2 Personenbezug bei Pseudonymisierung und Anonymisierung

Können pseudonymisierte Daten aus Sicht eines Empfängers als anonym gelten, wenn der Sender den Schlüssel für die Pseudonymisierung verwahrt und dieser für den Empfänger nicht zugänglich ist? Geben Sie an, welche Gründe in Literatur und Rechtsprechung für oder gegen die Annahme des Konzepts des relativen Personenbezugs sprechen.

Ein Personenbezug ist das entscheidende Kriterium für die Anwendung des Datenschutzrechts. Ohne einen Personenbezug würden sich die nachfolgend untersuchten datenschutzrechtlichen Herausforderungen überhaupt nicht stellen. Daher soll hier zunächst auf die Frage nach dem Personenbezug, insbesondere bei Pseudonymisierung und Anonymisierung, eingegangen werden.

„Anonymisieren ist das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können" (§ 3 Abs. 6 BDSG). Pseudonymisieren ist dagegen „das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren" (§ 3 Abs. 6a BDSG).

Pseudonymisierte Daten weisen vor diesem Hintergrund nach einhelliger Auffassung in der juristischen Literatur für die Stelle, welche über die Zuordnung des

Pseudonyms zu der dahinter stehenden Person verfügt, einen Personenbezug im Sinne des Datenschutzrechts auf.[2] Gibt diese Stelle die pseudonymen Daten an einen Empfänger weiter, sind die Daten für diese Entität dann als anonym anzusehen, wenn sie nicht mehr oder nicht mehr mit verhältnismäßigem Aufwand einer natürlichen Person zugeordnet werden können. Auf welche Perspektive (verantwortliche Stelle oder Empfänger) bei der Beurteilung dieser Frage abzustellen ist (dazu sogleich: Relativität des Personenbezugs in subjektiver Hinsicht), ist gleichermaßen umstritten wie die Anforderungen, die an eine hinreichende Anonymität eines Datums zu stellen sind (dazu unten: Relativität des Personenbezugs in objektiver Hinsicht).[3]

Eine Differenzierung nach dem Ort der Niederlassung und der Art der jeweils verantwortlichen Stelle ist hier nicht vorzunehmen und erscheint für die Beantwortung dieser Frage auch nicht erforderlich, denn die Begriffe „personenbezogene Daten", „Pseudonymisierung" und „Anonymisierung" sind nach dem Bundesdatenschutzgesetz (BDSG), den Landesdatenschutzgesetzen sowie den auf Kliniken anwendbaren Datenschutzvorschriften der Länder auch vor europarechtlichem Hintergrund letztlich gleich zu verstehen.[4]

2.1 Relativität des Personenbezugs in subjektiver Hinsicht

2.1.1 Überblick

Die Frage, ob ein Personenbezug vorliegt, kann zum einen, bei einer relativen Betrachtungsweise, aus der Perspektive der jeweils datenverarbeitenden Stelle vorgenommen werden (relatives Verständnis). Möglich erscheint jedoch auch, bei der Frage der Bestimmbarkeit der Person das Wissen Dritter mit einzubeziehen (absoluter Personenbezug). Der Wortlaut der Definition des Personenbezugs im Datenschutzrecht ist insoweit offen und lässt beide Ansichten zu.

In der jüngeren Vergangenheit ist die Problematik des Personenbezugs vor allem anhand der Frage kontrovers diskutiert worden, ob IP-Adressen einen Personenbezug aufweisen können.[5] Ob ein relatives oder absolutes Verständnis zugrunde zu legen ist, wird seitens der Gerichte und der Literatur aber nicht einheitlich beurteilt. In der instanzgerichtlichen Rechtsprechung wird tendenziell eine eher relative Sichtweise zugrunde gelegt.[6] Abschließende höchstrichterliche Stellungnahmen zur Frage, ob bei der Beurteilung des Personenbezugs auf die verarbeitende Stelle oder auch

2 Vgl. nur Buchner, in: Taeger/Gabel, BDSG, § 3 Rdnr. 50; Gola/Schomerus, BDSG, § 3 Rdnr. 46; Plath/Schreiber, in: Plath, BDSG, § 3 Rdnr. 61ff.; Schaffland/Wiltfang, BDSG, § 3 Rdnr. 13; Scholz, in: Simitis (Hg.), BDSG, § 3 Rdnr. 215f.

3 Vgl. zur folgenden Problematik des Personenbezug und der Anonymität von Daten Kühling/Klar, NJW 2013, 3611ff.

4 Vgl. 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. EG 1995 Nr. L 281 S. 31. Der Begriff der „personenbezogenen Daten" ist in Art. 2 Buchst. a dieser Richtlinie definiert, welche von Bund und Ländern in nationales Recht umgesetzt werden musste. Vor allem der Begriff der Anonymität, weitgehend aber auch derjenige der Pseudonymität, leitet sich hiervon ab.

5 Dazu etwa Gerlach, CR 2013, 478ff.; Krüger/Maucher, MMR 2011, 433ff.; Meyerdierks, MMR 2009, 9ff.; Pahlen-Brandt, K&R 2008, 288ff.

6 OLG Hamburg, CR 2011, 126; LG Wuppertal, MMR 2011, 65, 66; LG Bamberg, ZD 2013, 628 m. Anm. Arning/Moos; LG Berlin, CR 2013, 471; AG München, ZUM-RD 2009, 413, 414; a.A. wohl AG Berlin-Mitte, K&R 2007, 600, 601; VG Wiesbaden, MMR 2009, 428, 432.

auf Dritte abzustellen ist, liegen dagegen nicht vor.[7] Dies gilt auch mit Blick auf die Rechtsprechung des EuGH, der bislang ebenfalls keine verlässlichen Aussagen zu entnehmen sind.[8] Erst jüngst wurde beim EuGH auf Vorlage des Bundesgerichtshofs ein noch laufendes Verfahren zur Entscheidung über den absoluten oder relativen Ansatz des Personenbezugs in Gang gesetzt.[9] In der behördlichen Aufsichtspraxis zeichnet sich derzeit auch noch keine konsistente Linie ab.

Trotz einer vergleichsweise langen Datenschutztradition in Deutschland ist damit zu konstatieren, dass der Begriff des Personenbezugs bislang noch keiner abschließenden Konturierung zugeführt worden ist. Dies ist umso misslicher, als das Vorliegen eines Personenbezugs in der Praxis von entscheidender Bedeutung ist, da dieser wesentlich für die Anwendbarkeit des Datenschutzrechts ist.

2.1.1.1 Absolutes Verständnis

Nach einem absoluten Verständnis ist von einem Personenbezug bereits dann auszugehen, wenn lediglich für Dritte, die nicht notwendigerweise (potenzielle) Datenempfänger sind, die Möglichkeit der Zuordnung zu einer Person besteht. Eine solch weite Sichtweise wird vor allem von einigen deutschen Datenschutzbehörden sowie wohl auch dem *Düsseldorfer Kreis*[10] dieser Behörden vertreten, welche die Anwendungsvoraussetzungen des Datenschutzrechts in der Regel weniger restriktiv auslegen.[11] Mit dem Argument eines optimalen Schutzes der Betroffenenrechte haben sich aber auch vereinzelte Stimmen in der datenschutzrechtlichen Literatur[12] dieser weiten Ansicht angeschlossen. Was die Position der *Artikel-29-Datenschutzgruppe* der Aufsichtsbehörden der EU-Mitgliedstaaten anbelangt, so ist diese nicht eindeutig. Die Ausführungen in deren Stellungnahme 4/2007 zum Begriff „personenbezogene Daten“[13] lassen sich nicht klar dem absoluten oder dem relativen Konzept zuordnen.[14]

---

7 Auch dem Urteil des BGH v. 13.01.2011 (III ZR 146/10, MMR 2011, 341) zum Umgang mit dynamischen IP-Adressen bei einem Access-Provider (insoweit hat der BGH unproblematisch einen Personenbezug unterstellt) kann keine eindeutige Positionierung im Hinblick auf den absoluten oder relativen Ansatz entnommen werden (Lorenz, jurisPR-ITR 15/2011 Anm. 2; a.A. Krüger/Maucher, MMR 2011, 433, 436); vgl. Klar, Datenschutzrecht und die Visualisierung des öffentlichen Raums, 2012, S. 144f. Allerdings hat der BGH mit Beschluss v. 28.10.2014 (VI ZR 135/13, CR 2015, 109) dem EuGH die Frage vorgelegt, ob die Definition der personenbezogenen Daten in Art. 2 Buchstabe a der Datenschutz-Richtlinie 95/46/EG dahin auszulegen ist, dass die IP-Adresse, die ein Websitebetreiber beim Zugriff auf seine Internetseite speichert, für diesen schon dann ein personenbezogenes Datum darstellt, wenn ein Dritter (wie der Access-Provider) über das zur Identifizierung der betroffenen Person erforderliche Zusatzwissen verfügt. Letztlich wird der EuGH also um Vorabentscheidung darüber ersucht, ob vor europarechtlichem Hintergrund der Personenbezug absolut oder relativ zu verstehen ist.

8 Der EuGH, Urt. v. 24.11.2011, Rs. C-70/10, Rdnr. 51 – Scarlet Extended, hat die Frage im Zusammenhang mit IP-Adressen lediglich gestreift; kritisch dazu Klar, DÖV 2013, 103, 112.

9 Das beim EuGH unter dem Az. C-582/14 geführte Verfahren wurde auf das in der obigen Fn. 7 angeführte Vorabentscheidungsersuchen des BGH vom 28.10.2014 (Az. VI ZR 135/13) hin eingeleitet.

10 Düsseldorfer Kreis, Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich am 26./27.11.2009 in Stralsund, S. 1, in Bezug auf IP-Adressen.

11 So etwa der ehemalige Bundesbeauftragte für den Datenschutz und die Informationsfreiheit Schaar, Datenschutz im Internet, 2002, Kap. 3 Rdnr. 175; die Datenschutzbeauftragte der Freien Universität Berlin Pahlen-Brandt, K&R 2008, 288; dies., DuD 2008, 34; der Datenschutzbeauftragte des Landes Schleswig-Holstein Weichert, in: Däubler/Klebe/Wedde/Weichert, BDSG, 3. Aufl. 2010, § 3 Rdnr. 13; vgl. auch die Argumentation des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein (ULD), abrufbar unter https://www.datenschutzzentrum.de/artikel/575-IP-Adressen-und-andere-Nutzungsdaten-Haeufig-gestellte-Fragen.html; ebenso wohl auch der europäische Datenschutzbeauftragte Hustinx, EDPS comments on selected issues that arise from the IMCO report on the review of Directive 2002/22/EC (Universal Service) & Directive 2002/58/EC (ePrivacy), 2008, S. 2ff.; relativierend in Bezug auf IP-Adressen jedoch Hustinx, Protection of Personal Data On-Line: The Issue of IP Adresses, 2009, S. 7.

12 Scheja/Haag, in: Leupold/Glossner (Hrsg.), Münchener Anwaltshandbuch IT-Recht, Teil 4. E. Rdnr. 40.

13 Artikel-29-Datenschutzgruppe, Stellungnahme 4/2007 zum Begriff „personenbezogene Daten“, S. 19ff. Siehe ferner Artikel-29-Datenschutzgruppe, Stellungnahme 1/2008 zu Datenschutzfragen im Zusammenhang mit Suchmaschinen, S. 9.

14 Näher dazu Kühling/Klar, NJW 2013, 3611, 3614.

Folge der Annahme eines absoluten Verständnisses wäre, dass das in der Fragestellung angedachten Pseudonymisierungsverfahren nicht zur Anonymität für den Empfänger der pseudonymen Daten führen würden, selbst wenn dieser nicht im Besitz der Vorschrift für die Zuordnung des Pseudonyms zur dahinter stehenden Person ist. Bereits für die Übertragung solcher Daten an diese Empfänger wäre dann eine datenschutzrechtliche Erlaubnis und eine – das Arzt-Patienten-Verhältnis einbeziehende – Befugnis nach § 203 StGB erforderlich.

2.1.1.2 Relativer Personenbezug

In der datenschutzrechtlichen Literatur wird dagegen überwiegend – allerdings meist ebenfalls ohne tiefgreifende Auseinandersetzung – eine restriktive Auffassung vertreten, wonach der Personenbezug relativ zu verstehen sei und eine Beurteilung aus der Sicht der datenverarbeitenden Stelle heraus vorgenommen werden solle.[15]

Bei Zugrundelegung dieses relativen Konzepts könnte für die Behandlungseinrichtung der Personenbezug durch Pseudonymisierung erhalten bleiben, dieser für den externen Dienstleister, der nicht im Besitz der Zuordnungsvorschrift ist, jedoch grundsätzlich ausgeschlossen werden, weil die Daten für ihn dann als anonymisiert gelten könnten.[16]

2.1.2 Stellungnahme

Das Konzept des relativen Personenbezugs ist gegenüber dem absoluten Verständnis vorzugswürdig, denn Letzteres führt dazu, dass nahezu jeder Datenumgang an den Vorschriften des Datenschutzrechts zu messen wäre. So wird man nämlich nur in den seltensten Fällen ausschließen können, dass eine Person für einen beliebigen Dritten bestimmbar ist, zumal diese Auffassung sogar dann Geltung beansprucht, wenn der Dritte unter Umständen niemals Einsicht in den Datensatz erlangt.

Bei isolierter Betrachtung eines effektiven Schutzes des Grundrechts auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG mag das absolute Verständnis zwar zielführend erscheinen. Ein derart umfassendes Schutzverständnis würde allerdings auch im Rahmen des notwendigen Ausgleichs der sich gegenüberstehenden Interessen zu einer fragwürdig einseitigen Privilegierung der Position der Betroffenen führen, zumal gerade mit Blick auf private Stellen gilt, dass deren Datenumgang ebenfalls grundrechtlichen Schutz genießt. Er unterfällt zumindest der allgemeinen Handlungsfreiheit des Art. 2 Abs. 1 GG, ggf. aber auch der Berufsfreiheit aus Art. 12 Abs. 1 GG oder der Wissenschaftsfreiheit des Art. 5 Abs. 3 GG, wobei letztere prinzipiell auch für öffentliche Stellen (wie Universitäten oder

15 Arning/Forgó/Krügel, DuD 2006, 700; Bergmann/Möhrle/Herb, BDSG, § 3 Rdnr. 32; Braun, in: Geppert/Schütz, BeckOK TKG, § 91 Rdnr. 15; Buchner, in: Taeger/Gabel, BDSG, § 3 Rdnr. 13; Casper, DÖV 2009, 965, 966; Dammann, in: Simitis (Hg.), BDSG, § 3 Rdnr. 32ff.; Gola/Schomerus, BDSG, § 3 Rdnr. 10; Kroschwald, ZD 2014, 75, 76; Krüger/Maucher, MMR 2011, 433, 436; Meyerdierks, MMR 2013, 705, 706; Moos, K&R 2008, 137, 139; Plath/Schreiber, in: Plath, BDSG, § 3 Rdnr. 15; Polenz, in: Kilian/Heussen (Hg.), Computerrecht, Rechtsquellen und Grundbegriffe des allgemeinen Datenschutzes, Teil 13. Rdnr. 68; Rammos, ZD 2013, 599, 601; Redeker, IT-Recht, Rdnr. 935; Roßnagel/Scholz, MMR 2000, 722, 723f.; Schaffland/Wiltfang, BDSG, § 3 Rdnr. 17; Scholz, in: Simitis (Hg.), BDSG, § 3 Rdnr. 217f.; Spindler/Nink, in: Spindler/Schuster (Hg.), Recht der elektronischen Medien, § 11 TMG Rdnr. 5a; Tinnefeld, in: Roßnagel (Hg.), Handbuch Datenschutzrecht, Kap. 4.1 Rdnr. 20f.; Voigt, Datenschutz bei Google, MMR 2009, 377, 379; zu einem Mittelweg zwischen objektiver und relativer Theorie tendierend Specht/Müller-Riemenschneider, ZD 2014, 71, 74.

16 Zu den weiteren Voraussetzungen an die Annahme einer Anonymisierung für den Außenstehenden durch effektive Pseudonymisierung s.u. S. 17ff.

sonstige Forschungseinrichtungen) gilt. Ohne relevante Gefährdungen der Persönlichkeitsrechte der Betroffenen wäre eine Regulierung daher als bedenklich anzusehen.[17] Ohnehin ist die Konzeption des einfachgesetzlichen Datenschutzrechts insoweit kritisch, als dass die Erlaubnisnormen materiell oft nur unscharfe Konturen aufweisen und im Ergebnis häufig zu einer nur schwer prognosefähigen und damit für den Rechtsanwender mit erheblichen Haftungs- und Bußgeldrisiken verbundenen Abwägungsentscheidung führen. Hinzu kommt, dass auch ein Ausweichen auf das Instrument der Einwilligung nicht immer zielführend erscheint, da das Einwilligungskonzept zum Beispiel im Arbeitsrecht,[18] zum Teil aber auch im Gesundheitsrecht an seine Grenzen stößt.[19] Die praktische Umsetzbarkeit des Datenschutzrechts würde daher reduziert, wenn nun neben den vergleichsweise unbestimmten Zulässigkeitstatbeständen auch noch der Personenbezug als die maßgebliche Anwendungsvoraussetzung extensiv verstanden würde. Vor diesem Hintergrund ist eine moderat antizipierte Abwägung, wie sie das Verständnis des relativen Personenbezugs bereits im Rahmen der Definition des Personenbezugs vornimmt, als sachgerecht anzusehen.

Das Konzept eines relativen Personenbezugs ist auch deshalb vorzugswürdig, weil die Persönlichkeitsrechte der Betroffenen nicht ein solch weitgehendes Verständnis des Personenbezugs gebieten, wie es die Vertreter eines absoluten Konzeptes proklamieren. Denn eine Verletzung bzw. eine Bedrohung des allgemeinen Persönlichkeitsrechts ist fernliegend, wenn nur Dritte, nicht aber die verantwortliche Stelle einen Personenbezug herstellen können.[20] Auch in dieser Hinsicht erscheint das relative Konzept daher zielführender, indem es – gekennzeichnet von einer Sphärenbetrachtung – im Wege einer Abschätzung der Risiken für das Recht auf informationelle Selbstbestimmung nicht-persönlichkeitssensible Verarbeitungsvorgänge von vornherein aus dem Anwendungsbereich des Datenschutzrechts auszuscheiden vermag. Diese relative Sichtweise führt bei konsequenter Anwendung aber auch dazu, dass eine datenschutzrechtlich relevante Übermittlung anzunehmen ist, wenn die Daten zwar nicht aus Sicht der übermittelnden Stelle, wohl aber für den Empfänger einen Personenbezug aufweisen können.[21]

Hinzu kommt, dass das Datenschutzrecht nicht nur den Zentralbegriff der personenbezogenen Daten kennt,[22] der das Schutzobjekt definiert, sondern mit der verantwortlichen Stelle auch eine Zentralfigur einführt,[23] die primär dem Schutz dieser Daten verpflichtet ist. Dies deutet darauf hin, dass auch bei der Frage, auf wessen Möglichkeiten es bei der Zuordenbarkeit eines Datums zu einer bestimmten oder bestimmbaren natürlichen Person ankommen soll, auf die jeweils betrachtete (verantwortliche) Stelle abzustellen ist.

Dies gilt nicht nur für die verantwortliche Stelle, sondern auch für den Auftragsdatenverarbeiter, welcher seine Berechtigung zum Datenumgang letztlich immer von einer

17 Ebenfalls den grundrechtlichen Schutz privater Daten verarbeitender Stellen hervorhebend Masing, NJW 2012, 2305, 2307; ähnlich Härting, NJW 2013, 2065, 2070; siehe mit Blick auf Gesundheitsdaten auch Kühling/Seidel, GesR 2010, S. 231, 231ff.

18 Vgl. dazu unten in Kap I.15, S. 328.

19 Vgl. näher zum Gesundheitsbereich etwa Kühling/Klar, DuD 2013, 791, 794f., und vor allem im Hinblick auf die Freiwilligkeit unten S. 113ff.

20 Ausführlich dazu Klar, Datenschutzrecht und die Visualisierung des öffentlichen Raums, 2012, S. 144f.

21 Zutreffend Gola/Schomerus, BDSG, § 3 Rdnr. 10 und 44a.

22 Definiert z.B. in § 3 Abs. 1 BDSG oder Art. 2 Buchst. a Datenschutzrichtlinie 95/46/EG.

23 Definiert z.B. in § 3 Abs. 7 BDSG oder (aussagekräftiger) in Art. 2 Buchst. d Datenschutzrichtlinie 95/46/EG.

verantwortlichen Stelle ableitet. Und jede Stelle, die mit personenbezogenen Daten umgeht, ist entweder verantwortliche Stelle oder Auftragsdatenverarbeiter.[24] Dies entspricht nicht nur dem Zweck eines möglichst umfassenden Datenschutzes (vgl. § 1 Abs. 1 BDSG), sondern auch den klaren Regeln zum Anwendungsbereich in § 1 Abs. 2 BDSG, die insbesondere für private Stellen nur Tätigkeiten für ausschließlich persönliche oder familiäre Zwecke ausnehmen. Die Unterteilung der Stellen, welche das Datenschutzrecht beachten müssen, in vollumfänglich (eigen-)verantwortliche Stellen einerseits (§ 3 Abs. 7 BDSG) und weisungsgebundene Auftragsdatenverarbeiter mit eingeschränkter Verantwortung andererseits (§ 11 BDSG) dient lediglich der Abgrenzung der Pflichtenkreise im Einzelnen, nicht aber der Klärung der Frage nach der grundsätzlichen Anwendbarkeit des Datenschutzrechts. Verantwortlich ist somit auch jede Stelle, welche faktisch die Verfügungsgewalt über personenbezogene Daten innehat, ohne im Sinne der Auftragsdatenverarbeitung an Weisungen eines Dritten gebunden zu sein, unabhängig davon, zu welchen Zwecken (ausgenommen ausschließlich persönliche oder familiäre), mit welchen Mitteln und ob mit oder ohne Erlaubnis diese Verfügungsmacht ausgeübt wird. Entscheidend ist allein, dass für diese Stelle ein Personenbezug besteht.

Die Bestimmung und Abgrenzung der Pflichten je nach betrachteter Stelle legt es daher nahe, dass es auch für die vorgelagerte Frage, ob überhaupt ein Personenbezug vorliegt, auf die Möglichkeiten genau dieser Stelle ankommt.

Der hier vertretenen Auffassung steht schließlich auch nicht die europäische Datenschutzrichtlinie entgegen, die nach Ansicht des EuGH eine prinzipiell vollharmonisierende Wirkung entfaltet.[25] Zwar wird in Erwägungsgrund 26 der Richtlinie hinsichtlich des Vorliegens eines Personenbezugs angedeutet, dass „alle Mittel berücksichtigt werden [sollten], die vernünftigerweise entweder von dem Verantwortlichen für die Verarbeitung oder von einem Dritten eingesetzt werden könnten". Entgegen der nicht selten vertretenen Auffassung[26] stellt dies aber nicht zwingend eine Entscheidung zugunsten der absoluten Theorie dar.[27] Denn der Erwägungsgrund zwingt nicht dazu, alle bei einem Dritten vorhandenen Mittel zu berücksichtigten, sondern

24 Dementgegen nimmt Dierks, Rechtsgutachten zur elektronischen Datentreuhänderschaft, S. 63, an, dass es Stellen geben könne, die weder verantwortliche Stelle noch Auftragsdatenverarbeiter sind und daher nicht dem Datenschutzrecht unterlägen, so beispielsweise zu einem Datentreuhänder, da dieser weder wie die verantwortliche Stelle Daten für sich selbst noch wie der Auftragsdatenverarbeiter Daten nach Weisung Dritter verarbeiten, sondern Daten für Dritte, aber nicht in Weisungsabhängigkeit von diesen, also auch nicht als Auftragnehmer im Sinne des Datenschutzrechts, verarbeite. Dies würde eine nach hier vertretener Auffassung in keiner Weise zu vertretende Regelungslücke darstellen – und zwar nicht nur vor dem Hintergrund grundrechtlicher Schutzpflichten und Drittwirkungen, sondern auch in einfachrechtlicher Hinsicht. Denn § 29 BDSG zeigt, dass auch Stellen in den Anwendungsbereich des Datenschutzrechts fallen, die Daten zwar nicht für eigene Geschäftszwecke, sondern zum Zweck der Übermittlung (an Dritte) in eigener Verantwortung verarbeiten. Auch solche Stellen erheben, verarbeiten oder nutzen personenbezogene Daten für sich selbst, wie es u.a. § 3 Abs. 7 BDSG für die verantwortliche Stelle verlangt. Dabei wird der Datenumgang einschließlich der Übermittlung selbst zum Geschäftszweck der verantwortlichen Stelle und dient nicht wie § 28 BDSG es verlangt, anderen (eigenen) Geschäftszwecken, wobei die Übermittlung nach § 29 BDSG auch den (außerhalb des reinen Datenumgang liegenden) Geschäftszwecken Dritter dient. Außerdem ist vor dem europarechtlichem Hintergrund jede Stelle, die über die Zwecke und wesentlichen Mittel des Datenumgangs bestimmen darf oder faktisch bestimmt, verantwortlich für den Datenschutz (Art. 29-Datenschutzgruppe, Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher" und „Auftragsverarbeiter", S. 10ff.).

25 Vgl. EuGH, Urt. v. 24.11.2011 – C-468/10 u.a. (ASNEF), Rdnr. 30 und 52; ausführlich dazu Kühling/Seidel, GesR 2012, 402ff., die allerdings nicht darauf eingehen, dass der EuGH, a.a.O., Rdnr. 48, ausdrücklich einen Vorbehalt gegenüber der Vollharmonisierung in Bezug auf besonders sensible Daten (darunter Gesundheitsdaten) nach Art. 8 der Richtlinie formuliert hat. Dieser Vorbehalt erstreckt sich allerdings nicht auf die vorgelagerte Frage nach dem Personenbezug, sondern nur auf den Umfang des Verbotes bzw. der Erlaubnisse, sensible personenbezogene Daten zu verarbeiten. Zum letzten Punkt s.a. unten Fn. 780.

26 Vgl. z.B. Forgó/Krügel/Müllenbach/Schütze, Gutachten Google StreetView, S. 37f.; Pahlen-Brandt, DuD 2008, 34, 37f.

27 So nun auch BGH, Beschluss v. 28.10.2014 – VI ZR 135/13, CR 2015, 109, Rdnr. 28. Dazu ausführlich Klar, Datenschutzrecht und die Visualisierung des öffentlichen Raums, 2012, S. 145.

nur diejenigen, die „vernünftigerweise“ eingesetzt werden könnten. Und die vernünftigerweise durch den Dritten einsetzbaren Mittel sind seitens der verantwortlichen Stelle auch im Rahmen eines relativen Verständnisses grundsätzlich zu berücksichtigen, nämlich dann, wenn die Daten an den Dritten übermittelt werden.[28]

2.2 Relativität des Personenbezugs in objektiver Hinsicht

Kommt es damit hinsichtlich der Frage, ob ein Personenbezug vorliegt, nach zutreffender Auffassung auf die jeweilige datenverarbeitende Stelle an, ist daran anknüpfend zu klären, welche Anforderungen in objektiver Hinsicht an den Personenbezug zu stellen sind, d.h. auf welche Möglichkeiten der Re-Identifizierung es in sachlicher Hinsicht ankommt, um einen Personenbezug annehmen bzw. ablehnen zu können. Nach dem in § 3 Abs. 6 BDSG zum Ausdruck gebrachten Willen des Gesetzgebers soll es für eine Anonymisierung ausreichen, wenn Angaben nicht mehr (absolute Anonymisierung) oder jedenfalls nur mit unverhältnismäßig großem Aufwand an Zeit, Kosten und Arbeitskraft einer Person zugeordnet werden können (faktische Anonymisierung).

In der Kommentarliteratur wird zu den Anforderungen an eine hinreichende Anonymisierung überwiegend vertreten, dass diese dann vorliegen soll, wenn die Herstellung des Personenbezugs überhaupt nicht mehr möglich ist oder eine Deanonymisierung zumindest unter normalen Bedingungen ausscheidet.[29] Als Folge hiervon wird angenommen, dass nach § 3 Abs. 6 BDSG anonymisierte Daten auch keine personenbezogenen Daten im Sinne von Abs. 1 dieser Vorschrift mehr darstellen und damit aus dem Anwendungsbereich des Datenschutzrechts ausscheiden.[30] Dies entspricht auch dem natürlichen Wortverständnis, das anonyme Daten nicht als personenbezogen ansieht.[31]

2.2.1 Datenschutzrechtliche Anforderungen an eine faktische Anonymisierung

Hinsichtlich der Frage, ab wann der für eine Re-Identifizierung nötige Aufwand als unverhältnismäßig anzusehen ist, enthält die Vorschrift des § 3 Abs. 6 BDSG keine näheren Anhaltspunkte und überantwortet eine weitere Interpretation dieses unbestimmten Rechtsbegriffs dem Rechtsanwender.[32]

28 In diese Richtung geht auch BGH, Beschluss v. 28.10.2014 – VI ZR 135/13, CR 2015, 109, Rdnr. 28. Vgl. oben Fn. 21. Gleiches gilt, wenn die „Mittel“ des Dritten (wie eine einschlägige Vorschrift zur Pseudonym-Personen-Zuordnung) an die betrachtete Stelle übertragen werden.

29 Vgl. nur Gola/Schomerus, BDSG, § 3 Rdnr. 44.

30 Bergmann/Möhrle/Herb, BDSG, § 3 Rdnr. 18 und 130; Dammann, in: Simitis (Hg.), BDSG, § 3 Rdnr. 23 (anders noch in der 6. Auflage von 2006); Gola/Schomerus, BDSG, § 3 Rdnr. 44; Polenz, in: Kilian/Heussen (Hg.), Computerrecht, Rechtsquellen und Grundbegriffe des allgemeinen Datenschutzes, Teil 13 Rdnr. 77; Roßnagel/Scholz, MMR 2000, 721; Scheja/Haag, in: Leupold/Glossner (Hg.), Münchener Anwaltshandbuch IT-Recht, 2. Aufl. 2011, Teil 4. E Rdnr. 40; Wuermeling, Scoring von Kreditrisiken, NJW 2002, 3508, 3509.

31 Auch wenn dies nach dem Verhältnis der juristischen Definitionen des Personenbezugs in § 3 Abs. 1 und der Anonymisierung in § 3 Abs. 6 BDSG nicht ganz eindeutig ist.

32 Auch insoweit existiert leider nicht immer eine einheitliche Aufsichtspraxis. Exemplarisch seien hier die auseinandergehenden Positionen zur Anonymisierung von Rezeptdaten durch Apothekenrechenzentren genannt: Hier legt beispielsweise das Unabhängigen Landeszentrum für Datenschutz in Schleswig-Holstein strengere Maßstäbe an (https://www.datenschutzzentrum.de/medizin/gkv/20131028-weichert-rezeptdaten.html) als das Landesamt für Datenschutzaufsicht in Bayern (http://www.lda.bayern.de/lda/datenschutzaufsicht/ p_archiv/2013/pm005.html).

Davon ausgehend wird man im Einzelnen bei der Prüfung der (Un-)Verhältnismäßigkeit des Referenzierungsaufwands zutreffenderweise eine Wahrscheinlichkeitsbetrachtung vornehmen müssen,[33] die eine individuelle Risikoanalyse voraussetzt.[34] Eine absolute Sicherheit dahingehend, dass der Personenbezug nicht (wieder) hergestellt werden kann, ist nicht zu verlangen, da dann eine absolute Anonymisierung vorläge. Als ausreichender Maßstab wird hier vielmehr jedenfalls das allgemeine (prozessuale) Beweismaß anzusehen sein, d.h. üblicherweise die an Sicherheit grenzende Wahrscheinlichkeit, welche auch sonst der Rechtsordnung genügt.[35] Somit wäre von einem Personenbezug auszugehen, wenn die praktische Vernunft entsprechenden Zweifeln nicht Schweigen gebietet.[36]

Ob eine Deanonymisierung voraussichtlich erfolgen wird, hat sich auch daran zu messen, ob die datenhaltende Stelle ein hinreichendes Deanonymisierungsinteresse hat. Dabei ist insbesondere zu berücksichtigen, inwiefern sich hieraus ein wirtschaftlicher Nutzen für sie ergeben kann, der auch einen hohen finanziellen Aufwand als gerechtfertigt erscheinen lässt.[37] Bloß theoretische, ganz entfernt liegende Möglichkeiten sind indes nicht zu berücksichtigen.

Dies spricht dagegen, eine Möglichkeit der Re-Identifizierung nur unter Verstoß gegen ein Gesetz als beachtenswert anzusehen.[38] Allerdings wird man hier die tatsächlichen Sanktionsrisiken nicht ganz außer Acht lassen können.[39] Je üblicher das inkriminierte Handeln, je geringer die Entdeckungswahrscheinlichkeit und je weniger scharf die drohende Sanktion ist, desto eher wird man auch solche Möglichkeiten berücksichtigen müssen.[40]

Dabei spielt es im Grundsatz keine Rolle, wenn bloß nicht ausgeschlossen werden kann, dass eine Deanonymisierung irgendwann zu einem späteren, nicht exakt vorhersehbaren Zeitpunkt möglich sein wird, da andernfalls die eigene datenschutzrechtliche Kategorie der faktischen Anonymisierung praktisch überflüssig würde.[41] Ein Personenbezug ist folglich erst dann anzunehmen, wenn eine Deanonymisierung (wieder) mit verhältnismäßigen Mitteln erreicht werden kann.

Eine andere Auslegung würde kaum Anreize für eine Anonymisierung von Daten erzeugen, was auch rechtspolitisch nicht wünschenswert erschiene.[42] Ferner gilt, dass ein derart restriktives Verständnis auch mit Blick auf einen wirksamen Schutz des

33 Vgl. Roßnagel, NZV 2006, 281, 282; ähnlich auch ders./Scholz, MMR 2000, 721, 724; vgl. dazu auch Dammann, in: Simitis (Hg.), BDSG, § 3 Rdnr. 23; ferner Klar, Datenschutzrecht und die Visualisierung des öffentlichen Raums, S. 151.

34 Dammann, in: Simitis (Hrsg.), BDSG, § 3 Rdnr. 23.

35 Vgl. Nell, Wahrscheinlichkeitsurteile in juristischen Entscheidungen, S. 93ff. m.w.N.

36 Vgl. insoweit auch Erwägungsgrund 26 der Datenschutzrichtlinie 95/46/EG, der vorsieht, dass „alle Mittel berücksichtigt werden [sollten], die vernünftigerweise entweder von dem Verantwortlichen für die Verarbeitung oder von einem Dritten eingesetzt werden könnten, um die betreffende Person zu bestimmen". S.a. oben S. 16.

37 Gola/Schomerus, BDSG, § 3 Rdnr. 44; a.A. Weichert, in: Däubler/Klebe/Wedde/Weichert, BDSG, 3. Aufl. 2010, § 3 Rdnr. 47; Pahlen-Brandt, DuD 2008, 34, welche die „Relativität" des Personenbezugs ablehnen.

38 Scholz, in: Simitis (Hg.), BDSG, § 3 Rdnr. 217a, der nur „jeweils (legal) verfügbares Zusatzwissen" berücksichtigt.

39 Differenzierter auch: Dammann, in: Simitis (Hg.), BDSG, § 3 Rdnr. 28.

40 So wird man kaum mit einem Verbrechen (Freiheitsstrafe im Mindestmaß ein Jahr, § 12 Abs. 1 StGB) wie einem Raub (§ 249 StGB) rechnen müssen, mit einem einfacheren Vergehen wie dem Diebstahl (§ 242 StGB) aber schon eher, jedenfalls wenn man es dem Dieb durch Herumliegenlassen von Schlüsseln etc. leicht macht; s. dazu auch unten S. 49 zur Frage des Offenbarens von Patientengeheimnissen durch Unterlassen von Sicherheitsvorkehrungen.

41 Ebenso Meyerdierks, MMR 2009, 9, 11; a.A. Weichert, in: Däubler/Klebe/Wedde/Weichert, BDSG, § 3 Rdnr. 15; Pahlen-Brandt, K&R 2008, 288, 290. Dies könnte auch für den Fall der Verschlüsselung gelten, die ähnlich wie die Pseudonymisierung auf Umkehrbarkeit, wenn auch nur für Eingeweihte, angelegt ist; s. dazu aber auch den differenzierenden Ansatz von Hermeler, Rechtliche Rahmenbedingungen der Telemedizin, S. 152ff., und unten S. 260ff., vor allem Fn. 772.

42 Zu diesem Anliegen zuletzt eingehend Härting, NJW 2013, 2065ff.

Persönlichkeitsrechts im Regelfall nicht zwingend geboten erscheint. Denn in dem Moment, in dem die zuvor anonymen Daten wieder einer Person zuordenbar sind, findet das Datenschutzrecht ohnehin wieder Anwendung, sodass im Regelfall keine dogmatische Lücke im System des Datenschutzes entstehen würde.[43] Hinzuweisen ist auch darauf, dass die Datenbestände mit fortschreitendem Zeitablauf in der Regel ohnehin entsprechend an Aktualität verlieren, d.h. die persönlichkeitsrechtliche Relevanz selbst im Fall einer künftigen Deanonymisierung deutlich reduziert sein dürfte.

Im Rahmen der antizipierten Abwägung, welche – wie oben ausgeführt – u.a. für die Relativität des Personenbezugs in subjektiver Hinsicht spricht,[44] wird allerdings in objektiver Hinsicht zu berücksichtigen sein, dass im speziellen Fall der Verarbeitung von Gesundheitsdaten etwas strengere Anforderungen an die Annahme einer (faktischen) Anonymisierung (d.h. der Unverhältnismäßigkeit der Re-Identifizierung) zu stellen sein dürften. Denn das BDSG stellt besondere Arten personenbezogener Daten im Sinne von § 3 Abs. 9 BDSG, darunter Gesundheitsdaten, in Umsetzung von Art. 8 der Datenschutzrichtlinie 95/46/EG unter besonderen Schutz. Gleiches gilt für die anderen anwendbaren deutschen Rechtsgrundlagen, also die Datenschutzvorschriften der Bundesländer und der Kirchen. Insoweit dürfte auch bei der Frage des Personenbezugs bzw. im Rahmen der Prüfung der Verhältnismäßigkeit des Deanonymisierungsaufwands ein etwas schärferer Maßstab gelten. Bereits nach allgemeinen Grundsätzen sind für die Annahme eines Personenbezugs an die Wahrscheinlichkeit einer Deanonymisierung umso geringere Anforderungen zu stellen, je gravierender das Ausmaß einer tatsächlichen Re-Identifikation und damit eines „Schadens" an den Rechtsgütern des Betroffenen wäre. Gerade bei Daten zu chronischen Krankheiten mit ihrer im Zweifel lebenslangen Gültigkeit und insbesondere bei Gendaten mit ihrer definitiv lebenslangen Gültigkeit[45] sollten daher die im Bewertungszeitpunkt schon konkreter absehbaren Entwicklungen bzw. Re-Identifizierungsmöglichkeiten der näheren Zukunft Berücksichtigung finden.

Ob ein Zuordnungsschlüssel wie bei der Pseudonymisierung vorhanden ist oder nicht, ist damit nicht allein maßgeblich für die Einschätzung, ob faktische oder absolute Anonymität vorliegt.[46] Es ist auch die Möglichkeit der Re-Identifizierung ohne einen solchen Schlüssel durch einen Vergleich mit dem Zusatzwissen, welches für die datenhaltende bzw. datenempfangende Stelle verfügbar ist, in Betracht zu ziehen.[47]

---

43 Möglicherweise kann es aber zu einer pragmatischen Schutzlücke kommen, denn wenn zuvor die – dann noch als anonym, also nicht personenbezogenen anzusehenden – Daten frei zirkulieren dürfen, haben der Betroffene und die ursprünglich verantwortliche Stelle unter Umständen keine Kontrolle mehr, wo sich „ihre Daten" in dem Moment befinden, in dem der Personenbezug (wieder) herstellbar ist. Auch dieser Aspekt spricht für eine gewisse Risikovorsorge für den Fall, dass doch eine Re-Identifizierung wieder mit vertretbarem Aufwand möglich wird.

44 S. oben S. 15.

45 Gendaten verfügen zudem über einen Aussagewert zu Blutsverwandten, insbesondere den Nachkommen, auch über das eigene Leben hinaus. Diese Daten lassen sich ohnehin nur schwer anonymisieren. Bei genetischen Proben, Daten der vollständig sequenzierten DNS oder auch nur der Nukleotid-Sequenz eines längeren DNS-Abschnittes wird dies überhaupt nicht möglich sein. Letzteres gilt insbesondere, wenn dort nicht-codierende bzw. exprimierende Sequenzen, mit ihrer mangels biologischen Selektionsdrucks hohen Varianz und Identifizierungswirkung, und codierende/exprimierende, also Merkmale des Individuums festlegende Gene gemeinsam auftreten. Gleiches gilt für das Genom oder längere Zusammenstellungen individueller genetischer Ausprägungen (auch abstrakt-funktional, also unabhängig von den Nukleotidsequenzen als materielle Träger). Zum Gendatenschutz s.a. unten S. 53ff.

46 Bei Vorhandensein eines Zuordnungsschlüssels besteht aber sicher Personenbezug für die Stelle, welche Zugriff auf diesen hat. Im Übrigen ist die angesprochene Risikobewertung vorzunehmen, wobei das Risiko im Allgemeinen bei Nichtvorhandensein eines solchen Schlüssels, also wenn eine Re-Identifizierung nur über Mustervergleich möglich wäre und nicht über Kompromittierung des Schlüssels, geringer einzustufen ist, wenn auch nicht von vornherein komplett ausgeschlossen werden kann.

47 Beispielsweise über Quasi-Identifikatoren, s. dazu sogleich unten S. 20ff.

2.2.2 Methoden der Anonymisierung

Eine Anonymisierung, sowohl eine faktische, aber auch – erst recht – eine absolute, setzt zunächst die Entfernung unmittelbarer Identifikationsmerkmale wie Namen und Anschriften aus einem Datensatz voraus.[48]

Auf die Identität des Betroffenen kann jedoch nicht selten auch mittelbar über andere Merkmale eines Datensatzes (sogenannte Quasi-Identifikatoren) geschlossen werden. Ist ein solcher Schluss noch mit verhältnismäßigem Aufwand möglich, liegt – wie gesehen – noch Bestimmbarkeit und damit ein Personenbezug vor. Eine Anonymisierung muss also gewährleisten, dass ein entsprechender Rückschluss nicht mehr oder nicht mehr mit verhältnismäßigem Aufwand möglich ist. Hierfür ist an den Quasi-Identifikatoren anzusetzen und diese sind entweder zu aggregieren (generalisieren), zu rekombinieren (data swapping) oder auszudünnen (zu eliminieren); daneben können auch in kontrollierter Weise Zufallsfehler in einen Datenbestand eingebracht werden.[49]

Exemplarisch sei zu den möglichen Faktoren und Methoden der Anonymisierung Folgendes ausgeführt:

2.2.2.1 Quasi-Identifikator

Ein Quasi-Identifikator ist ein Merkmal (z.B. Alter, Geschlecht oder PLZ), welches selbst eine Person nicht eindeutig identifizieren kann, aber mit dieser Person so in Beziehung steht, dass dieses Merkmal in Kombination mit anderen Quasi-Identifikatoren diese Person eindeutig identifizieren kann. Dies soll anhand Tabelle 1 veranschaulicht werden.

Tab. 1 Beispiel Quasi-Identifikatoren

Name	Alter	Geschlecht	PLZ
Hans Albers	45	M	12345
Eva Fleck	28	W	67890
Max Bräutigam	45	M	67890
Berta Roos	28	W	12345

In dieser Tabelle ist nur das Merkmal „Name" ein echter Identifikator. Bei den Merkmalen „Alter", „Geschlecht" und „PLZ" handelt es sich um Quasi-Identifikatoren, da es nach Entfernen des Merkmals „Namen" möglich ist, zumindest eine Person in der Tabelle anhand der Merkmale „Alter", „Geschlecht" und „PLZ" eindeutig zu identifizieren.

Soweit eine (Behandlungs-)Einrichtung bereits über personenbezogene Gesundheitsdaten als Vergleichsbasis bzw. sogenanntes Zusatzwissen verfügt, das für einen Mustervergleich mit einem überlassenen mehr oder weniger anonymisierten Daten-

48 Allgemein zu diesen Methoden: Dammann, in: Simitis (Hg.), BDSG, § 3 Rdnr. 205ff. m.w.N. Zur datenschutzrechtlichen Bewertung des Vorgangs des Anonymisierens im Übrigen (also der Frage nach dem Erlaubnisvorbehalt) s.u. S. 251f.

49 S.a. Hauf, K-Anonymity, l-Diversity and T-Closeness, S. 14: Dataswapping, Ading Noise (Fehlinformation), Generalisierung oder Suppression durch Elimination.

bestand anderer Einrichtungen in Betracht kommt, können auch die medizinischen Daten als Quasi-Identifikatoren herangezogen werden.

2.2.2.2 *k*-Anonymität und *k*-Anonymisierung

Ein mögliches Maß zur Messung der Re-Identifizierbarkeit anhand von Quasi-Identifikatoren ist die *k*-Anonymität. Ein Datentableau ist k-anonym, wenn jeder Datensatz in der entsprechenden Tabelle von mindestens *k*-1 anderen Datensätzen in Bezug auf die Quasi-Identifikatoren nicht zu unterscheiden ist.[50] Dies soll anhand Tabelle 2 veranschaulicht werden.

Tab. 2 Beispiel für eine 2-anonyme Tabelle[51]

	PLZ	Alter	Geschlecht	Diagnose
1	130**	< 30	*	Hepatitis
2	130**	< 30	*	Pneumonie
3	148**	≥ 40	*	Krebs
4	148**	≥ 40	*	Pneumonie
5	130**	3*	*	Krebs
6	130**	3*	*	Krebs

Diese Tabelle ist bezüglich der Quasi-Identifikatoren „PLZ", „Alter" und „Geschlecht" 2-anonym. Es ist also nicht mehr möglich, eine Person anhand dieser drei Merkmale eindeutig zu identifizieren; die jeweils genannte Diagnose könnte auch auf mindestens eine andere aufgeführte Person zutreffen.

Die *k*-Anonymisierung ist ein Verfahren zur Herstellung einer bestimmten *k*-Anonymität einer Datensammlung. In einer *k*-anonymisierten Datensammlung kommt jede Merkmalskombination, die zur Re-Identifizierung eines Betroffenen genutzt werden kann, in mindestens *k* Datensätzen vor.[52] Ein Beispiel für eine solche Merkmalskombination sind die Merkmale Geschlecht, Geburtsdatum und Postleitzahl. Für sich genommen kann keiner dieser Quasi-Identifikatoren genutzt werden, um eine Person eindeutig zu identifizieren. Werden diese Merkmale allerdings miteinander kombiniert, können Personen unter Umständen mit einer recht hohen Wahrscheinlichkeit identifiziert werden. So wird zum Beispiel angeführt, dass etwa 87% der US-Amerikaner anhand dieser Merkmalskombination eindeutig identifiziert werden können.[53]

50 Eder/Ciglic/Koncilia, ANON: Ein Tool zur Anonymisierung medizinischer Daten. Vortrag auf dem TMF-Jahreskongress 2013, Folie. 5.

51 In Anlehnung an Eder/Ciglic/Koncilia, ANON: Ein Tool zur Anonymisierung medizinischer Daten. Vortrag auf dem TMF-Jahreskongress 2013, Folie 5.

52 TMF, TMF Jahresbericht 2013, S. 113.

53 Sweeney, Simple Demographics Often Identify People Unique; wo allerdings der in den USA sehr einfache Rückgriff auf die Listen registrierter Wähler zugrunde gelegt wurde (S. 2), welche die entsprechenden Vergleichsdaten zu den quasi-identifizierenden Merkmalen enthalten. In der BRD sind die entsprechenden Daten in den Melderegistern enthalten, auf welche nicht ohne Weiteres massenhaft zugegriffen werden kann; im Einzelfall bekommt man aber auch hier Auskunft, wenn man ein berechtigtes Interesse darlegt; z.B. die politischen Parteien können zudem auch hier vollständige Listen mit den Daten wahlberechtigter Bürger anfordern, wenn diese dem nicht widersprochen haben. Somit dürfte die Identifizierungswahrscheinlichkeit in der BRD zwar geringer, eine Re-Identifizierung aber auch hier keineswegs ausgeschlossen sein. Jedenfalls solange Parteien oder Meldeämter nicht Empfänger der mehr oder weniger anonymisierten Daten sind und diese auch nicht veröffentlicht werden, muss diese Re-Identifizierungsmöglichkeit jedoch nicht zwingend in die Betrachtung einbezogen werden und keinesfalls zwingend zur Annahme eines Personenbezugs führen. Im Gesundheitswesen wird man aber die Möglichkeit zum Abgleich mit den in den verschiedenen beteiligten Einrichtungen vorhandenen Stammdaten der Patienten in Betracht ziehen müssen.

2.2.2.3 *l*-Diversität, Zufallsfehler und Restrisiken

Auch wenn eine Datensammlung *k*-anonym ist, kann es möglich sein, auf ein bestimmtes Merkmal zu schließen. Dies gilt auch für sensitive Merkmale einer Person, etwa wenn alle Personen in einer Gruppe mit den gleichen Quasi-Identifikatoren an der gleichen Krankheit leiden. So kann beispielsweise in Tabelle 2 darauf geschlossen werden, dass die gesuchte Person an Krebs leidet, wenn bekannt ist, dass diese erkrankt ist, zwischen 30 und 39 Jahren alt ist und im PLZ-Bereich 130** wohnt.

Doch selbst wenn dies nicht der Fall ist, da die Datensammlung auch *l*-divers ist, also jede Personengruppe für jedes sensitive Merkmal mindestens *l* wohldefinierte Werte (z.B. unterschiedliche Krankheiten) beinhaltet,[54] kann es möglich sein, bestimmte Aussagen über eine Person zu treffen, etwa dass diese an irgendeiner (schweren) Krankheit leidet, wenn auch ohne weitere Details.[55] Beispielsweise ist in Tabelle 2 bei einem Alter unter 30 zwar kein Rückschluss auf die genaue Erkrankung möglich, es kann aber zumindest die Aussage getroffen werden, dass die Person an einer nicht ganz leichten Krankheit (Hepatitis oder Pneumonie) leidet.

Dieses Risiko kann verringert werden, indem eine Kontrollgruppe mit gesunden Personen der Datensammlung hinzugefügt wird (Zufallsfehler).[56] Soweit jedoch noch überwiegend kranke Personen in ihr enthalten sind, können aus der Feststellung der bloßen Zugehörigkeit einer Person zur untersuchten Population, deren Daten gesammelt wurden, mit gewisser (überwiegender) Wahrscheinlichkeit Rückschlüsse darauf gezogen werden, dass diese Person erkrankt ist.[57]

Trotz *k*-Anonymität und *l*-Diversität ist daher mit entscheidend, dass es möglichst unwahrscheinlich ist, dass von den Quasi-Identifikatoren mittels Zusatzwissen überhaupt auf tatsächliche Identifikatoren und damit auf eine Person oder überschaubare Gruppe von Personen geschlossen werden kann. Als solches Zusatzwissen könnten z.B. bei einem Datenempfänger aus dem medizinischen Bereich (wie einer forschenden Klinik) die dort vorhandenen Patientenstammdaten fungieren.

Allerdings kann durch eine Kombination der Ausdünnung von Quasi-Identifikatoren mit *k*-Anonymität, *l*-Diversität und Zufallsfehlern ein sehr hoher Schutz gegenüber der Re-Identifizierung von Daten erreicht werden.[58] Entscheidend für die Anonymität ist es, *k*, *l* und die Anzahl der Zufallsfehler möglichst groß zu wählen, um die

54 Eder/Ciglic/Koncilia, ANON: Ein Tool zur Anonymisierung medizinischer Daten. Vortrag auf dem TMF-Jahreskongress 2013, S. 5.

55 Wenn man das Attribut „schwer krank" oder auch nur „krank" einer bestimmten Person zuordnen könnte, läge schon ein personenbezogenes Gesundheitsdatum vor; auf medizinische Details kommt es dafür nicht an. Zur Problematik der entspr. semantischen Ähnlichkeit verschiedener (*l*-diverser) Attributwerte auch knapp Hauf, K-Anonymity, l-Diversity and T-Closeness, S. 16.

56 Eder, k-Anonymität und l-Diversität bieten sicheren Schutz vor dem Ausspionieren personenbezogener Daten.

57 In § 28b BDSG werden Wahrscheinlichkeitswerte im Rahmen des Scoring explizit als personenbezogene Daten anerkannt. Entspr. im Umfeld des Data Mining: Dammann, in: Simitis (Hg.), BDSG, § 3 Rdnr. 72 m.w.N. Auch Aussagen, die auf statistischen Durchschnittswerten beruhen, sind personenbezogene Daten, wenn sie auf die Einzelperson durchschlagen, Gola/Schomerus, § 3 Rdnr. 3 u.a. unter Bezug auf BAG, Urt. v. 26.07.1994 – 1 ABR 6/94, RDV 1995, 29. Zu restriktiv dagegen Saeltzer, DuD 2004, 218, 225f., der am Beispiel der Videoüberwachung, aber mit Anspruch auf Verallgemeinerung, noch bei einer Identifizierungswahrscheinlichkeit kleiner oder gleich 50% von fehlendem Personenbezug ausgeht. Trotz der von Saeltzer dargestellten interessanten informationstheoretischen Ansätze ist diese starre und recht hohe Grenze nicht haltbar (krit. gegenüber Saeltzer auch Hornung, DuD 2004, 429; allg. krit. gegenüber fixen Grenzwerten Nell, Wahrscheinlichkeitsurteile in juristischen Entscheidungen, S. 109ff.). Dies wird schon dadurch deutlich, dass beispielsweise ein Privatversicherer auch bei „nur" 25% Wahrscheinlichkeit für eine schwere Erkrankung beim Antragsteller bzw. der 25%-igen Wahrscheinlichkeit, dass dieser zu einer Gruppe von schwer erkrankten Personen gehört, in aller Regel für die private Lebens- oder Berufsunfähigkeitsversicherung nennenswerte Beitragsaufschläge verlangen, Risikoausschlüsse vereinbaren oder die Deckung ablehnen würde.

58 Eder, k-Anonymität und l-Diversität bieten sicheren Schutz vor dem Ausspionieren personenbezogener Daten.

Wahrscheinlichkeit einer validen Eigenschaftszuschreibung an eine re-identifizierte Person aus der untersuchten Population möglichst gering zu halten. Hierbei besteht jedoch ein gewisses Spannungsverhältnis zur Erhaltung einer validen Datenbasis für (wissenschaftliche) Auswertungen.

Letztlich wird man jedenfalls bei komplexeren Datenstrukturen und Erhaltung eines Einzelfallbezugs, also ohne weitreichende Aggregierung, trotz *k*-Anonymität, *l*-Diversität und Zufallsfehlern eher selten absolute Anonymität, sondern in den meisten Fällen nur, aber immerhin faktische Anonymität erreichen können.

2.2.3 Empfehlungen zur Risikovorsorge

Bei lediglich faktischer Anonymisierung bleibt somit die Möglichkeit der Re-Identifizierung erhalten, wenn auch nach derzeitiger Einschätzung nur mit unverhältnismäßigen Mitteln. Die zur Verfügung stehenden Mittel können sich jedoch mit der Zeit ändern, z.B. aufgrund erschwinglicherer Kapazitäten von Großrechnern oder einer erleichterten Zusammenschaltung von (Grid-)Rechnern, sodass ein ursprünglich unverhältnismäßiger Aufwand verhältnismäßig werden kann. Ab diesem Zeitpunkt läge dann wieder ein Personenbezug vor mit der Folge, dass die über die Daten verfügende Stelle wieder verantwortliche Stelle im Sinne des Datenschutzrechts würde und sich, wenn keine entsprechende Erlaubnis vorliegt, Sanktionsrisiken ausgesetzt sähe.

Gegenüber diesen Restrisiken einer Re-Identifizierung bei faktisch anonymen Daten empfiehlt sich daher eine gewisse Vorsorge.[59] So könnten beispielsweise bestimmte technisch-organisatorische Sicherheitsmaßnahmen getroffen werden, vor allem gegen einen Datenzugriff von außen.[60] Ein Verbot mit Erlaubnisvorbehalt besteht für den Umgang mit faktisch anonymen Daten jedoch nicht.

Bei Übertragung faktisch anonymer Daten an andere Stellen sollten allerdings das bei diesen möglicherweise vorhandene Zusatzwissen oder sonstige Re-Identifizierungsmöglichkeiten eingeschätzt werden. Denn diese könnten zu einer Re-Identifizierbarkeit mit verhältnismäßigem Aufwand und damit zum Wiederaufleben des Personenbezugs sowie letztlich zum Vorliegen einer rechtfertigungsbedürftigen Übermittlung führen.[61] Eine entsprechende Einschätzung sollte auch die empfangende Stelle vornehmen, damit sich aus einer möglichen Zusammenführung mit bei ihr bereits vorhandenen Datenbeständen kein doch wieder personenbezogener Datenumgang ergibt. Die übertragende Stelle könnte sich durch vertragliche Verpflichtungen des Datenempfängers weiter absichern, welche Re-Identifizierungsverbote und gewisse technisch-organisatorische Schutzmaßnahmen einschließen.[62] Beim Outsourcing des Datenumgangs auf technische Dienstleister bietet sich der Abschluss von Vereinbarungen mit diesen analog zu den Regeln der Auftragsdatenverarbeitung an.

59 S.a. unten S. 265

60 Auch wenn diese Sicherheitsmaßnahmen keineswegs so umfassend sein müssen wie diejenigen nach den für personenbezogene Daten einschlägigen Datenschutzgesetzen (z.B. § 9 BDSG), welche für faktisch anonyme Daten nicht gelten. Eine gewisse Orientierung an den entsprechenden Regelungen bietet sich gleichwohl an.

61 Dammann, in: Simitis (Hg.), BDSG, § 3 Rdnr. 211; Gola/Schomerus, BDSG, § 3 Rdnr. 44a. Dammann entwickelt, a.a.O., § 3 Rdnr. 36, zudem die weitergehende Idee einer Kategorie von potenziell personenbezogenen Daten und präventiven Schutzpflichten; kritisch demgegenüber Härting, NJW 2013, 2065, 2066.

62 Denkbar, wenn auch weniger wichtig, wäre eine interne Selbstbindung hinsichtlich der Verwendungszwecke (z.B. für die wissenschaftliche Forschung im Allgemeinen), welche auch auf den Datenempfänger erstreckt werden könnte.

2.3 Ergebnis

Damit ist im Ergebnis festzuhalten, dass der Beurteilung des Personenbezugs nach zutreffender Ansicht ein relatives Verständnis zugrunde zu legen ist. Werden von einer verantwortlichen Stelle pseudonymisierte Daten ohne Mitteilung der Zuordnungsliste an einen Dritten weitergegeben, so bedeutet dies in der Konsequenz, dass diese Daten für den Empfänger grundsätzlich als anonym anzusehen sind, sofern *dieser* die Daten nicht mit verhältnismäßigem Aufwand einer natürlichen Person zuordnen kann. Die Datenweitergabe durch die verantwortliche Stelle an den Empfänger stellt dann keine „Übermittlung" im Sinne des Datenschutzrechts dar, sodass die verantwortliche Stelle auch keinen die Datenweitergabe legitimierenden Erlaubnistatbestand benötigt. Allerdings muss bei der Weitergabe der Daten die Entschlüsselungsfähigkeit des Empfängers evaluiert werden. Ist mit dieser zu rechnen, d.h. kann dieser mit verhältnismäßigem Aufwand eine Re-Identifizierung vornehmen, unterliegt sowohl der Übermittlungsvorgang als auch jeglicher Datenumgang durch den Empfänger dem Datenschutzrecht. Dabei ist zu berücksichtigen, dass die Anforderungen an die Wahrscheinlichkeit einer Deanonymisierung durch den Datenempfänger speziell im Bereich von Gesundheitsdaten mit langer Gültigkeit niedriger sind, also die Effektivität der eingesetzten Anonymisierungs- bzw. Pseudonymisierungsverfahren besonders hoch sein muss. Zudem kann es sich im Sinne einer Vorsorge gegenüber der Realisierung verbleibender Restrisiken der Re-Identifizierung empfehlen, zusätzliche technische und organisatorische Sicherungsvorkehrungen zu treffen sowie Datenschutzklauseln in Verträge mit den Datenempfängern aufzunehmen.