Studium und Praxis

Datenschutzrecht

Grundlagen und europarechtliche Neugestaltung

Bearbeitet von
Von PD Dr. Giselher Rüpke, M.C.L., Rechtsanwalt, Prof. Dr. Kai Lewinski, und Dr. Jens Eckhardt, Rechtsanwalt

1. Auflage 2018. Buch. Rund 454 S. Kartoniert
ISBN 978 3 406 50199 9
Format (B x L): 16,0 x 24,0 cm

oberfläche[45] wie auch über aufstehende Gebäude (Google Street View)[46] haben die Besonderheit, dass sie praktisch ausnahmslos in Kombination mit Flurkarten, Grundbüchern sowie Telefon- und Adressbüchern mit jeweiligen Personen als Grundstückseigentümer, Pächter oder Mieter in Verbindung gebracht werden können. Von hier aus zeichnet sich die Möglichkeit ab, jedwede verfügbaren Informationen als (mehrfach-)personenbezogene anzusehen.[47]

Eine Luftaufnahme vom Hühnerstall eines vermutlichen Kleinbauern ist als solche nicht als personenbezogene Information zu behandeln. Dasselbe gilt für eine Information über das Baujahr einer Gerätschaft, vorfindlich in einem Labor in einem Vorort von Wien, in Bezug auf den unbenannten Inhaber der Einrichtung. Dritte dürfen sich z. B. Kenntnis über das Alter vorhandener Gerätschaften verschaffen und sich per E-Mail darüber austauschen, ohne sich hierfür auf ein berechtigtes Interesse im Sinne des Art. 6 Abs. 1 lit. f DS-GVO (bzw. § 28 Abs. 1 Nr. 2 BDSG-alt) stützen zu müssen. **18**

Voraussetzung für datenschutzrechtliche Relevanz ist, wie für Drittkonstellationen bereits dargestellt wurde,[48] ein ***materieller* Personen*bezug***, hier also **zum** in Rede stehenden **Sachverhalt**. So, wie die Vermögenslage des Geschäftspartners nicht per se eine eigene personenbezogene Information darstellt, so gilt das analog auch für die Eigenschaften im eigenen Umfeld vorfindlicher Sachen. Zur Veranschaulichung hat die Art. 29-Gruppe folgendes Beispiel gebildet: **19**

„Der **Wert einer Immobilie** ist eine Information über einen Gegenstand. Hier finden Datenschutzbestimmungen eindeutig keine Anwendung, wenn die Information ausschließlich dazu verwendet wird, die Immobilienpreise in einem bestimmten Wohngebiet zu veranschaulichen. Unter bestimmten Umständen ist jedoch auch diese Information der Kategorie ‚personenbezogene Daten' zuzurechnen. Die Immobilie ist nämlich ein Vermögenswert, der unter anderem zur Festsetzung der vom Eigentümer zu entrichtenden Steuern herangezogen wird. In diesem Kontext ist die Personenbezogenheit dieser Information nicht zu bestreiten."[49] **20**

Demzufolge ist auf den Kontext – auf den tatsächlichen oder vorgesehenen **Verwendungszusammenhang** abzustellen. Damit wird die Qualifizierung der Information als personenbezogen nicht subjektivem Belieben anheimgegeben. Maßgebliches ergibt sich regelmäßig aus dem Geschäftsmodell, in dem die Informationen zur Verwendung gelangen.[50] Hierin zeigt sich erneut die Parallelität zur Bedeutung der geschäftlichen/behördlichen Intentionen – z. B. einer Auskunftei oder eines Nachrichtendienstes – in Bezug auf (dritt)betroffene Personen.[51] **21**

Personenbezug liegt immer dann vor, wenn Sachdaten zu gemeinsamer Verwendung mit Identifikationsdaten einer Person in geeigneter Weise verknüpft sind[52] **22**

[45] Zur angewandten Technik *Weichert*, Geodaten – datenschutzrechtliche Erfahrungen, Erwartungen und Empfehlungen, DuD 2009, 347 ff.

[46] Hierzu *Spiecker gen. Döhmann*, Datenschutzrechtliche Fragen und Antworten in Bezug auf Panorama-Abbildungen im Internet – Google Steet View und die Aussichten, CR 2010, 311 ff.; Simitis/*Ehmann*, BDSG § 29 Rn. 99 m. w. Nachw.

[47] Zur Gefahr, dass das Datenschutzrecht so insgesamt nicht mehr handhabbar wäre, Simitis/*Dammann*, BDSG § 3 Rn. 57 ff.

[48] → Rn. 11; beachte hierzu die kritische Analyse bei *Haase*, Datenschutzrechtliche Fragen, S. 240 ff.

[49] Art. 29-Gruppe in: Simitis u. a., WP 136, Abschn. III 2, Beispiel 5; vgl. auch Gola/Schomerus/*Gola/Körffer/Klug*, BDSG § 3 Rn. 4 zu Angaben in einem Stadtführer.

[50] Übereinstimmend Simitis/*Dammann*, BDSG § 3 Rn. 59; *Forgó/Krügel*, Der Personenbezug von Geodaten – Cui bono, wenn alles bestimmbar ist?, MMR 2010, 17 (21 ff.); a. A. *Weichert*, DuD 2009, 347 (351); auch *Karg*, Die Rechtsfigur des personenbezogenen Datums – Ein Anachronismus des Datenschutzes?, ZD 2012, 255 (256 f.).

[51] → Rn. 15.

[52] Vgl. BVerfG, Urt. v. 24.11.2010 – 1 BvF 2/05, BVerfGE 128, 1 (42 ff.) zum Standortregister für technisch veränderte Organismen nach § 16a GenTG.

oder wenn eine solche Verknüpfung intendiert ist.[53] So ist die Standortüberwachung von Taxis geeignet, das Verhalten der beteiligten Taxifahrer zu überwachen, und beinhaltet von daher auf diese Personen bezogene Informationen.[54]

D. Identifizierte oder identifizierbare Betroffene

I. Die Einzelnen im Fokus

23 Neben die sachlich-inhaltliche Dimension des Personenbezugs tritt dessen formal-selektive **(sigmatische) Funktion**.[55] Als betroffen ist eine Person nur anzusehen, wenn die jeweilige Information einer identifizierten (bestimmten) oder zumindest identifizierbaren (bestimmbaren) Person gilt. Deshalb scheiden allgemeine Aussagen aus, z. B. über die Hilfsbereitschaft von Menschen, über deren Lebenserwartung oder über ein gegenwärtiges Erdbeben im Raum von Lissabon, obwohl solche Feststellungen durchaus Belangvolles für das Leben von Personen beinhalten. Insofern ziehen auch Meinungs- und Informationsfreiheit denkbarem Datenschutz deutlich Grenzen.[56]

24 Allerdings können umgekehrt bei statistischen Erkenntnissen – die auf der Aggregation von bei je Einzelnen erhobenen Informationen beruhen – Zweifel daran aufkommen, ob sie keinen Personenbezug aufweisen. Unkompliziert ist dazu das Beispiel sogenannter Ausreißer. Aus einer Darstellung der Ergebnisse einer Umfrage in einer Gemeinde mit 2000 Einwohnern nach deren parteipolitischen Präferenzen, aufgegliedert nach dem jeweiligen Lebensalter der Befragten, ist die Aussage des einzigen dort lebenden 91-Jährigen diesem leicht zuzuordnen.[57] **Höhere Aggregation** der Altersgruppen, – z. B. nach Jahrzehnten – bietet da Hilfe zur Aufhebung oder zumindest Erschwerung der Bestimmbarkeit des Betroffenen.[58]

25 Die datenschutzrechtliche Literatur hat von Anfang an die Frage beschäftigt, wieweit im Hinblick auf mathematische Analysetechniken („Schnüffeltechniken") zur Reidentifikation auf der Basis statistischen Datenmaterials von der *Bestimmbarkeit* Einzelner auszugehen sei. Der Gesetzgeber hat diesbezüglich durch die im Jahre 1990 eingefügte Definition des Anonymisierens eine Klarstellung bewirkt. Für den Ausschluss des Personenbezugs kommt es nicht darauf an, dass auch „nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft" die Identifizierung herbeigeführt werden könnte, § 3 Abs. 6 [früher Abs. 7] BDSG-alt. Ausschlaggebend ist danach die **faktische Anonymität**.[59]

II. Die Bedeutung des informationellen Umfelds

26 Das „Rätsel" der Identifizierbarkeit begegnet uns nicht nur bei zusammengefassten Informationen. Zur Veranschaulichung diene ein schlichtes Beispiel: Die Mittei-

[53] Vgl. *Forgó/Krügel*, MMR 2010, 17 (21 ff.).

[54] Beispiel Nr. 8 aus Stellungnahme 4/2007 der Art. 29-Gruppe, Working Paper (WP) 136, Abschn. III 2.

[55] Zur Terminologie Simitis/*Dammann,* BDSG § 3 Rn. 6 f., 59.

[56] Vgl. den Hinweis bei Simitis/*Dammann,* BDSG § 3 Rn. 58.

[57] Vgl. dazu BVerfG, Beschl. v. 18.12.1987 – 1 BvR 962/87 –, NJW 1988, 959 f.; *Dorer/Mainusch/Tubies*, Bundesstatistikgesetz, 1988, § 16 Rn. 27.

[58] Vgl. für Weiteres Simitis/*Dammann,* BDSG § 3 Rn. 14, der zur Erläuterung der Aggregation von 3er-Gruppen ausgeht; aus praktischer Sicht sollte sich die Zusammenfassung eher auf 5 bis 8 Personen erstrecken.

[59] Vgl. zur Volkszählung 1987 BVerfG, Beschl. v. 14.9.1987 – 1 BvR 970/87, NJW 1987, 2805 (2807 l. Sp. – wo es in der dritten Zeile „Deanonymisierung" heißen sollte); BVerfG, Beschl. v. 28.9.1987 – 1 BvR 1063/87, NJW 1988, 962 (963 f.).

lung darüber, dass A seinen Büroschlüssel verloren hat, wäre eine auf diese Person bezogene Information. Doch der Finder des Gegenstands erfährt durch seine Wahrnehmung zunächst nur, dass der Schlüssel *irgendjemandem* verloren gegangen ist. Später beobachtet er, dass A. dabei ist, in den Gängen des Bürogebäudes etwas zu suchen. Diese **Zusatzinformation** ermöglicht ihm die Schlussfolgerung, dass A (vermutlich) der Verlierer ist. – Immer dann, wenn die Erlangung entsprechender Zusatzinformation wahrscheinlich gelingen kann, ist schon aufgrund der Ausgangsinformation von der Identifizierbarkeit des Betroffenen auszugehen. Dieser Grundsatz wird in ErwG 26 der DS-DVO so festgehalten:

„Um festzustellen, ob eine natürliche Person identifizierbar ist, sollten alle Mittel berücksichtigt werden, die von dem Verantwortlichen oder einer anderen Person **nach allgemeinem Ermessen [vernünftigerweise]**[60] **wahrscheinlich genutzt** werden, um die natürliche Person … zu identifizieren … Bei der Feststellung, ob Mittel nach allgemeinem Ermessen [vernünftigerweise] wahrscheinlich zur Identifizierung… genutzt werden, sollten alle objektiven Faktoren, wie die Kosten der Identifizierung und der dafür erforderliche Zeitaufwand herangezogen werden …"

Die zuletzt genannten Kriterien[61] weisen große Ähnlichkeit mit den in § 3 Abs. 6 BDSG-alt aufgestellten Bedingungen für die *Herstellung* faktischer Anonymität auf. Sie begegnen uns – spiegelbildlich – wieder in der DS-GVO als Voraussetzungen der Identifizierbarkeit.

27 In der deutschen Rechtsprechung aus jüngerer Zeit finden sich zwei **konträre gerichtliche Beurteilungen faktischer Anonymität** bezüglich der Speicherung von Kfz-Kennzeichen und Fahrzeugidentifikationsnummern beim Hinweis- und Informationssystem (HIS) der deutschen Versicherungswirtschaft. Die dortigen Einträge beruhen auf Meldungen regulierter Schadensfälle seitens der beteiligten Versicherungsunternehmen. Diese wollen sich durch die zentral vorgehaltenen Informationen dagegen schützen, dass nach einer sogen. fiktiven Schadensregulierung – ohne Vorlage einer konkreten Reparaturkostenrechnung – betrügerisch die erneute Inanspruchnahme einer Versicherung gelingen kann. Informationen zum Eigentümer des Fahrzeugs oder zu sonstigen Personen mit Berührung zum Versicherungsfall werden dafür nicht gespeichert. Das AG Coburg[62] meinte dessen ungeachtet, das Vorliegen auf den Eigentümer bezogener Informationen beim HIS ließe sich bejahen, weil sich aufgrund der diesem bereits vorliegenden Daten im Wege einer Halterauskunft[63] bei der Kfz-Zulassungsstelle bzw. beim Kfz-Bundesamt die erforderliche Zusatzinformation ohne unverhältnismäßigen Aufwand erlangen ließe. Das AG Kassel[64] wies demgegenüber auf den mit einem solchen Vorgehen erforderlichen Zusatzaufwand und auf die Notwendigkeit der „Darlegung des die Abfrage erlaubenden besonderen Interesses" hin; dabei „handelt es sich nicht mehr um einen nicht unverhältnismäßigen Aufwand". Ein solcher läge nur vor, „wenn zwanglos etwa Haltername oder -anschrift aus der Datenbank heraus ermittelt werden könnten."

28 Das erläuterte Beispiel hat eine **typische Sachdatei** zum Gegenstand. Die in ihr enthaltenen Informationen über Autos haben als solche die erforderliche Aussagekraft zur Erfüllung der vom HIS vertraglich eingegangenen Verpflichtungen zur Auskunftserteilung. Ein berechtigtes Interesse des HIS zur Einholung einer Halterauskunft ist daher nicht erkennbar. Eben dies ergibt sich aus dem verfolgten – begrenzten – Geschäftszweck. Die Erlangung personenbezogener „Zusatzinforma-

[60] Im entsprechenden ErwG 26 DSRL lautete die analoge Formulierung: „sollten alle Mittel berücksichtigt werden, die vernünftigerweise… eingesetzt werden könnten". Eine wesentliche Bedeutung kommt der in der deutschsprachigen Fassung der Verordnung vorgenommenen sprachlichen Abwandlung nicht zu. In der französischen bzw. englischen Fassung wurde eine solche Abwandlung nicht vorgenommen; vielmehr ist hier übereinstimmend in DSRL und DS-GVO von „raisonnablement" bzw. „reasonably" – statt „nach allgemeinem Ermessen" die Rede.

[61] Sie werden bei Roßnagel/*Barlag*, DS-GVO, 2017, § 3 Rn. 9 f., nicht hinreichend berücksichtigt.

[62] AG Coburg, Urt. v. 7.11.2012 – 12 C 179/12, ZD 2013, 458.

[63] Vgl. § 39 Abs. 1 StVG.

[64] AG Kassel, Urt. v. 7.5.2013 – 435 C 584/13, ZD 2014, 90.

tion“ verstieße also mangels Grundlage im StVG und mangels Erforderlichkeit gegen § 16 Abs. 1 Nr. 2 BDSG-alt bzw. gegen Art. 6 Abs. 1 lit. f DS-GVO. Dem AG Kassel ist also im Ergebnis zu folgen. Das gilt unabhängig davon, ob man seinem eher lakonischen Hinweis auf einen unverhältnismäßigen Aufwand zustimmen möchte. Zu darauf abgestimmten Gewichtungen wird es noch weiterer Konkretisierung durch die künftige Rechtsprechung bedürfen.

III. Zusatzwissen im rechtlichen Rahmen

29 Insgesamt kann nach zutreffender Auffassung etwaig **rechtswidrig erlangbare** Zusatzinformation **nicht zur Begründung des Personenbezugs** der Ausgangsinformation herangezogen werden.[65] Es besteht keine Grundlage, einen Verarbeiter von Information den Beschränkungen des Datenschutzrechts nur deshalb zu unterwerfen, weil es möglich ist, dass Personen in seiner Lage bereit sein können, das Recht zu verletzen. Dadurch ließe sich auch schwerlich erhöhter Persönlichkeitsschutz erreichen, weil solche Bereitschaft, wenn sie denn besteht, sich gleichermaßen bei feststehendem Personenbezug der Ausgangsinformation realisieren dürfte. Rechtssystematisch ist – über den zuvor erörterten Rechtsfall hinaus – zu berücksichtigen, dass die über möglichen Personenbezug gesteuerten datenschutzrechtlichen Normen nicht für sich allein stehen, sondern im Rahmen der Rechtsordnung, im Zusammenspiel mit anderen (informationsrechtlichen) Normen verstanden werden müssen.[66] Das gilt insbesondere mit Blick auf die Berufs- und Amtsgeheimnisse oder das Telekommunikationsgeheimnis, für deren Verletzung spezifische rechtliche Sanktionen vorgesehen sind.

IV. Zusatzwissen Dritter

1. Relativer/absoluter Personenbezug

30 Umfangreich ist in der Literatur die Frage diskutiert worden, ob der Verantwortliche personenbezogene Daten auch dann verarbeitet, wenn er über das erforderliche Zusatzwissen zur Herstellung des Personenbezugs nicht selbst verfügt, sondern nur Dritte (außerhalb seines kommunikativen Umfelds).[67] Nach herrschender Auffassung ist, was das Wissen Dritter anbetrifft, die erkennbare Zugänglichkeit für den Verantwortlichen rechtsstaatlich begründete Voraussetzung („**relativer Personenbezug**“).[68] Nach der Theorie vom „absoluten Personenbezug“ würde hingegen die Fähigkeit jedes beliebigen Dritten zur Deanonymisierung genügen.[69] Solche Versuche der Ausweitung des Kreises personenbezogener Daten kann dem Schutz damit einbezogener „Betroffener“ durchaus nicht förderlich sein, weil ein diesbezüglich Verantwortlicher in Ermangelung möglicher Kenntnis der zu schützenden Individuen deren eventuelle Rechtsstellung nicht berücksichtigen kann und wird.[70] Für die Rechtslage nach der DS-GVO ist der bereits zitierte

[65] Näheres dazu bei Simitis/*Dammann,* BDSG § 3 Rn. 26 ff., 33.
[66] Das übersehen Däubler/Klebe/Wedde/*Weichert,* BDSG § 3 Rn. 15; *Pahlen-Brandt*, K&R 2008, 288 (289) im Anschluss an das AG Berlin Mitte, Urt. v. 27.3.2007 – 5 C 314/06, K&R 2007, 600.
[67] Vgl. dazu *Kühling/Klar*, Unsicherheitsfaktor Datenschutzrecht – das Beispiel des Personenbezugs und der Anonymität, NJW 2013, 3611 (3614 ff.).
[68] Vgl. Taeger/Gabel/*Buchner,* BDSG § 3 Rn. 13; *Brink/Eckhardt*, Wann ist ein Datum ein personenbezogenes Datum?, ZD 2015, 205 (209 ff.).
[69] Das gilt im wesentlichen für etliche Stellungnahmen von deutschen Datenschutzbeauftragten; vgl. Nachweise bei *Kühling/Klar*, NJW 2013, 3611 Fn. 30.
[70] Vgl. die Überlegungen zu Art. 11 DS-GVO → Rn. 40.

ErwG 26 (→ Rn. 26) zu berücksichtigen, in welchem allerdings ausdrücklich „von dem Verantwortlichen *oder einer anderen Person*" als mögliche Benutzer von Mitteln zur Identifizierung die Rede ist. Doch orientiert sich eben dieser Erwägungsgrund, wie bereits dargestellt wurde, an einer nach allgemeinem Ermessen [vernünftigerweise][71] zu erwartenden Nutzung. Zugleich gelten die Grundsätze zur Abgrenzung gegenüber faktischer Anonymität im nachfolgenden Satz des ErwG 26 DS-DVO.[72]

Damit ist deutlich geworden, dass ein Verarbeiter von Information sich nicht **31**
um Identifizierungsmöglichkeiten zu kümmern hat, die jenseits seines Wirkungskreises liegen. Ein einzelner Unternehmer braucht sich nicht dafür zu interessieren, ob das statistische Material, das ihm sein Berufsverband zur Verfügung gestellt hat, möglicherweise von Letzterem durch diesem zur Verfügung stehende Methoden mit verhältnismäßigem Aufwand auf Individuen rückführbar sei. Das gleiche gilt für den **Cloud Service-Provider**, dem der Cloud Service-Nutzer stark verschlüsselte personenbezogene Informationen nach dem Stand der Technik anvertraut hat.[73] Demgegenüber ist bei einer Weiterleitung von Informationen ohne Personenbezug an einen Inhaber erforderlichen Zusatzwissens Vorsicht geboten. Insoweit kann von einer Übermittlung im Sinne des Art. 4 Nr. 2 DS-GVO auszugehen sein.[74]

2. Dynamische IP-Adresse als personenbezogenes Datum?

In diesen Kontext gehört auch die stattgefundene Kontroverse um die Qualität **32**
der dynamischen *I*nternet *P*rotocol-Adresse.[75] Diese stellt sich als eine dem Rechner beim Anschluss an das Internet jeweils neu zugeteilte Zahlenfolge dar. Sie dient der Kommunikation zwischen Nutzern und jeweiligen Online-Mediendiensten (Content-Provider). Inhaltlich ermöglicht sie diesen lediglich eine grobe regionale Zuordnung des Nutzers. Die IP-Adresse lässt als solche einen Rückschluss auf die Person des Nutzers/Teilnehmers[76] nicht zu. Allein der Internet-Zugangsanbieter (Access-Provider), der die IP-Adressen jeweils vergibt, verfügt über die entsprechenden Bestandsdaten der Teilnehmer (§ 95 TKG) und hat die technische Möglichkeit der Verknüpfung. Nur er ist in der Lage, auf der Grundlage einer IP-Adresse und entsprechender Zeitangabe zu ermitteln, um welchen Teilnehmer es sich im Einzelfall gehandelt hat. Freilich ist ihm die Offenbarung im Hinblick auf das **Telekommunikationsgeheimnis** nur unter eng begrenzten, gesetzlich geregelten Voraussetzungen möglich (§ 88 TKG). Ohne Vorliegen dieser Voraussetzungen ist die IP-Adresse also durchweg für den Zugangsanbieter auf einen identifizierten/

[71] → Rn. 26 mit Fn. 60.

[72] Vgl. dazu auch *Brink/Eckhardt*, ZD 2015, 205 (208 f.); der Auffassung *Härtings*, DS-GVO, 2016, Rn. 270 ff., die DS-GVO tendiere zur Theorie vom absoluten Personenbezug, kann deshalb nicht gefolgt werden.

[73] Vgl. dazu *Grenzer/Heitmüller*, Zur Problematik des Personenbezuges beim Cloud Computing, PinG 2014, 221 (229 f.). – Das schließt nicht aus, dass die für den Cloud Service-Nutzer zuständige Aufsichtsbehörde sich um die erforderliche Qualität der Übermittlung – der Verschlüsselung – an den Cloud Service-Provider, kümmern kann; vgl. zu diesen Besorgnissen die „Orientierungshilfe – Cloud Computing", Version 2.0, v. 9.10.2014, S. 12 f.; dazu *Eckhardt*, DuD 2015, 176 (179 f.).

[74] Vgl. Simitis/*Dammann,* BDSG § 3 Rn. 34; Gola/Schomerus/*Gola/Körffer/Klug,* BDSG § 3 Rn. 44a; *Kühling/Klar*, NJW 2013, 3611 (3615 bei Fn. 39).

[75] Eine Übersicht über den Meinungsstand gab der BGH in seinem Vorlagebeschluss an den EuGH v. 28.10.2014 – VI ZR 135/13, ZD 2015, 80 Rn. 23 ff.; *Eckhardt*, IP-Adresse als personenbezogenes Datum – neues Öl ins Feuer, CR 2011, 399 ff.

[76] Zu diesen Begriffen § 3 Nr. 14, 20 TKG.

identifizierbaren Teilnehmer bezogen, schwerlich aber für den Content-Provider (→ Rn. 30, 29).

33 Der **EuGH** hat am 19.10.2016[77] – auf Vorlage des BGH hin[78] – auf der Grundlage des Art. 2 lit. a DSRL entschieden, dass eine dynamische IP-Adresse für den Mediendienstanbieter ein personenbezogenes Datum darstellt, wenn dieser „über rechtliche Mittel verfügt, die es ihm erlauben, die betreffende Person anhand der Zusatzinformationen, über die der Internetzugangsanbieter dieser Person verfügt, bestimmen zu lassen." Diese Aussage steht für sich genommen in Übereinstimmung mit dem zuvor Dargelegten, vorausgesetzt, der Content-Provider hat Kenntnis davon erlangt, welcher Access-Provider die Zuordnung der entsprechenden IP-Adresse vorgenommen hat, um sich unter Bezugnahme auf triftige Gründe – Abwehr von Cyberattaken – an diesen mit der Bitte um Offenlegung des Teilnehmers wenden zu können. Unklar bleibt die Entscheidung freilich hinsichtlich einer entsprechenden rechtlichen Zulässigkeit für die Offenlegung. Der EuGH verweist diesbezüglich auf „vom vorlegenden Gericht insoweit vorzunehmende Prüfungen".[79] Die Entscheidung hierüber wurde dem BGH überlassen, der zwischenzeitlich zur Annahme vorliegenden Personenbezugs gelangte, wenngleich ohne den nachfolgend festgehaltenen Einwänden gerecht zu werden.[80]

34 Die letztlich verborgen gebliebene Grundsatzfrage wird unter der Geltung der DS-GVO gleichermaßen der Klärung bedürfen. Sie ergibt sich daraus, dass weder dem Content- noch dem Access-Provider die Möglichkeit offensteht, die von Ersterem gewünschte Information ohne **Einschaltung staatlicher Instanzen** – der Sicherheitsbehörden – in Erfahrung zu bringen. Deren Entscheidung im konkreten Fall beinhaltet fraglos einen Eingriff in den Persönlichkeitsbereich des Betroffenen, um dessen Identität es geht. Dafür stehen spezifische, die staatliche Tätigkeit eingrenzende Rechtsgrundlagen zur Verfügung.[81] Deren Einhaltung – vor dem Hintergrund der allseitigen Beachtung des Telekommunikationsgeheimnisses – dient dem insoweit nach Art. 10 GG gebotenen Persönlichkeitsschutz. Dem allgemeinen Datenschutzrecht verbleibt im Hinblick auf die spezialgesetzlichen Regelungen keine konfliktlösende Rolle. Denn soweit sich aufgrund des Spezialrechts im Einzelfall ergibt, dass der staatliche Zugriff unzulässig ist, gibt es für das Datenschutzrecht nichts mehr zu entscheiden. Dessen Anwendung wegen trotzdem abstrakt/absolut anzunehmenden Personenbezugs auch beim Content Provider ginge ins Leere. Darüber hinaus gilt es zu bedenken, dass staatliches Vorgehen seitens der Sicherheitsbehörden (oftmals vorbehaltlich richterlicher Entscheidung) in vielen anderen Lebensbereichen gleichermaßen in Betracht kommt. Es ist wenig plausibel und verfassungsrechtlich bedenklich, dass deshalb (faktisch) anonyme Datenbestände – interne Statistiken, Planungen, Berichte über betriebliche, technische Abläufe und Forschungsberichte – in großem Umfang als personenbezogene zu behandeln sein sollten.

---

[77] EuGH, Urt. v. 19.10.2016 – C-582/14, ZD 2017, 24, Rn. 31 ff., 49 – Breyer./. BRD; orientiert an den Schlussanträgen des Generalanwalts GA *Campos Sánchez-Bordona,* SchlA v. 12.5.2016 – C-582/14, ECLI:EU:C:2016:339; Anm. von *Kühling/Klar*, ZD 2017, 27 ff.

[78] BGH, EuGH-Vorlage v. 28.10.2014 – VI ZR 135/13, ZD 2015, 80 ff.

[79] EuGH, Urt. v. 19.10.2016 – C 582/14, ZD 2017, 24, Rn. 47.

[80] BGH, Urt. v. 16.5.2017 – VI ZR 135/13, NJW 2017, 2416, Rn. 26.

[81] §§ 161, 163 StPO, § 22a Abs. 2 BPolG, Art. 34b Abs. 4 S. 1 BayPAG, § 15a Abs. 2 S. 5 HSOG, § 20a Abs. 1 S. 1 Nr. 1, Hs. 2 nrwPolG, § 8d Abs. 2 S. 1 BVerfSchG, jeweils i. V. m. § 113 Abs. 1 S. 3, Abs. 2–4 TKG; dazu BVerfGE 125, 260 (340 ff., 356 f. = Rn. 254 ff., 288 ff.); §§ 100g, 100j, 101a StPO.

V. Abstufung zwischen identifizierten und identifizierbaren Betroffenen

In der **Literatur zum BDSG-alt** findet sich häufiger die Überlegung, das Gesetz mache zwischen der Bestimmtheit und der Bestimmbarkeit natürlicher Personen **keinen Unterschied**; eine Abgrenzung zwischen diesen beiden Kriterien sei deshalb überflüssig bzw. „allenfalls von theoretischem Interesse".[82] Diese Auffassung ist weder mit Blick auf die Rechtstatsachen noch auf die rechtlichen Erfordernisse nach der DS-GVO akzeptabel. **35**

1. Pseudonymität

Insbesondere die Pseudonymisierung beruht regelmäßig auf einer **Umwandlung** von auf ***identifizierte*** Personen bezogenen Informationen zu solchen, die mithilfe zusätzlicher Information, nämlich einer festgelegten Zuordnungsregel, auf ***identifizierbare*** Personen bezogen bleiben.[83] Im Anschluss an die Definition in Art. 4 Nr. 5 DS-GVO[84] wird in ErwG 26 und 28 DS-DVO u. a. ausgeführt: **36**

„Einer Pseudonymisierung unterzogene personenbezogene Daten, die durch Heranziehung zusätzlicher Informationen einer natürlichen Person zugeordnet werden könnten, sollten als Informationen über eine identifizierbare natürliche Person betrachtet werden."

„Die Anwendung der Pseudonymisierung auf personenbezogene Daten kann die Risiken der betroffenen Person senken und die Verantwortlichen…bei der Einhaltung ihrer Datenschutzpflichten unterstützen."

In Art. 25 Abs. 1 und Art. 32 Abs. 1 lit. a DS-GVO wird die Pseudonymisierung/Verschlüsselung, welche nach § 3a S. 2 BDSG-alt nur als Programmsatz vorgesehen wird,[85] als geeignete technische/organisatorische Maßnahme vorgeschrieben.[86] Sie unterscheidet sich von der Datenaggregation (zu statistischen Zwecken) durch die Erhaltung der (verschleierten) Zuordnung jeweiliger Daten(sätze) zur einzelnen Person. Das ermöglicht die Verkettbarkeit mit nachfolgenden Speicherungen unter demselben Pseudonym und damit Langzeitstudien und Profilbildung.[87]

Pseudonymisierung ist ein **Instrument möglichen Interessenausgleichs** zwischen Verantwortlichem und Betroffenem. Der alltägliche Umgang in Arbeit, Wirtschaft und Verwaltung orientiert sich überwiegend (anders bei Bargeschäften) an dem direkten – namentlichen – Bezug auf die jeweils beteiligten Personen. Demgegenüber sind (medizinische) Forschung, Planung, Rechnungsprüfung oder Qualitätssicherung darauf i. d. R. nicht angewiesen, wenngleich in einzelnen Fällen – z. B. aufgedeckter Erkrankungen – nicht darauf verzichtet werden sollte, den konkreten Personenbezug herzustellen. Die Ersetzung des Namens und vergleichbarer Identifikationsmerkmale[88] lässt regelmäßig die beteiligten Individuen unerkannt und er- **37**

---

[82] Vgl. Taeger/Gabel/*Buchner,* BDSG § 3 Rn. 11; Simitis/*Dammann,* BDSG § 3 Rn. 23; *Kühling/Seidel/Sivridis*, DatSchR, Rn. 219; *Haase*, Datenschutzrechtliche Fragen, S. 259 f.

[83] Vgl. – noch zu § 3 Abs. 6a BDSG-alt – Simitis/*Scholz,* BDSG § 3 Rn. 214 f.; zur Vergleichbarkeit der beiden Bestimmungen auch Roßnagel/*Johannes*, DS-GVO, 2017, § 4 Rn. 92; zur Pseudonymisierung gerichtlicher Entscheidungen → § 25 Rn. 18.

[84] Im wesentlichen übereinstimmend – für den Sicherheitsbereich – § 46 Nr. 5 BDSG 2018.

[85] Vgl. Gola/Schomerus/*Gola/Körffer/Klug,* BDSG § 3a Rn. 2.

[86] Zu diesen Maßnahmen → §§ 19 f.

[87] Hierzu und zum folgenden Simitis/*Scholz,* BDSG § 3 Rn. 216 ff.; auch *Karg*, Anonymität, Pseudonyme und Personenbezug revisited?, DuD 2015, 520 (523 f.); *Roßnagel/Scholz*, Datenschutz durch Anonymität und Pseudonymität, MMR 2000, 721 ff.; beachte § 30 Abs. 1 BDSG-alt.

[88] Im Überblick → Rn. 5.

möglicht dem Verantwortlichen einen freieren Umgang mit der betroffenen (partiell verschlüsselten) Information, z. B. bei Übermittlungen in beteiligten Fachkreisen.[89]

2. Eingeschränkte Anwendung datenschutzrechtlicher Bestimmungen gemäß Art. 11 DS-GVO

38 Die Bedeutung der Unterscheidung zwischen Informationen mit Bezug auf identifizierte und auf identifizierbare Personen ist anhand der ausdrücklichen gesetzlichen Regelungen zur Pseudonymität deutlich hervorgetreten. Der Verordnungsgeber geht zurecht davon aus, dass der Umgang mit Direktinformationen datenschutzrechtlich einem anderen, strengeren Regime unterworfen sein soll als der Umgang mit pseudonymisierten Informationen, mögen auch beide Kategorien unter den Begriff personenbezogene Daten fallen. Das mehrfach hervorgehobene Postulat der Pseudonymisierung ist Ausdruck dieser Abstufung. Ein Beispiel dafür im deutschen Recht ist – als (bislang) verbindliche Regelung[90] – in **§ 15 Abs. 3 TMG** enthalten, wonach der Diensteanbieter für Zwecke der Werbung etc. Nutzungsprofile nur bei Verwendung von Pseudonymen erstellen darf (sofern der Nutzer dem nicht widerspricht – Opt-out-Regelung). Unter anderem Cookies-Dateien können dabei der Verknüpfung dienen.[91]

39 Diese Feststellungen werfen die weitere Frage auf, wieweit das Konzept der Pseudonymität aufgrund nur identifizierbarer Betroffener verallgemeinerungsfähig ist. Das betrifft gerade auch **Big-Data-Anwendungen**, etwa zur Vorhersage von Epidemien aufgrund individueller Nutzungen des Internet oder zur Beurteilung der Verkehrslage aufgrund der Erfassung von Echtzeit-Standortdaten.[92] Oftmals ist die Identifizierung der involvierten Personen selbst dabei überflüssig.[93] Die pseudonyme Erhebung des Basismaterials bzw. dessen pseudonyme Behandlung ist insoweit datenschutzrechtlich geboten. Von daher kann die Abwägung der wechselseitigen Interessen zu weitgehender Zulässigkeit der Weiterverwendung führen.[94]

40 Für die Fälle fehlender Identifizierung bei bestehender Identifizierbarkeit des Betroffenen legt Art. 11 DS-GVO dies fest:

> „Ist für die Zwecke, für die ein Verantwortlicher personenbezogene Daten verarbeitet, die Identifizierung der betroffenen Person durch den Verantwortlichen nicht oder nicht mehr erforderlich, so ist dieser nicht verpflichtet, **zur bloßen Einhaltung dieser Verordnung zusätzliche Informationen** aufzubewahren, einzuholen oder zu verarbeiten, um die betroffene Person zu identifizieren."[95]

---

[89] In die gleiche Richtung weisen schon §§ 30, 40 Abs. 2 S. 2, 3 BDSG-alt; nicht gefolgt werden kann der skeptischen Interpretation zur DS-GVO bei *Härting*, DS-GVO, 2016, Rn. 300 ff.

[90] Die datenschutzrechtlichen Vorschriften der §§ 11 ff. TMG werden durch die GS-GVO verdrängt, vgl. Gola/*Gola,* DS-GVO Art. 6 Rn. 30; Plath/*Hullen/Roggenkamp,* BDSG/DSGVO, TMG Einleitung Rn. 13; → § 26 Rn. 21 ff.

[91] Vgl. Simitis/*Dammann,* BDSG § 3 Rn. 65; Spindler/Schuster/Nink/*Schuster/Nink*, Recht der elektronischen Medien, 2015, TMG § 15 Rn. 9; *Schleipfer*, Datenschutzkonformer Umgang mit Nutzungsprofilen, ZD 2015, 399 ff.

[92] Dazu das Beispiel „Intrix" bei *Mayer-Schönberger/Cukier*, Big Data, 2013, S. 169 f.; weitere Nachweise → § 1 Rn. 1 Fn. 7.

[93] Vgl. *Leonard*, Customer data analytics: privacy settings for ‚Big Data' business, IDPL 2014, 53 (60, 62); *Türpe u. a.,* Denkverbote für Star-Trek-Computer?, DuD 2014, 31 ff.

[94] Vgl. zur Pseudonymität als Abwägungsbelang Simitis/*Scholz,* BDSG § 3 Rn. 219d; *Härting*, NJW 2013, 2065 (2067); *Eckhardt/Kramer*, EU-DSGVO – Diskussionspunkte aus der Praxis, DuD 2013, 287 (288 f.).

[95] Zur Widersprüchlichkeit des nachfolgenden Abs. 2 S. 1 DS-GVO Plath/*Plath,* BDSG/DSGVO, DS-GVO Art. 11 Rn. 7; *Laue/Nink/Kremer*, § 2 Rn. 69; beachte auch ErwG 57 DS-GVO.