte Aufgabe beurteilen zu können[115]. Es handelt sich also um Metadaten von Bilddateien, und sie sind zu unterscheiden vom Bild selbst, also seinem Inhalt.

bb) Verwendung des Begriffs in der Rechtsprechung und Rechtswissenschaft

Verstreut finden sich Anwendungsbeispiele für den Begriff Metadaten in der obergerichtlichen Rechtsprechung. Ein Oberverwaltungsgericht hatte über einen Anspruch auf Aufnahme unbeweglicher Kulturdenkmäler in die

---

[111] § 1 Gesetz über den Zugang zu digitalen Geodaten (Geodatenzugangsgesetz) in der Fassung vom 10.2.2009, BGBl. I 2009, 278

[112] Vgl. die Begründung des Regierungsentwurfs für das Geodatenzugangsgesetzt (BT-Drs. 16/10530 S. 1 ff.)

[113] Gesetz vom 23.11.2007, BGBl. I 2007, 2590

[114] Vgl. in der Begründung des Regierungsentwurfs BT-Drs. 16/4763 S. 1

[115] BT-Drs. 16/4763 S. 28

Geobasisinformationen zu entscheiden. Dabei fand es zu der Ausführung, § 9 Abs. 1 Landesgeodateninfrastrukturgesetzes – LGDIG sehe vor, dass Metadaten, Geodaten, Geodatendienste und Netzdienste als Bestandteile der Geodateninfrastruktur über ein geeignetes elektronisches Netzwerk zu verknüpfen seien. Zudem bestimme § 11 LGDIG, dass Geodaten und Geodatendienste der Öffentlichkeit zur Verfügung stehen[116]. Der hier verwendete Begriff Metadaten gehört aber nicht zum Gebiet der Telekommunikation.

Im Urteil eines Verwaltungsgerichts zum Urheberrechtsschutz für die in einem Gericht dokumentarisch aufbereiteten Entscheidungen findet sich die Ausführung, schließlich stelle der Bearbeiter Querbezüge zu Gesetzen und in Bezug genommene Gerichtsentscheidungen durch die Eingabe, Auswahl, Einteilung und Anordnung von Metadaten zum Zweck der erfolgreichen Suchoptimierung her[117]. Hierbei geht es um Dokumentationsrecht und nicht um digitalisierte Metadaten aus der Telekommunikation.

Ein anderes Verwaltungsgericht war mit dem Anspruch eines Unternehmens befasst, das sich im IT-Bereich u.a. mit dem Aufbau und der Pflege von Datenbanken auf Zurverfügungstellung von Informationen bzw. Daten, die zum Zwecke des Aufbaus der Bundesrechtsdatenbank an juris übermittelt werden, beschäftigt. Bei zwei der Dateien handelte es sich nach den Ausführungen im Urteil um XML-Dateien. Sie unterschieden sich lediglich darin, dass die "E-Norm-Datei" im Wesentlichen nur den entsprechenden Rechtstext als Information enthielt, während die von den Dokumentaren des BfJ besonders aufbereiteten Dateien zusätzlich die für die Verwendbarkeit der Rechtstexte in einer Datenbank erforderlichen Informationen, die sog. Metadaten, enthielten[118]. In diesem Fall ging es um die Metadaten bei der Textdokumentation und nicht in der Telekommunikation.

Ein anderes verwaltungsgerichtliches Urteil betraf eine verlangte Einsicht in Unterlagen der Forschungsgruppe Rosenholz, also in Unterlagen aus dem Tätigkeitsbereich der Stasi. In dem Urteil findet sich die Aussage, dass auch personenbezogene Informationen, die im Rahmen der Aufarbeitung der Tätigkeit des Staatssicherheitsdienstes durch die BStU aus Stasi-Unterlagen exzerpiert und aufgezeichnet würden - sog. „Meta-Daten" in Tabellen, Listen, Aufsatzentwürfen, Übersichten, Zusammenstellungen etc. -, die nicht in den Anwendungsbereich des Informationsfreiheitsgesetzes fielen[119]. Insoweit ging es also um Metadaten im Dokumentationsbereich.

---

[116] Oberverwaltungsgericht Rheinland-Pfalz, Beschluss vom 09. Dezember 2016 – 8 A 10618/16 –, Rn. 14, juris

[117] VG Karlsruhe, Urteil vom 03. November 2011 – 3 K 2289/09 –, Rn. 35, juris

[118] VG Köln, Urteil vom 26. Mai 2011 – 13 K 5747/07 –, Rn. 67, juris

[119] VG Berlin, Urteil vom 08. September 2009 – 2 A 8.07 –, Rn. 26, juris

In einer anderen obergerichtlichen Entscheidung ging es um eine mögliche Rechtsverletzung durch die abgelehnte Löschung des Namens und des Aktenzeichens aus dem EDV-Programm "EUREKA-Vormundschaft" nach Abschluss eines Betreuungsverfahrens. Unabhängig von der Frage, ob die hier maßgeblichen Metadaten Sozialdaten im Sinne der §§ 35 Abs. 1 SGB-I, 67 SGB-X darstellen könnten, handelte es sich nach den Ausführungen des Oberlandesgerichts beim Amtsgericht im gegebenen Zusammenhang nicht um einen Leistungsträger im Sinne der §§ 35 Abs. 1, 12 SGB-I bzw. eine sonstige Stelle im Sinne des § 35 Abs. 1 SGB-I, auf die die genannte Vorschrift sich bezieht[120].

In einem landgerichtlichen Strafurteil ging es um gefährliche Körperverletzung und nicht unerhebliche Beeinträchtigung eines Soldaten ohne Einwilligung des Betroffenen. In dem Urteil wird u.a. ausgeführt, ein Sachverständige habe bekundet, dass die von der Kammer an das LKA übersandte asservierte CD mit den darauf gespeicherten Fotos von der Übung aus dem 2. Quartal auftragsgemäß untersucht worden sei; dabei seien die "Meta-Daten" (auch "Exif-Daten" genannt, bezeichnet nach dem bei der Speicherung verwendeten Dateiformat) jedes einzelnen Fotos sichtbar gemacht worden[121]. Es handelte sich also um digitalisierte Daten eines Bildträgers.

cc) Verwendung des Begriffs bei Regierungshandeln und in der Verwaltung

Eine große Rolle spielt die Standardisierung von Metadaten bei der Nutzung von Open Data, d.h. der Zugänglichmachung von öffentlichen Datenbeständen. Dabei geht es um die kostenfreie Bereitstellung und Verfügbarkeit von im öffentlichen Sektor anfallenden Daten für kommerzielle wie auch nichtkommerzielle Zwecke u. a. für mehr Innovation, Transparenz und Wertschöpfung[122]. Es handelt sich hierbei um einen Prozess, der eng mit Fragen der Digitalisierung verzahnt ist und auch – nach Einschätzung der Bundesregierung - mit einem Kulturwandel einhergeht[123]. Er weist Nähen zu den Digitalisierungsvorgängen in der Telekommunikation auf, ist aber selbst nicht Gegenstand von Telekommunikation und den einschlägigen gesetzlichen Regelungen. Dennoch lohnt ein Blick auf die Entwicklung dieses

---

[120] OLG Frankfurt, Beschluss vom 05. Januar 2009 – 20 VA 10/06 –, Rn. 9, juris

[121] LG Münster, Urteil vom 12. März 2008 – 8 KLs 81 Js 1837/04 (25/05) –, Rn. 291, juris

[122] BT-Drs. 18/7485 S. 2

[123] BT-Drs. 18/6027 S. 3

Teils des öffentlichen Sektors, weil er zumindest an der Entwicklung eines bestimmten Sprachgebrauchs beteiligt ist.

1994 hat das Bundesministerium für Verkehr (BMV) im Rahmen des Forschungsprogramms Stadtverkehr (FOPS) ein Projekt aufgelegt, das die technische Machbarkeit einer deutschlandweiten elektronischen Fahrplanauskunft nachweisen sollte (DELFI I). Die Gutachter kamen zu einem positiven Ergebnis, allerdings nicht ohne darauf hinzuweisen, dass aus ihrer Sicht noch vertiefende Untersuchungen notwendig werden. Die Länder waren nicht eingebunden. Das BMV legte daraufhin das Folgeprojekt DELFI II auf, diesmal allerdings unter Einbezug aller Bundesländer. DELFI III ist im Juni 2002 erfolgreich abgeschlossen worden. Es wurde nachgewiesen, dass in einer Testumgebung die verteilte Verbindungssuche funktioniert. Mit Mitteln der Anschubfinanzierung der Länder sind im Rahmen eines Testbetriebs in Echtzeit via Internet zwischen Juli 2002 und Dezember 2002 erkannte Fehlerquellen beseitigt und der Aufbau der sog. Metadatenverwaltung (gemeinsam verwendete Daten, die für das Zusammenspiel der einzelnen Systeme essentiell sind) optimiert worden[124].

Ein weiteres Verwendungsbeispiel findet sich in der Gesetzessprache. Nach § 12 Zensusgesetz 2011 i.d.F. vom 08.07.2009 stellt das Statistische Bundesamt das Metadatensystem für den Zensus bereit[125]. Auch hier gehört der Begriff nicht zum Telekommunikationsrecht.

Eine zentrale Rolle spielt der Begriff Metadaten im Zusammenhang mit Projekten zum Open Government oder E-Government. Ausgangspunkt im nationalen Rahmen ist Art. 91c Abs. 2 Satz 1 GG, wonach Bund und Länder auf Grund von Vereinbarungen die für die Kommunikation zwischen ihren informationstechnischen Systemen notwendigen Standards und Sicherheitsanforderungen festlegen können. Zur Ausführung von Art. 91c GG haben Bund und Länder Vertrag über die Errichtung des IT-Planungsrats und über die Grundlagen der Zusammenarbeit beim Einsatz der Informationstechnologie in den Verwaltungen von Bund und Ländern – Vertrag zur Ausführung von Artikel 91c GG geschlossen.

Auf der Grundlage von § 1 Absatz 1 Satz 1 Nr. 3 des IT-Staatsvertrages steuert der IT-Planungsrat die E-Government-Projekte (Steuerungsprojekte), welche ihm durch den Chef des Bundeskanzleramts und die Chefinnen und Chefs der Staats- und Senatskanzleien der Länder zugewiesen werden. Dies sind Projekte von herausragender Bedeutung für die Zusammenarbeit von Bund, Ländern und Kommunen. Der IT-Planungsrat gibt die Projektzielsetzungen vor, steuert die Umsetzung und lässt sich regelmäßig zum Projektstand berichten. Zu seinen Aufgaben gehört nach § 3 Abs. 1 des Staatsvertrags die

[124] Aus: Website von DELFI-Service im Auftrag der Bundesländer und der DB AG

[125] Zensusgesetz 2011 vom 8. Juli 2009 (BGBl. I S. 1781)

Festlegung von gemeinsamer Standards von Bund und Ländern u.a. für den Datenaustausch und die IT-Sicherheit.

Der IT-Planungsrat hatte in der 12. Sitzung am 2. Oktober 2013 die Metadatenstruktur für offene Verwaltungsdaten in die Standardisierungsagenda aufgenommen. Die Bearbeitung des Standardisierungsbedarfs wird im Rahmen des Betriebs von GovData vorangebracht. Sachstand ist danach die Empfehlung der „OGD-Metadatenstruktur Deutschland", die im Sinne eines offenen Verwaltungshandelns frei zugänglich ist. Parallel zu einer Erprobung und Diskussion insbesondere mit den Datenbereitstellern von GovData erfolgt auch ein Abgleich mit anderen internationalen Standards, z.B. im Rahmen der G8, im D-A-CH-Li[126]-Raum sowie auf europäischer Ebene[127].

Das Bundeskabinett hat am 17. September 2014 den „Nationalen Aktionsplan zur Umsetzung der Open-Data-Charta der G 8" beschlossen. Zu einem solchen Aktionsplan hatten sich die G8-Mitgliedstaaten beim Gipfel am 17./18. Juni 2013 mit Unterzeichnung der G8-Open-Data-Charta verpflichtet. In der Charta verständigten sich die G8-Staaten auf fünf grundlegende Prinzipien zur Umsetzung von Open Data, darunter das Kernprinzip, Verwaltungsdaten künftig standardmäßig offen bereitzustellen („Open Data by default"). Das BMI hat im November 2014 den Zusammenhang des Open Data Konzepts zu einem „Nationalen Aktionsplan der Bundesregierung zur Umsetzung der Open-Data-Charta der G8"[128] verbreitert und dabei die bereits laufenden Anstrengungen mit den Bundesländern im Rahmen des IT-Planungsrates einbezogen. Der Aktionsplan sieht vor, das Prinzip „Open Data als Standard" langfristig und Schritt für Schritt umzusetzen. Im Aktionsplan sind konkrete Verpflichtungen benannt, die schrittweise bis Ende 2015 zu erfüllen waren, um die Ziele der G8-Charta zu erreichen. Für die Förderung und Sichtbarkeit von Open Data in Deutschland spielt das Datenportal GovData als ebenenübergreifende technische Infrastruktur eine zentrale Rolle. Es handelt sich um einen Metadatenkatalog, auf dem Datenbeschreibungen (Metadaten) zu bereitgestellten Daten aus Bund, Ländern und Kommunen zentral verfügbar sind. Das ursprünglich von BMI initiierte und finanzierte Portal wird seit dem 1. Januar 2015 als Anwendung des IT-Planungsrates in gemeinsamer Verantwortung des Bundes und der Länder Baden-Württemberg, Berlin, Brandenburg, Hamburg, Nordrhein-Westfalen, Rheinland-Pfalz, Sachsen und Bremen betrieben und finanziert. Die Verantwortung für den Betrieb hat die gemeinsame Geschäfts- und Koordinierungsstelle GovData mit Sitz in der Finanzbehörde Hamburg

---

[126] Deutschland (D), Österreich (A), Schweiz (CH), Liechtenstein (Li)

[127] BT-Drs. 18/7485 S. 11 ff.

[128] Veröffentlichung im Internet

übernommen. Strategische Entscheidungen zu GovData trifft der ITP-Planungsrat[129].

Um die veröffentlichen Verwaltungs-Daten bestmöglich auffindbar zu machen, beabsichtigt das BMI gemeinsam mit den Ländern und Kommunen im Rahmen der Standardisierungsagenda des IT-Planungsrats an der Standardisierung der Metadatenstruktur für offene Daten zu arbeiten. Eine Aufgabe hierbei wird es sein, die semantische Interoperabilität der Datenbeschreibungen – z.B. durch einheitliche Thesauri – zu fördern und so die Qualität der Metadaten auf effiziente Art und Weise zu verbessern. Die Open-Data-Metadatenstruktur wird auf bereits existierende und anerkannten Standards aufsetzen, um unnötige Aufwände und Doppelarbeiten in der öffentlichen Verwaltung zu vermeiden[130].

Die OGD-Metadatenstruktur wird nach Auskunft von GOVDATA[131] auf GitHub[132] gepflegt. Sie ist nicht nur als Werkzeug gedacht, um valide Metadaten bestimmen zu können, sondern vielmehr als Kommunikationsmittel für Interessierte wie öffentliche Entscheider, Datenbereitsteller, Entwickler und andere Open-Data-Initiativen im deutschsprachigen Raum. Diesen Zwecken dient auch die frühzeitige Veröffentlichung im Beta-Stadium und die öffentlich nachvollziehbare Entwicklung auf GitHub. Über das Datenportal für Deutschland – GovData, über das Beteiligungsportal open-data-aktionsplan.de sowie über Social-Media-Kanäle wurden darüber hinaus regelmäßig aktuelle Themen, aber auch z. B. Leitfäden zur Datenveröffentlichung kommuniziert. Technische Grundlagen wie z. B. das Metadatenformat, aber auch der Quellcode von GovData, wurden über den Online-Dienst GitHub öffentlich zur Verfügung gestellt[133].

Die Metadatenstruktur, die sowohl die Beschreibung von Datensätzen (inkl. von Datendiensten), von Dokumenten und von Applikationen unterstützt, ist wie folgt aufgebaut: Die wichtigsten Eigenschaften werden auf oberster Ebene abgelegt. Dazu gehören: Titel, Bezeichner, Beschreibung, Verantwortliche und

---

[129] BT-Drs. 18/6027 S. 2

[130] Nationalen Aktionsplan der Bundesregierung zur Umsetzung der Open-Data-Charta der G8 S. 11

[131] GovData, das Datenportal für Deutschland, bietet einen einheitlichen, zentralen Zugang zu Verwaltungsdaten aus Bund, Ländern und Kommunen. Ziel ist es, diese Daten an einer Stelle auffindbar und so einfacher nutzbar zu machen. Im Sinne von „Open Data" ist es das Bestreben, die Verwendung offener Lizenzen zu fördern und das Angebot von maschinenlesbaren Rohdaten zu erhöhen.

[132] Dabei handelt es sich um einen webbasierten online-Dienst mit Sitz in San Francisco, der u.a. das Versionsverwaltungssystem Git entwickelt hat

[133] Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Volker Beck (Köln), Dr. Konstantin von Notz, Dieter Janecek, weiterer Abgeordneter und der Fraktion BÜNDNIS 90/DIE GRÜNEN – Drucksache 18/7327 – Chancen der Nutzung von Open Data, BT-Drs. 18/7485 S. 6

Nutzungsbestimmungen. Weiterhin essenziell ist die Liste der Ressourcen, also die eigentlichen Daten, Dokumente oder Applikationen. Wichtigste Eigenschaft jeder Ressource ist wiederum deren URL. Außerdem können je Ressource Beschreibung und Format vermerkt werden. Dieser Aufbau ermöglicht es beispielsweise, inhaltlich zusammengehörende Dateien als einen Datensatz zu erfassen, für gegebenenfalls verschiedene Zeitabschnitte, in verschiedenen Sprachen oder Formaten. Innerhalb des Bereichs "Extras" werden alle weiteren Angaben gespeichert. Dazu gehören vor allem die zeitliche und räumliche Einordnung, sowie die Angaben zur Herkunft bei importierten Einträgen.

dd) Allgemeine wissenschaftliche Verwendung des Begriffs

Stellvertretend für viele andere werden hier die im Internet veröffentlichten „DFG-Praxisregeln „Digitalisierung"" angeführt. Die Deutsche Forschungsgemeinschaft (DFG)[134] fördert im Bereich der Wissenschaftlichen Literaturversorgungs- und Informationssysteme (LIS) Projekte an wissenschaftlichen Einrichtungen, insbesondere Service- und Informationseinrichtungen in Deutschland. Förderziel ist der Aufbau leistungsfähiger Informationssysteme und -infrastrukturen für die Forschung unter überregionalen Gesichtspunkten. Die Ergebnisse der Projekte sollen für die Wissenschaft frei und dauerhaft zugänglich sein. Die Standards ergänzend finden sich in den Praxisregeln auch weiterführende Ausführungen, beispielsweise zur konservatorischen Prüfung der zur Digitalisierung vorgesehenen Materialien, zum Erheben von Metadaten, zur Herstellung der Digitalisate, zur Indexierung von Bildinhalten, zur Herstellung von Volltexten oder auch zur Perspektive der Langzeitsicherung digitaler Inhalte[135]. Die DFG-

---

[134] Die Deutsche Forschungsgemeinschaft (DFG) ist die zentrale Selbstverwaltungseinrichtung der Wissenschaft zur Förderung der Forschung an Hochschulen und öffentlich finanzierten Forschungsinstitutionen in Deutschland. Die DFG dient der Wissenschaft in allen ihren Zweigen durch die finanzielle Unterstützung von Forschungsvorhaben und durch die Förderung der Zusammenarbeit unter den Forschern (http://www.dfg.de). Die DFG unterstützt auch Vorhaben zur Verbesserung der wissenschaftlichen Informations-Infrastrukturen in Deutschland. Die Ergebnisse der geförderten Projekte sollen für die Wissenschaft frei und dauerhaft zugänglich sein (http://www.dfg.de/lis). Zu beachten ist, dass die definierten Trägeraufgaben und -finanzierungen der antragstellenden Einrichtungen durch die Förderung nicht substituiert werden dürfen. Projekte müssen daher in ihrer Profilierung über die regulären Grundaufgaben einer Einrichtung hinausgehen, zeitlich und inhaltlich begrenzt sein sowie herausragende und überregional bedeutende Materialien zum Gegenstand haben. Nicht förderfähig sind damit Vorhaben, die vorrangig der Kulturförderung, Kulturgutvermittlung oder vergleichbaren Zielsetzungen dienen, sowie kommerziell orientierte Projekte.

[135] DFG-Praxisregeln „Digitalisierung" S. 6

Praxisregeln „Digitalisierung" setzen ihrerseits bereits an anderer Stelle festgelegte Standardisierungen voraus und stützen sich auf diese[136].

ee) Verwendung des Begriffs in der medialen Umgangssprache

In Ermangelung einer verbindlichen Definition des Begriffs gibt es Definitionsangebote: „Metadaten sind nicht der tatsächliche Inhalt der Kommunikation, sondern die Daten über die Kommunikation; etwa die Nummern, die er anruft oder antextet, und wo sein Handy sich zu einem bestimmten Zeitpunkt befindet. Wem er E-Mails schreibt, die Betreffzeilen der E-Mails und die Webseiten, die er besucht."[137] Diese Begriffsbestimmung für Metadaten in der Telekommunikation erscheint sinnvoll, hat aber nur eine auf den unmittelbaren Kontext beschränkte Reichweite.

Der Gebrauch des Begriffs Metadaten kommt in der medialen Umgangssprache als Paraphrase für technische Telekommunikationsdaten vor, und wird dann mitunter unpräzise eingesetzt zur Umschreibung enger gefasster Sachverhalte. In der Besprechung einer Entscheidung des EuGH zur Vorratsdatenspeicherung[138] wird unter Benennung einer genauen Fundstelle von Metadaten gesprochen obwohl der Begriff dort nicht verwendet wird: „Diesen Daten spricht der EuGH – in Übereinstimmung mit allen in den letzten Jahren gewonnenen Erkenntnissen – eine hohe Bedeutung zu, auch wenn es sich „nur" um sog. Metadaten handelt (Rn. : 27):....". Das muss im Verwendungszusammenhang nicht als falsch bezeichnet werden, ist aber in der Wiedergabe des Urteils ungenau und möglicherweise der Verwendung eines Jargons geschuldet[139]. Der Begriff Metadaten wird in der gesamten Entscheidung des EuGH nicht verwendet.

ff) Zwischenergebnis

---

[136] „Die Erzeugung von Metadaten, welche erst die Auffindbarkeit der Objekte gewährleisten und eine kontextualisierende Präsentation ihrer digitalen Images erlauben, ist zentraler Bestandteil der Digitalisierung. Die DFG geht davon aus, dass die der Digitalisierung zu Grunde liegenden analogen Objekte bereits primär in anerkannten digitalen Nachweissystemen erschlossen sind bzw. mit der Digitalisierung einhergehend erschlossen werden." (DFG-Praxisregeln „Digitalisierung" S. 30)

[137] Aus: Netzpolitik.org Metadaten: Wie dein unschuldiges Smartphone fast dein ganzes Leben an den Geheimdienst übermittelt von Gastbeitrag am 29. Juli 2014, 17:00

[138] URTEIL DES Europäischen GERICHTSHOFS (Große Kammer) 8. April 2014 in den verbundenen Rechtssachen C-293/12 und C-594/12

[139] Aus: Offene Netze und Recht. EuGH erklärt Vorratsdatenspeicherungsrichtlinie für ungültig – kurze Analyse. Der Begriff wird in der gesamten Entscheidung des EuGH nicht verwendet.

Der Begriff „Metadaten" ist in der Rechts-, Verwaltungs- und Umgangssprache sehr verbreitet. Er hat aber keinen definierten Platz im Telekommunikations- und Telemedienrecht. Deshalb wird er auf solche Sachverhalte nicht terminologisch angewendet, sondern nur als Jargon, also in Form einer nicht standardisierten Sprachvarietät oder eines nicht standardisierten Wortschatzes, der einer beruflich, gesellschaftlich, politisch oder kulturell abgegrenzten Gruppe, einem bestimmten sozialen Milieu oder einer Subkultur („Szene") zur Verständigung dient.[140] Im Verhältnis zu dem telekommunikationsrechtlichen Begriff der „Verkehrsdaten" oder dem telemedienrechtlichen der „Nutzerdaten" wird das Wort „Metadaten" deshalb nur paraphrasierend benutzt ohne definierte Bestimmtheit. Eine Übereinstimmung liegt – soweit beobachtbar – aber darin, dass sich alle drei nicht auf Inhaltsdaten beziehen, sondern auf Inhalte umgebende technische oder formale Merkmale. Frage 1 c) des Beweisbeschlusses, nämlich wie der Begriff Verkehrsdaten und Nutzungsdaten vom Begriff der Metadaten abzugrenzen sei ist daher eindeutig zu beantworten: Telekommunikations- und telemedienrechtlich liegt bei dem Begriff Metadaten ein aliud im Vergleich mit den dort terminologisch einschlägigen Begriffen Verkehrs- und Nutzungsdaten vor, weil es sich nicht um einen definierten Begriff in diesen Rechtsgebieten handelt. Lediglich neben der Rechtssprache wird er als erklärende Umschreibung eines Sachverhalts benutzt, um Inhalte von Telekommunikation oder Telemedien von den technischen Umgebungsdaten abzugrenzen.

b) Wann ist ein Telekommunikationsdatum „personenbezogen"?

Während es im ersten Antwortabschnitt auf Beweisfrage 3 – voranstehend unter a) – darum ging, welche Arten von Verkehrsdaten bei den verschiedenen Formen digitaler Telekommunikation entstehen, geht es im vorliegenden zweiten Abschnitt – nachfolgend unter b) – darum, welche datenschutzrechtlichen Schlüsse sich aus ihrer Analyse ziehen lassen. Schutzgut des Datenschutzes sind die personenbezogenen Daten[141]. Die Beantwortung der Frage erfordert daher eine Betrachtung des grundrechtlichen Schutzes von Telekommunikationsverkehrsdaten. Dabei geht es nacheinander um (aa)) das Verhältnis von Art. 10 Abs. 1 GG und Verkehrsdaten, (bb)) das Verhältnis von Art. 10 Abs. 1 GG und Internet, (cc))

---

[140] Vgl. die Definition von „Jargon" bei Wikipedia

[141] § 1 Abs. 1 BDSG: Zweck dieses Gesetzes ist es, den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird.

das Verhältnis der Schutzbereiche von Art. 10 Abs. 1 GG und des informationellen Selbstbestimmungsrechts aus Art. 1 Abs. 1 i.V.m. Art. 2 Abs. 1 GG, (dd)) den Kernbereichsschutz, (ee)) sowie das Verhältnis der Schutzbereiche von Art. 10 Abs. 1 GG und des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (Art 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG). Denn die untersuchungsgegenständlichen Verkehrsdaten fallen bei der Telekommunikation an und werden primär aus diesem Entstehungszusammenhang heraus grundrechtlich geschützt. Ein gesonderter Blick ist schließlich auf die statischen und dynamischen IP-Adressen zu werfen (gg)); deren rechtliche Bewertung war supranational, verfassungs- und einfachrechtlich bis in die allerjüngste Zeit umstritten. Inzwischen dürften die wesentlichen Streitpunkte aber als entschieden anzusehen sein.

aa) Art. 10 Abs. 1 GG und Verkehrsdaten

Der Schutzbereich des Art 10 Abs. 1 GG umfasst nicht nur die Vertraulichkeit der Inhalte von Telekommunikation; dieses Grundrecht schützt zudem auch die Vertraulichkeit der näheren Umstände des Kommunikationsvorgangs. Dazu gehört, ob, wann und wie oft Telekommunikationsverkehr stattgefunden hat oder versucht worden ist[142]. Umfasst sind darüber hinaus auch die Datenverarbeitungsprozesse, die sich an eine Kenntnisnahme von geschützten Telekommunikationsvorgängen anschließen, und auf die Verwendung erlangter Kenntnisse[143].

Dem Schutzbereich des Art. 10 Abs. 1 GG unterfallen somit auch die TK-Verkehrsdaten. Da eine Auswertung dieser Daten tief in das Privatleben eindringende Rückschlüsse und unter Umständen detaillierte Persönlichkeits- und Bewegungsprofile ermöglicht, kann insoweit nicht ohne weiteres davon ausgegangen werden, dass der Rückgriff auf diese Daten grundsätzlich geringer wiegt als eine inhaltsbezogene Telekommunikationsüberwachung[144]. Ein Eingriff in Art. 10 Abs. 1 GG durch Erhebung von Telekommunikationsverkehrsdaten wiegt, auch wenn hierdurch nicht unmittelbar der Inhalt der Kommunikation erfasst wird, schwer[145].

---

[142] BVerfG, 27.02.2008, 1 BvR 370/07, BVerfGE 120, 274 <307>

[143] BVerfG, Urteil vom 02. März 2010 – 1 BvR 256/08 –, Rn.189 juris unter Hinweis auf BVerfG, 14.07.1999, 1 BvR 2226/94, BVerfGE 100, 313 <359 ff>

[144] BVerfG, Urteil vom 02. März 2010 – 1 BvR 256/08 –, Rn. 227, juris

[145] BVerfG, Urteil vom 20. April 2016 – 1 BvR 966/09 –, BVerfGE 141, 220-378, Rn. 249 unter Hinweis auf BVerfGE 107, 299 <318 ff.>; für die vorsorgliche Speicherung solcher Daten vgl. auch BVerfGE 125, 260 <318 ff.>

Der Schutz durch Art. 10 Abs. 1 GG gilt nicht nur dem ersten Zugriff, mit dem die öffentliche Gewalt von Telekommunikationsvorgängen und -inhalten Kenntnis nimmt. Seine Schutzwirkung erstreckt sich auch auf die Informations- und Datenverarbeitungsprozesse, die sich an die Kenntnisnahme von geschützten Kommunikationsvorgängen anschließen, und auf den Gebrauch, der von den erlangten Kenntnissen gemacht wird[146]. Ein Grundrechtseingriff ist jede Kenntnisnahme, Aufzeichnung und Verwertung von Kommunikationsdaten sowie jede Auswertung ihres Inhalts oder sonstige Verwendung durch die öffentliche Gewalt[147]. In der Erfassung von Telekommunikationsdaten, ihrer Speicherung, ihrem Abgleich mit anderen Daten, ihrer Auswertung, ihrer Selektierung zur weiteren Verwendung oder ihrer Übermittlung an Dritte liegen damit je eigene Eingriffe in das Telekommunikationsgeheimnis[148]. Folglich liegt in der Anordnung gegenüber Kommunikationsunternehmen, Telekommunikationsdaten zu erheben, zu speichern und an staatliche Stellen zu übermitteln, jeweils ein Eingriff in Art. 10 Abs. 1 GG[149].

bb) Art. 10 Abs. 1 GG und Internet

Das Internet ist ein elektronischer Verbund von Rechnernetzwerken. Es besteht damit aus informationstechnischen Systemen und kann zudem auch selbst als informationstechnisches System angesehen werden[150]. Der Schutz des Art. 10 Abs. 1 GG erfasst Telekommunikation, einerlei, welche Übermittlungsart - Kabel oder Funk, analoge oder digitale Vermittlung - und welche Ausdrucksform - Sprache, Bilder, Töne, Zeichen oder sonstige Daten - genutzt werden[151]. Der Schutzbereich des Telekommunikationsgeheimnisses erstreckt sich danach auch auf die Kommunikationsdienste des Internet[152]. Zudem sind nicht nur die Inhalte der Telekommunikation vor einer Kenntnisnahme geschützt, sondern auch ihre Umstände. Zu ihnen gehört insbesondere, ob, wann und wie oft zwischen welchen Personen oder Telekommunikationseinrichtungen Telekommunikationsverkehr stattgefunden hat oder versucht worden ist[153]. Das Telekommunikationsgeheimnis begegnet in diesem Rahmen alten sowie

---

146 BVerfGE 100, 313 <359>

147 BVerfGE 85, 386 <398>; 100, 313 <366>; 110, 33 <52 f.>

148 BVerfGE 100, 313 <366 f.>

149 BVerfG, Urteil vom 02. März 2010 – 1 BvR 256/08 –, Rn. 190, juris unter Hinweis auf BVerfGE 107, 299 <313>

150 BVerfG, Urteil vom 27. Februar 2008 – 1 BvR 370/07 –, BVerfGE 120, 274-350, Rn. 4

151 BVerfGE 106, 28 <36>; 115, 166 <182>

152 vgl. zu E-Mails BVerfGE 113, 348 <383>

153 BVerfGE 67, 157 <172>; 85, 386 <396>; 100, 313 <358>; 107, 299 <312 f.>

neuen Persönlichkeitsgefährdungen, die sich aus der gestiegenen Bedeutung der Informationstechnik für die Entfaltung des Einzelnen ergeben. Soweit eine Ermächtigung sich auf eine staatliche Maßnahme beschränkt, durch welche die Inhalte und Umstände der laufenden Telekommunikation im Rechnernetz erhoben oder darauf bezogene Daten ausgewertet werden, ist der Eingriff allein an Art. 10 Abs. 1 GG zu messen. Der Schutzbereich dieses Grundrechts ist dabei unabhängig davon betroffen, ob die Maßnahme technisch auf der Übertragungsstrecke oder am Endgerät der Telekommunikation ansetzt[154]. Dies gilt grundsätzlich auch dann, wenn das Endgerät ein vernetztes komplexes informationstechnisches System ist, dessen Einsatz zur Telekommunikation nur eine unter mehreren Nutzungsarten darstellt[155].

cc) Verhältnis der Schutzbereiche von Art. 10 Abs. 1 und des informationellen Selbstbestimmungsrechts aus Art. 1 Abs. 1 i.V.m. Art. 2 Abs. 1 GG

In seinem Anwendungsbereich enthält Art. 10 Abs. 1 GG bezogen auf den Fernmeldeverkehr eine spezielle Garantie, die die allgemeine Gewährleistung des Rechts auf informationelle Selbstbestimmung verdrängt[156]. Soweit der Eingriff in das Fernmeldegeheimnis die Erlangung personenbezogener Daten betrifft, sind aber die Maßgaben, die für Eingriffe in das Grundrecht auf informationelle Selbstbestimmung gelten, grundsätzlich auf die speziellere Garantie in Art. 10 Abs. 1 GG zu übertragen[157].

Soweit ein Eingriff in das Fernmeldegeheimnis die Erlangung personenbezogener Daten betrifft, sind die Anforderungen, die für Eingriffe in das Grundrecht auf informationelle Selbstbestimmung gelten[158], grundsätzlich auf Eingriffe in das speziellere Grundrecht aus Art. 10 Abs. 1 GG zu übertragen[159]. Zu diesen Anforderungen gehört, dass sich die Voraussetzungen und der Umfang der Beschränkungen aus dem Gesetz klar und für den Bürger erkennbar ergeben. Der Anlass, der Zweck und die Grenzen des Eingriffs in das Fernmeldegeheimnis müssen in der Ermächtigung bereichsspezifisch und präzise bestimmt sein[160].

---

[154] BVerfGE 106, 28 <37 f.>; 115, 166 <186 f.>

[155] BVerfG, Urteil vom 27. Februar 2008 – 1 BvR 370/07 –, BVerfGE 120, 274-350, Rn. 184

[156] BVerfGE 100, 313 <358>; 107, 299 <312>; 110, 33 <53>; 113, 348 <364>; 115, 166 <188 f.>

[157] BVerfG, Beschluss vom 16. Juni 2009 – 2 BvR 902/06 –, Rn. 49, juris

[158] BVerfGE 65, 1 <44 ff.>

[159] vgl. BVerfGE 110, 33 <53>; 115, 166 <189>

[160] BVerfG, Beschluss vom 16. Juni 2009 – 2 BvR 902/06 –, Rn. 60, juris unter Hinweis auf BVerfGE 100, 313 <359 f., 372>; 110, 33 <53>

dd) Kernbereichsschutz

Das grundrechtliche Schutzniveau ist noch gesteigert, wenn der Eingriff in die Telekommunikation den sog. Kernbereich betrifft, weil dann nicht nur das Verhältnis des Telekommunikationsgrundrechts zum informationellen Selbstbestimmungsrecht betroffen ist, sondern darüber hinaus zu Art. 1 Abs. 1 GG. Die nach Art. 1 Abs. 1 GG garantierte Unantastbarkeit der Menschenwürde fordert auch im Gewährleistungsbereich des Art. 10 GG Vorkehrungen zum Schutz individueller Entfaltung im Kernbereich privater Lebensgestaltung. Es kann nicht ausgeschlossen werden, dass bei der Erfassung der Kommunikationsinhalte personenbezogene Daten betroffen sind, die sich auf den Kernbereich höchstpersönlicher Lebensgestaltung beziehen. Ob eine personenbezogene Kommunikation diesem Kernbereich zuzuordnen ist, hängt davon ab, ob sie nach ihrem Inhalt höchstpersönlichen Charakters ist und in welcher Art und Intensität sie aus sich heraus die Sphäre anderer oder Belange der Gemeinschaft berührt[161]. Maßgebend sind die Besonderheiten des jeweiligen Einzelfalls[162]. Nicht zu diesem Kernbereich gehören Kommunikationsinhalte, die in unmittelbarem Bezug zu konkreten strafbaren Handlungen stehen, wie etwa Angaben über die Planung bevorstehender oder Berichte über begangene Straftaten[163]. Bestehen im konkreten Fall tatsächliche Anhaltspunkte für die Annahme, dass ein Zugriff auf gespeicherte Telekommunikation Inhalte erfasst, die zu diesem Kernbereich zählen, ist er insoweit nicht zu rechtfertigen und hat insoweit zu unterbleiben[164]. Es muss sichergestellt werden, dass Kommunikationsinhalte des höchstpersönlichen Bereichs nicht gespeichert und verwertet werden, sondern unverzüglich gelöscht werden, wenn es ausnahmsweise zu ihrer Erhebung gekommen ist[165].

Der Kernbereichsschutz spielt beim staatlichen Zugriff auf Verkehrsdaten insofern – noch – keine große Rolle, als damit noch nicht die Kenntnisnahme von Inhalten verbunden ist. Dennoch ist er bei der Gesetzgebung zur Vorratsdatenspeicherung 2015 erwogen worden. In der Gesetzesbegründung findet sich der Gedanke, ob für Berufsgeheimnisträger in § 100g Abs. 5 StPO eine Ausnahme aufgenommen werden sollte. Die Berufsgeheimnisträger in ihrer Gesamtheit schon von der Speicherung ihrer Verkehrsdaten auszunehmen, wurde aber nicht für möglich gehalten. Dazu müsste

---

[161] BVerfGE 80, 367 <374>; 109, 279 <314>; 113, 348 <391>

[162] BVerfGE 80, 367 <374>; 109, 279 <314>

[163] BVerfGE 80, 367 <375>; 109, 279 <319>; 113, 348 <391>

[164] BVerfGE 113, 348 <391 f.>

[165] BVerfG, Beschluss vom 16. Juni 2009 – 2 BvR 902/06 –, Rn. 90, juris unter Hinweis auf BVerfGE 113, 348 <392>

sämtlichen Telekommunikationsanbietern, von denen es in Deutschland ca. 1 000 gibt, mitgeteilt werden, wer Berufsgeheimnisträger im Sinne des § 53 StPO sei; diese Liste müsste dauernd aktualisiert werden. Hinzu komme, dass Berufsgeheimnisträger in vielen Fällen nicht über statische, sondern über dynamische IP-Adressen verfügten, so dass eine Liste der verwendeten Adressen gar nicht erstellt werden könnte[166].

ee) Verhältnis der Schutzbereiche von Art. 10 Abs. 1 GG und des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme (Art 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG)

Die Gewährleistung des Telekommunikationsgeheimnisses nach Art. 10 Abs. 1 GG schützt die unkörperliche Übermittlung von Informationen an individuelle Empfänger mit Hilfe des Telekommunikationsverkehrs[167], nicht aber auch die Vertraulichkeit und Integrität von informationstechnischen Systemen[168]. Der Grundrechtsschutz des Art. 10 Abs. 1 GG erstreckt sich nämlich nicht auf die nach Abschluss eines Kommunikationsvorgangs im Herrschaftsbereich eines Kommunikationsteilnehmers gespeicherten Inhalte und Umstände der Telekommunikation, soweit dieser eigene Schutzvorkehrungen gegen den heimlichen Datenzugriff treffen kann. Dann bestehen hinsichtlich solcher Daten die spezifischen Gefahren der räumlich distanzierten Kommunikation, die durch das Telekommunikationsgeheimnis abgewehrt werden sollen, nicht fort[169]. Der durch das Telekommunikationsgeheimnis bewirkte Schutz besteht ebenfalls nicht, wenn eine staatliche Stelle die Nutzung eines informationstechnischen Systems als solche überwacht oder die Speichermedien des Systems durchsucht. Hinsichtlich der Erfassung der Inhalte oder Umstände außerhalb der laufenden Telekommunikation liegt ein Eingriff in Art. 10 Abs. 1 GG selbst dann nicht vor, wenn zur Übermittlung der erhobenen Daten an die auswertende Behörde eine Telekommunikationsverbindung genutzt wird, wie dies etwa bei einem Online-Zugriff auf gespeicherte Daten der Fall ist[170]. Soweit der heimliche Zugriff auf ein informationstechnisches System dazu dient, Daten auch insoweit zu erheben, als Art. 10 Abs. 1 GG nicht vor einem Zugriff schützt, bleibt eine Schutzlücke, die durch das allgemeine

---

[166] BT-Drs. 18/5088 S. 33

[167] BVerfGE 67, 157 <172>; 106, 28 <35 f.>

[168] BVerfG, Urteil vom 27. Februar 2008 – 1 BvR 370/07 –, BVerfGE 120, 274-350, Rn. 182

[169] BVerfGE 115, 166 <183 ff.>

[170] BVerfG, Urteil vom 27. Februar 2008 – 1 BvR 370/07 –, BVerfGE 120, 274-350, Rn. 186

Persönlichkeitsrecht in seiner Ausprägung als Schutz der Vertraulichkeit und Integrität von informationstechnischen Systemen zu schließen ist[171].

ff) Reichweite von Verkehrsdaten in den individuellen Rechtskreis

In seinem Urteil zur Vorratsdatenspeicherung hat das BVerfG sich mit der Reichweite bei der Erfassung von Verkehrsdaten beschäftigt und diese für gravierend erachtet. Die Aussagekraft dieser Daten ist weitreichend. Je nach Nutzung von Telekommunikationsdiensten seitens der Betroffenen lassen sich schon aus den Daten selbst - und erst recht, wenn diese als Anknüpfungspunkte für weitere Ermittlungen dienen - tiefe Einblicke in das soziale Umfeld und die individuellen Aktivitäten eines jeden Bürgers gewinnen. Zwar werden mit einer Telekommunikationsverkehrsdatenspeicherung, wie in § 113a TKG vorgesehen, nur die Verbindungsdaten - Zeitpunkt, Dauer, beteiligte Anschlüsse sowie - bei der Mobiltelefonie - der Standort - festgehalten, nicht aber auch der Inhalt der Kommunikation. Allerdings lassen sich aus diesen Daten bei umfassender und automatisierter Auswertung bis in die Intimsphäre hineinreichende inhaltliche Rückschlüsse ziehen. Adressaten - deren Zugehörigkeit zu bestimmten Berufsgruppen, Institutionen oder Interessenverbänden oder die von ihnen angebotenen Leistungen -, Daten, Uhrzeit und Ort von Telefongesprächen erlauben, wenn sie über einen längeren Zeitraum beobachtet werden, in ihrer Kombination detaillierte Aussagen zu gesellschaftlichen oder politischen Zugehörigkeiten sowie persönlichen Vorlieben, Neigungen und Schwächen derjenigen, deren Verbindungsdaten ausgewertet werden. Einen Vertraulichkeitsschutz gibt es insoweit nicht. Je nach Nutzung der Telekommunikation und künftig in zunehmender Dichte kann eine solche Speicherung die Erstellung aussagekräftiger Persönlichkeits- und Bewegungsprofile praktisch jeden Bürgers ermöglichen. Bezogen auf Gruppen und Verbände erlauben die Daten überdies unter Umständen die Aufdeckung von internen Einflussstrukturen und Entscheidungsabläufen[172].

Ebenfalls lässt sich zum gegenwärtigen Zeitpunkt nicht feststellen, dass die Regelung im Zusammenwirken mit anderen Vorschriften darauf zielt oder hinausläuft, eine allgemein umfassende Datensammlung zur weitmöglichsten Rekonstruierbarkeit jedweder Aktivitäten der Bürger zu schaffen. Von Bedeutung sind insoweit die Geltung des das Datenschutzrecht sonst weithin durchziehenden Grundsatzes der Datensparsamkeit sowie zahlreiche Löschungspflichten, mit denen der Gesetzgeber das Entstehen vermeidbarer

---

[171] BVerfG, Urteil vom 27. Februar 2008 – 1 BvR 370/07 –, BVerfGE 120, 274-350, Rn. 187

[172] BVerfG, Urteil vom 02. März 2010 – 1 BvR 256/08 –, Rn. 211, juris

Datensammlungen grundsätzlich zu verhindern sucht. Maßgeblich für diese Beurteilung sind insoweit insbesondere etwa die §§ 11 ff. TMG, die die Diensteanbieter nach dem Telemediengesetz grundsätzlich zur Löschung von nicht für die Abrechnung erforderlichen Daten verpflichten (vgl. § 13 Abs. 4 Nr. 2, § 15 TMG) und so auch gegenüber privatwirtschaftlichen Anreizen verhindern, dass die Internetnutzung inhaltlich in allgemeinen kommerziellen Datensammlungen festgehalten wird und damit rekonstruierbar bleibt. § 113a TKG kann damit nicht als Ausdruck einer allgemeinen öffentlichen Datenvorsorge für Zwecke der Strafverfolgung und Gefahrenprävention verstanden werden, sondern bleibt trotz seiner Weite eine begrenzte Ausnahme, die den besonderen Herausforderungen der modernen Telekommunikation für die Strafverfolgung und Gefahrenabwehr Rechnung zu tragen versucht[173].

gg) Statische und dynamische Ip-Adressen

Alle im Internet dezentral verbundenen Rechner müssen untereinander identifizierbar sein, damit die Daten verlässlich zwischen ihnen fließen können. Hierzu wird das Internet-Protokoll (IP) verwendet, das gemeinsam mit dem Transmission Control Protocol (TCP) die Datenübertragung zwischen den Rechnern koordiniert. Dabei wird jedem Rechner eine einmalige Zahlenfolge (IP-Adresse) zugeteilt, die ihn zwischen den anderen Rechnern unverwechselbar macht. Fragt ein Rechner eine bestimmte Information ab, gibt er hierfür seine eigene IP-Adresse und die des Zielrechners an, damit in die Übermittlung eingebundene Rechner wissen, wie sie den Datenstrom weiterzuleiten haben[174].

Als Rechtsgrundlage für eine Speicherung der IP-Adressen kommen sowohl die Vorschriften des Telekommunikations- als auch des Telemediengesetzes in Betracht. Im Telekommunikationsrecht ist maßgeblich die Ermächtigung für die Speicherung von Verkehrsdaten in § 96 TKG. Soweit die Speicherung der IP-Adresse allein für die Herstellung einer verschlüsselten Verbindung unter Nutzung fremder Telekommunikationsdienst erforderlich wäre, kommen als Rechtsgrundlage §§ 14, 15 TMG in Betracht[175].

Während § 6 Abs. 1 Nr. 1 TDSV noch auf die Nummer des anrufenden bzw. angerufenen Anschlusses abstellte, bezieht sich § 96 Abs 1 Nr. 1 TKG nur noch auf die Nummer i.S.d. § 3 Nr. 13 TKG der beteiligten Anschlüsse oder Endeinrichtungen. Hierdurch fallen auch IP-Adressen unter den Begriff der

---

[173] BVerfG, Urteil vom 02. März 2010 – 1 BvR 256/08 –, Rn. 270, juris

[174] Graulich in Arndt/Fetzer/Scherer/Graulich, TKG 2. Aufl. § 88 Rn. 36

[175] BVerfG, Nichtannahmebeschluss vom 13. November 2010 – 2 BvR 1124/10 –, Rn. 21, juris

Verkehrsdaten, soweit sie zum Aufbau, zur Aufrechterhaltung der Telekommunikation oder zur Entgeltabrechnung notwendig sind. Erfasst werden damit insbesondere die IP-Adressen bei VoIP-Verbindungen. Während die Erhebung von IP-Adressen schon deshalb grundsätzlich erforderlich ist, weil sie für die Aufrechterhaltung einer Internetverbindung benötigt werden, ist im Hinblick auf deren weitere Verwendung, insbesondere die Zulässigkeit der Speicherung von IP-Adressen von VoIP-Adressen, zu differenzieren[176].

c) Wer kann die Personenbeziehbarkeit leisten?

Nach § 96 Abs. 2 TKG dürfen Verkehrsdaten über das Ende der Verbindung hinaus nur verwendet werden, wenn dies zum Aufbau weiterer Verbindungen oder für die in §§ 97, 99, 100 und 101 TKG genannten Zwecke - Abrechnungszwecke, Störungsbeseitigung und Missbrauchsbekämpfung - erforderlich ist; im Übrigen sind sie nach Beendigung der Verbindung unverzüglich zu löschen. Die §§ 113a, 113b TKG, nach denen Telekommunikationsdienste zur Speicherung von Verkehrsdaten über einen Zeitraum von sechs Monaten verpflichtet waren, hat das Bundesverfassungsgericht mit Urteil vom 2. März 2010[177] für nichtig erklärt; allerdings hat die Neuregelung der Vorratsdatenspeicherung im Jahr 2015 in abgeschwächter Form die Speicherung erneut ermöglicht. Nach der höchstrichterlichen Rechtsprechung kann jedoch auch die Speicherung von dynamischen IP-Adressen zur Missbrauchsbekämpfung gem. § 100 Abs. 1 TKG für eine Dauer von sieben Tagen zulässig sein, z.B. um sog. Denial-of-Service Angriffen oder dem Versenden von Spam-Mails und damit der Abwehr von Störungen entgegen zu wirken[178]. Diese Einschätzung wurde unionsrechtlich durch die untenstehende Antwort auf die – allerdings nicht auf der Grundlage des TKG, sondern des TMG gestellten - Vorlagefrage des BGH an den EuGH bekräftigt.

Soweit die Speicherung der IP-Adresse allein für die Herstellung einer verschlüsselten Verbindung unter Nutzung fremder Telekommunikationsdienste erforderlich wäre, kommen als Rechtsgrundlage §§ 14, 15 TMG in Betracht[179]. In seinem Urteil vom 19. Oktober 2016 hat der EuGH auf eine Vorlage des BGH zwei wichtige Fragen zur Rechtsnatur und zur Handhabung von dynamischen IP-Adressen beantwortet.

---

[176] Einzelheiten bei Lutz in Arndt/Fetzer/Scherer/Graulich, TKG 2. Aufl., § 96 Rn. 6

[177] BVerfG, Urteil vom 02. März 2010 – 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08 -, juris

[178] BGH, v. 13.01.2011, Az: III ZR 146/10, MMR 2011, 341

[179] BVerfG, Nichtannahmebeschluss vom 13. November 2010 – 2 BvR 1124/10 –, Rn. 21, juris

Die erste Frage betraf die grundrechtliche Natur dynamischer IP-Adressen. Nach dem Urteil des EuGH ist Art. 2 Buchst. a der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr[180] dahin auszulegen, dass eine dynamische Internetprotokoll-Adresse, die von einem Anbieter von Online-Mediendiensten beim Zugriff einer Person auf eine Website, die dieser Anbieter allgemein zugänglich macht, gespeichert wird, für den Anbieter ein personenbezogenes Datum im Sinne der genannten Bestimmung darstellt, wenn er über rechtliche Mittel verfügt, die es ihm erlauben, die betreffende Person anhand der Zusatzinformationen, über die der Internetzugangsanbieter dieser Person verfügt, bestimmen zu lassen[181]. Damit wird ein langewährender rechtlicher Streit höchstrichterlich abgeschlossen.

Die Antwort auf die zweite Frage bestätigte den BGH in seinem Rechtsstandpunkt, dass der Zugriff auf eine dynamische IP-Adresse zur Abwehr von Angriffen möglich sein müsse. Art. 7 Buchst. f der Richtlinie 95/46[182] ist nach Ansicht des EuGH nämlich dahin auszulegen, dass er einer Regelung eines Mitgliedstaats entgegensteht, nach der ein Anbieter von Online-Mediendiensten personenbezogene Daten eines Nutzers dieser Dienste ohne dessen Einwilligung nur erheben und verwenden darf, soweit ihre Erhebung und ihre Verwendung erforderlich sind, um die konkrete Inanspruchnahme der Dienste durch den betreffenden Nutzer zu ermöglichen und abzurechnen, ohne dass der Zweck, die generelle Funktionsfähigkeit der Dienste zu gewährleisten, die Verwendung der Daten über das Ende eines Nutzungsvorgangs hinaus rechtfertigen kann[183].

Als Folge der Digitalisierung hinterlässt vor allem jede Nutzung der Telekommunikation personenbezogene Spuren, die gespeichert und ausgewertet werden können. Auch der Zugriff auf diese Daten fällt in den Schutzbereich des Art. 10 GG; das Grundrecht schützt auch die Vertraulichkeit der näheren Umstände des Kommunikationsvorgangs[184]. Dazu gehört insbesondere, ob, wann und wie oft zwischen welchen Personen oder Endeinrichtungen Telekommunikationsverkehr stattgefunden hat oder versucht worden ist. Andernfalls wäre der grundrechtliche Schutz unvollständig; denn die Verbindungsdaten haben einen eigenen

---

[180] ABl. 1995, L 281, S. 31

[181] EuGH, Urteil vom 19. Oktober 2016 – C-582/14 –, juris Rn. 49

[182] Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (ABl. 1995, L 281, S. 31)

[183] EuGH, Urteil vom 19. Oktober 2016 – C-582/14 –, juris Rn. 62 ff.

[184] BVerfGE 67, 157 <172>; 85, 386 <396>; 110, 33 <53>; Urteil des Ersten Senats des Bundesverfassungsgerichts vom 27. Juli 2005 - 1 BvR 668/04 -, NJW 2005, S. 2603 <2604>

Aussagegehalt. Sie können im Einzelfall erhebliche Rückschlüsse auf das Kommunikations- und Bewegungsverhalten zulassen. Häufigkeit, Dauer und Zeitpunkt von Kommunikationsverbindungen geben Hinweise auf Art und Intensität von Beziehungen und ermöglichen auf den Inhalt bezogene Schlussfolgerungen[185]. Die nach Abschluss des Übertragungsvorgangs im Herrschaftsbereich des Kommunikationsteilnehmers gespeicherten Kommunikationsverbindungsdaten werden jedoch nicht durch Art. 10 Abs. 1 GG, sondern durch das Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG) und gegebenenfalls durch Art. 13 Abs. 1 GG geschützt[186].

Personenbeziehbare Daten im Zusammenhang mit der Telekommunikation sind Gegenstand des Datenschutzrechts, unabhängig davon, ob BDSG, TKG oder TMG auf einen konkreten Sachverhalt Anwendung finden. Dabei sind – abhängig vom Verhältnis zum Telekommunikationsvorgang – die Schutzbereiche des informationellen Selbstbestimmungsrechts sowie des Fernmeldegeheimnisses zu unterscheiden. Personenbezogene Daten sind nach § 3 Abs. 1 BDSG Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener). Im Internetrecht gehören dazu beispielsweise Name, Anschrift, E-Mail-Adresse, IP-Adresse, Vorlieben, Beziehungen zu Dritten usw. Nicht vom Datenschutzrecht erfasst werden hingegen anonymisierte Daten, die keinerlei Bezug zu einer bestimmten oder zumindest bestimmbaren Person aufweisen. Rein statistische Auswertungen müssen sich damit nicht an den datenschutzrechtlichen Vorschriften messen lassen[187].

Das Grundrecht auf informationelle Selbstbestimmung hat - bezogen auf Kommunikationsdaten - im Recht des Datenschutzes der §§ 91 ff. TKG seine einfachgesetzliche Ausprägung gefunden, die die Erhebung und Verwendung personenbezogener Daten im Bereich der Telekommunikation regeln[188]. Personenbezogene Daten im Sinne des § 3 Abs. 1 BDSG sind unter anderem die IP-Adressen, weil der Access-Provider einen Bezug zwischen den IP-Adressen und der Person des Nutzers herstellen kann[189].

Für den Bereich der Telekommunikation werden durch § 91 Abs. 1 Satz 2 TKG auch solche Daten geschützt, die sich auf juristische Personen beziehen[190]. Für

---

[185] BVerfG, Urteil vom 02. März 2006 – 2 BvR 2099/04 –, BVerfGE 115, 166-204, Rn. 72 unter Hinweis auf BVerfGE 107, 299 <320>

[186] BVerfG, Urteil vom 02. März 2006 – 2 BvR 2099/04 –, BVerfGE 115, 166-204, Rn. 73

[187] Köhler/Arndt/Fetzer, Recht des Internet, 5. Aufl., S. 297

[188] Durner, ZUM 2010, 833, 843

[189] BGH, Urteil vom 26. November 2015 – I ZR 3/14 –, Rn. 64, juris unter Hinweis auf EuGH, GRUR 2012, 265 Rn. 51 - Scarlet/SABAM; Braun in Geppert/Schütz, Beckscher TKG-Komm., 3. Aufl., § 91 Rn. 16; Kropp aaO S. 164

[190] § 91 Abs. 1 Satz 2 TKG: „Dem Fernmeldegeheimnis unterliegende Einzelangaben über Verhältnisse einer bestimmten oder bestimmbaren juristischen Person oder

das TKG gilt dies allerdings nur soweit, als die Daten dem Fernmeldegeheimnis nach § 88 Abs. 1 TKG unterfallen[191].

Im TMG liegen die tatsächlichen und rechtlichen Verhältnisse etwas anders als im TKG. Die Erhebung von Nutzungsdaten, die – anders als bei der Telekommunikationsüberwachung – nicht im Rahmen des eigentlichen Übertragungsvorgangs stattfindet, ist ein Eingriff in das Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG). Der Nutzer eines Telemediendienstes und der Diensteanbieter stehen zueinander im Verhältnis von Kommunikationspartnern. Soweit die Nutzungsdaten daher nach Abschluss der dem Telemediendienst zu Grunde liegenden Telekommunikation beim Diensteanbieter gespeichert werden, sind sie nicht vom Schutzbereich des Art. 10 GG umfasst[192], sondern unterfallen weiterhin dem Schutz durch das informationelle Selbstbestimmungsrecht.

Ein Eingriff in Art. 10 GG liegt hingegen bei der Erhebung von Nutzungsdaten nicht vor. Das Fernmeldegeheimnis nach Art. 10 GG schützt den durch Netzbetreiber vermittelten Fernmeldeverkehr und umfasst sowohl den Inhalt als auch die Umstände desselben. Das Fernmeldegeheimnis bezieht sich nur auf den eigentlichen Übertragungsvorgang. Der Schutzbereich wird durch den Herrschaftsbereich des Betreibers des Fernmeldenetzes umgrenzt. Der Grundrechtsschutz des Art. 10 GG endet daher am Endgerät des Telekommunikationsunternehmers und gilt nicht im Verhältnis der Kommunikationspartner zueinander[193].

aa) Begriff und Personenbeziehbarkeit von Verkehrsdaten (Metadaten)

Nach Beweisfrage (3) (c) (aa) soll zunächst aus technischer sowie aus juristischer Sicht der Begriff Metadaten geklärt werden. Dazu soll insbesondere geklärt werden, welche ggfs. feststehenden Indikatoren eine Einordnung eines einzelnen Datums als „personenbezogen" zulassen und inwiefern, unabhängig von einzelnen Datensätzen, Personenbezüge in der Zusammenschau verschiedener, für sich betrachtet nicht personenbezogener Einzeldaten möglich sind. Wegen des Begriffs Metadaten wird auf die obenstehenden Ausführungen unter 1. c) verwiesen. Danach handelt es sich

---

Personengesellschaft, sofern sie mit der Fähigkeit ausgestattet ist, Rechte zu erwerben oder Verbindlichkeiten einzugehen, stehen den personenbezogenen Daten gleich."

[191] Köhler/Arndt/Fetzer, Recht des Internet, 5. Aufl., S. 298

[192][192] BT-Drs. 16/3078 S. 18

[193] BT-Drs. 16/3078 S. 18

nicht um einen Begriff des Telekommunikations- und Telemedienrechts. Diesem Ergebnis folgend wird vorliegend deshalb stattdessen mit dem gesetzlich und rechtlich definierten Begriff Verkehrsdaten gearbeitet.

Bei den Verkehrsdaten handelt es sich um personenbezogene Daten, die einen erheblichen Aussagegehalt besitzen können und deshalb des Schutzes durch das Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG) bedürfen[194]. Telekommunikation hat mit der Nutzung digitaler Übertragungsgeräte an Flüchtigkeit verloren und hinterlässt beständige Spuren. Durch die Digitalisierung fallen nicht nur bei den Diensteanbietern, sondern auch in den Endgeräten der Nutzer ohne deren Zutun vielfältige Verbindungsdaten an, die über die beteiligten Kommunikationsanschlüsse, die Zeit und die Dauer der Nachrichtenübertragung sowie teilweise auch über den Standort der Teilnehmer Auskunft geben und regelmäßig über den jeweiligen Kommunikationsvorgang hinaus gespeichert werden. Die Menge und der Aussagegehalt anfallender Verbindungsdaten lassen ein immer klareres Bild von den Kommunikationsteilnehmern entstehen. Auf Grund der Konvergenzen der Übertragungswege, Dienste und Endgeräte kommt es in der Telekommunikation in zunehmendem Maße zu einer Komprimierung des Informationsflusses. Die Endgeräte, vor allem Mobiltelefon und Personalcomputer, dienen nicht nur dem persönlichen Austausch, sondern zunehmend auch der Abwicklung von Alltagsgeschäften, wie dem Einkaufen oder dem Bezahlen von Rechnungen, der Beschaffung und Verbreitung von Informationen und der Inanspruchnahme vielfältiger Dienste. Immer mehr Lebensbereiche werden von modernen Kommunikationsmitteln gestaltet. Damit erhöht sich nicht nur die Menge der anfallenden Verbindungsdaten, sondern auch deren Aussagegehalt. Sie lassen in zunehmendem Maße Rückschlüsse auf Art und Intensität von Beziehungen, auf Interessen, Gewohnheiten und Neigungen und nicht zuletzt auch auf den jeweiligen Kommunikationsinhalt zu und vermitteln - je nach Art und Umfang der angefallenen Daten - Erkenntnisse, die an die Qualität eines Persönlichkeitsprofils heranreichen können[195].

bb) Wer kann die Personenbeziehbarkeit und ggf. mit welchen Schritten leisten?

---

[194] BVerfG, Urteil vom 02. März 2006 – 2 BvR 2099/04 –, BVerfGE 115, 166-204, Rn. 92

[195] BVerfG, Urteil vom 02. März 2006 – 2 BvR 2099/04 –, BVerfGE 115, 166-204, Rn. 93

In einem zweiten Schritt sind – gemäß Beweisfrage 3. c) - die Personenbeziehbarkeit und die Aussagekraft von Metadaten aus technischer und juristischer Sicht zu bewerten. 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"? Entsprechend der Aufteilung in ein rechtliches und ein technisches Gutachten wird die Frage vorliegend nur rechtlich verstanden. Dabei wird der Begriff Metadaten aus den bereits ausgeführten Gründen[196] nicht verwendet, sondern der Bedeutung nach konzentriert auf die Verkehrsdaten.

Die Personenbeziehbarkeit von Verkehrsdaten entsteht unter zwei verschiedenen rechtlichen Blickwinkeln. Zum einen stellt jeder Zugriff auf Verkehrsdaten einen Personenbezug her, weil die Daten – ungeachtet ihres informationssprachlichen Ausdrucks – selbst als personenbezogene Daten angesehen werden. Dies ist gefestigte Rechtsprechung des Bundesverfassungsgerichts[197]: Die Verbindungsdaten bzw. Verkehrsdaten der Telekommunikation werden automatisch festgehalten und sind insofern ein technisches Nebenprodukt, das unabhängig von der Art der Kommunikationsinhalte anfällt; gleichwohl lassen die Verbindungsdaten erhebliche Rückschlüsse auf das Kommunikations- und Bewegungsverhalten zu, deren Genauigkeit von der Zahl und Vielfalt der erzeugten Datensätze abhängt. Aus der Gesamtheit der Kommunikationsdaten, die für die Anschlussnummer einer Person gespeichert sind, lassen sich insbesondere Informationen über das soziale Umfeld gewinnen. Deshalb sieht das Bundesverfassungsgericht in seiner Rechtsprechung die Verkehrsdaten selbst bereits als personenbezogene Daten an[198]. Insoweit entsteht die Personenbeziehbarkeit beispielsweise durch den Zugriff auf Verkehrsdaten im Strafverfahren, bei der Gefahrenabwehr oder der nachrichtendienstlichen Aufklärung wie dies oben dargestellt worden ist[199].

Die Personenbeziehbarkeit von Verkehrsdaten entsteht aber zum anderen dadurch, dass diese Daten Ausgangspunkt für die Bestandsdatenauskunft im Telekommunikations- Telemedienrecht sind. Nach § 111 Abs. 1 Satz 1 TKG hat, wer geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt und dabei Rufnummern oder andere Anschlusskennungen vergibt oder Telekommunikationsanschlüsse für von anderen vergebene

---

[196] Vgl. oben II. 1. c) ff)

[197] BVerfG, Urteil vom 02. März 2006 – 2 BvR 2099/04 –, BVerfGE 115, 166-204, Rn. 92

[198] BVerfG, Urteil vom 12. März 2003 – 1 BvR 330/96 –, Rn. 74, juris

[199] II. 1. a) bb), cc) und dd) unter Anführung der Normbeispiele in § 100g StPO, § 20m BKAG und § 8a Abs. 2 Nr. 4 BVerfSchG

Rufnummern oder andere Anschlusskennungen bereitstellt, hat für die Auskunftsverfahren nach den §§ 112 und 113 TKG (Nr. 1.) die Rufnummern und anderen Anschlusskennungen, (Nr. 2.) den Namen und die Anschrift des Anschlussinhabers, (Nr. 3.) bei natürlichen Personen deren Geburtsdatum, (Nr. 4.) bei Festnetzanschlüssen auch die Anschrift des Anschlusses, (Nr. 5.) in Fällen, in denen neben einem Mobilfunkanschluss auch ein Mobilfunkendgerät überlassen wird, die Gerätenummer dieses Gerätes sowie (Nr. 6.) das Datum des Vertragsbeginns vor der Freischaltung zu erheben und unverzüglich zu speichern, auch soweit diese Daten für betriebliche Zwecke nicht erforderlich sind. Durch das Vorhalten dieser Daten wird das informationelle Selbstbestimmungsrecht ein weiteres Mal berührt. Denn die Gewährleistung des Grundrechts auf informationelle Selbstbestimmung (Art 2 Abs. 1 GG i.V.m. Art 1 Abs. 1 GG) ist insbesondere dann betroffen, wenn personenbezogene Informationen von staatlichen Behörden in einer Art und Weise genutzt und verknüpft werden, die Betroffene weder überschauen noch beherrschen können[200]. Der Schutzumfang beschränkt sich dabei nicht auf Informationen, die bereits ihrer Art nach sensibel sind. Geschützt sind insbesondere auch personenbezogene Informationen zu den Modalitäten der Bereitstellung von Telekommunikationsdiensten[201]. Von § 111 TKG nicht umfasst sind zwar Regelungen, die auf die übermittelten Inhalte oder die Art der Nutzung der Telekommunikation gerichtet sind und etwa eine Telekommunikationsüberwachung zum Zwecke der Erlangung von Informationen für Aufgaben der Strafverfolgung oder der Gefahrenabwehr vorsehen. Solche Regelungen sind im Hinblick auf die Gesetzgebungskompetenz jeweils dem Rechtsbereich zuzuordnen, für dessen Zwecke die Überwachung erfolgt[202]. Solche Regelungen hat der Bundesgesetzgeber beispielsweise in §§ 112, 113, 113a TKG i.V.m. § 100g StPO, § 20m BKAG und § 8a Abs. 2 Nr. 4 BVerfSchG erlassen. Die Vorhaltung von Kundendaten in § 111 TKG zum jederzeitigen (Bestandsdaten-)Abruf aufgrund der vorgenannten Eingriffsbefugnisse berührt daher das informationelle Selbstbestimmungsrecht zusätzlich unter dem zweiten rechtlichen Blickwinkel.

d) Welche juristischen Aussagen und Bewertungen können anhand einzelner Daten getroffen werden?

---

[200] BVerfG, 13.06.2007, 1 BvR 1550/03, BVerfGE 118, 168 <184>

[201] BVerfG, Beschluss vom 24. Januar 2012 – 1 BvR 1299/05 –, BVerfGE 130, 151-212, Rn. 122 ff.

[202] Graulich in Arndt/Fetzer/Scherer/Graulich, TKG 2. Aufl., § 111 Rn. 6

Die Erhebung von Verkehrs- (§ 96 TKG) und Nutzungsdaten (§ 15 TMG) lässt Schlüsse darauf zu, mit welchen anderen Teilnehmern ein Betroffener kommuniziert bzw. welche Telemediendienste er nutzt. Dieses Verhalten kann zusätzlich nach Zeit und Ort spezifiziert werden. Wenn die Daten über einen längeren Zeitraum erhoben werde, lassen sich daraus Nutzerprofile erstellen. Von diesen Daten ausgehend können außerdem die personengenauen Bestandsdaten des Betroffenen beim Telefondienstleister (§§ 111 i.V.m. 112 ff. TKG) bzw. beim Anbieter eines Telemediendienstes (§ 14 TMG) abgefragt werden. Dazu bedarf es jeweils einer ergänzenden Befugnis in den Sicherheitsgesetzen oder beispielsweise im Wettbewerbsrecht.

(Dr. Kurt Graulich)

Berlin, d. 28. Februar 2017