Gegenstandes für die gesamte Laufzeit des Vertrages sicherzustellen, verfängt nicht. Denn aufgrund der in Ziff. 12 der Allgemeinen Geschäftsbedingungen der Klägerin erfolgten Abtretung sämtlicher Ansprüche an den Beklagten, kann dieser von der Lieferantin, der Wish4 Web GBR, die dauerhafte Gebrauchsüberlassung des Softwareprogramms bzw. den hierfür nötigen Online-Zugang einfordern. (...)

Das LG führt ferner zu Recht aus, dass der Leasingnehmer dem Leasinggeber als Nichterfüllungsschaden den Betrag zu ersetzen habe, den er bei ungestörter Abwicklung des Vertragsverhältnisses hätte zahlen müssen, gemindert um ersparte Aufwendungen und andere infolge der Kündigung erwachsende Vorteile des Leasinggebers (BGH, Urt. v. 29.6.1983 – VIII ZR 141/82, WM 1983, 931 ff. = juris Rz. 25 und 29; BGH, Urt. v. 29.6.1985 – VIII ZR 148/84, BGHZ 95, 39 ff. = juris Rz. 32, 58–60). Zwischen den Parteien steht außer Streit, dass sich der der Klägerin entstandene Schaden, nach Abzug der Finanzierungskosten, der Verwaltungskosten und des Gewinnanteils unter Berücksichtigung geleisteter Zahlungen auf einen Betrag von 27.669,70 € beläuft. (...)

Daten und Sicherheit

Aufsätze

Gerrit Hornung / Bernd Wagner*

Der schleichende Personenbezug

Die Zwickmühle der Re-Identifizierbarkeit in Zeiten von Big Data und Ubiquitous Computing

Das Vorliegen personenbezogener Daten ist die zentrale Frage der Anwendbarkeit des Datenschutzrechts. Hierbei kann die Re-Identifizierbarkeit von Daten Verantwortliche vor erhebliche Probleme stellen – wenn sie überraschend und schlagartig, noch mehr aber wenn sie schleichend auftritt. Das geltende Datenschutzrecht adressiert dieses Problem nicht explizit, so dass Datenverarbeiter vor erheblichen Rechtsunsicherheiten stehen. Technische und rechtliche Präventionsmaßnahmen können die Probleme mildern, aber nicht aufheben. Je nach weiterer technischer Entwicklung könnte deshalb der europäische Gesetzgeber zeitnah aufgerufen sein, das Problem der „gerade so" personenbezogenen Daten durch entsprechende Vorsorgeregelungen anzugehen.

I. Geklärte und offene Fragen des Personenbezugs

1 Für die Anwendbarkeit des Datenschutzrechts ist das Vorliegen personenbezogener Daten von entscheidender Bedeutung. In sehr vielen Fällen ist eindeutig, dass ein solcher Personenbezug besteht.[1] In Grenzbereichen herrscht jedoch weder über die anzuwendenden Kriterien, noch über die konkreten Lösungen Einigkeit. Dies lässt sich insbesondere am Beispiel der IP-Adressen zeigen. Die Frage des Personenbezugs hat hier nicht nur eine kaum noch zu überschauende (und vielfach redundant geführte) Diskussion,[2] sondern auch Entscheidungen des EuGH[3] und des BGH[4] hervorgebracht.

2 Mit diesen Urteilen dürfte die Diskussion für den konkreten Fall, nicht aber generell beendet sein, weil die Konstellationen in der Praxis sehr heterogen sind und deshalb im Einzelfall beurteilt werden muss, welche Mittel „von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren" (ErwGr 26 S. 3 DSGVO, s.u. III. 2).

Ein bislang wenig durchdrungenes Problem ist, dass Identifiziertheit und Identifizierbarkeit einerseits, Anonymität anderseits keine statischen Zustände sind, sondern sich je nach den Umständen dynamisch entwickeln können.[5] Zwar finden sich in der Literatur immer wieder Warnungen vor der Möglichkeit einer Re-Identifizierbarkeit bzw. De-Anonymisierung, wenn Verantwortliche große Datenmengen sammeln und diese mittels elaborierter Big Data-Analysealgorithmen auf vermutete oder sogar noch unbekannte Zusammenhänge durchforsten.[6] 3

* Der Text ist im Zusammenhang mit dem BMWi-Projekt ENTOURAGE, FKZ 01MD16009D, entstanden.

1 Die Konzentration auf Zweifelsfälle – die auch der vorliegende Text verfolgt – sollte deshalb nicht zu der Annahme verleiten, dass derartige Fälle überwiegen. S. dazu allgemein aus methodischer Sicht *Haft*, Einführung in das juristische Lernen, 7. Aufl. 2015, S. 181 ff.

2 S. z.B. *Meyerdierks*, MMR 2009, 8; *Sachs*, CR 2010, 547; *Eckhardt*, CR 2011, 339; *Krüger/Maucher*, MMR 2011, 433; *Gerlach*, CR 2013, 478; *Breyer*, ZD 2014, 400; *Nink/Pohle*, MMR 2015, 563; ausführlich *Haase*, Datenschutzrechtliche Fragen des Personenbezugs, 2015, S. 373 ff.

3 EuGH v. 19.10.2016 – C-582/14, ECLI:EU:C:2016:779, CR 2016, 791 m. Anm. *Nink* – Breyer.

4 BGH v. 16.5.2017 – VI ZR 135/13, ECLI:DE:BGH:2017:160517UVIZR 135.13.0, CR 2017, 662 m. Anm. *Keppeler* = NJW 2017, 2416.

5 So auch *Marnau*, DuD 2016, 428, 429.

6 *Tene/Polonetsky*, Stanford Law Review Online (64) 2012, 63; *Baeriswyl*, digma 2013, 14, 15 ff.; *Roßnagel*, ZD 2013, 562, 563; *ders.*, SVR 2014, 281, 284; *Roßnagel/Geminn/Jandt/Richter*, Datenschutzrecht 2016 – „Smart"

Wie mit dem Problem eines sich „schleichend" einstellenden Zustands der Identifizierbarkeit betroffener Personen umzugehen ist und welche Rechtsfolgen eingreifen, ist bislang aber kaum ausgearbeitet worden.[7]

II. Der Wert der Anonymität

4 Anonymität ist kein Wert an sich. In vielen Konstellationen ist es Menschen wichtig, erkannt oder wiedererkannt, beim Namen gerufen oder mit bestimmten Eigenschaften identifiziert zu werden.[8] Dies gilt insbesondere für persönliche Kommunikationsbeziehungen, kann aber auch und gerade dort eine Rolle spielen, wo Unbekannte an uns herantreten wollen. Nicht umsonst schützt § 12 BGB schon seit dem Jahre 1900 gegen Namensleugnung und Namensanmaßung.[9]

5 Erkannt und wiedererkannt zu werden ist aber nicht nur Ausdruck des Persönlichkeitsrechts, sondern kann dieses auch gefährden. Dies gilt insbesondere in sozialen Machtungleichgewichten, die in der Informationsgesellschaft oftmals dort auftreten, wo es zu starken Informationsgefällen kommt. In dieser Situation – wenn also der Einzelne nicht mehr weiß, „wer was wann und bei welcher Gelegenheit über ihn weiß"[10] – bedarf es effektiver Schutzmechanismen, um zu verhindern, dass der Einzelne zum Objekt einer für ihn undurchschaubaren und deshalb auch unkontrollierbaren Datenverarbeitung wird.

6 Diese Schutzmechanismen können einerseits rechtlicher Natur sein (Transparenzvorgaben, Beschränkungen der Datenverarbeitung, Betroffenenrechte, aufsichtsbehördliche Maßnahmen etc.). Andererseits sind oftmals technische Maßnahmen die effektivsten Mittel des Datenschutzes, da der Missbrauch personenbezogener Daten dadurch bereits faktisch verhindert werden kann. Verbote missbräuchlicher Datenverarbeitung werden so idealerweise obsolet. Eine mögliche technische Sicherung ist dabei in der Anonymisierung personenbezogener Daten zu sehen, bei der die betroffene Person durch die Aufhebung des Personenbezugs vor Verletzungen ihres Persönlichkeitsrechts weitgehend geschützt wird.[11] Gleichzeitig beseitigt die Anonymisierung die Anwendbarkeit des Datenschutzrechts und bietet so Verantwortlichen den Vorteil, der Regulierung des Datenschutzrechts zu entgehen.

7 Das frühere Recht unterschied in § 3 Abs. 6 BDSG a.F. zwischen einer *echten* und einer *faktischen* Anonymisierung – letztere liegt vor, wenn die Daten nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können.[12] Auch wenn die DSGVO diese Unterscheidung nicht explizit enthält, liegt sie der Beschreibung in ErwGr 26 zugrunde. Dort wird nämlich eine Wahrscheinlichkeitsbetrachtung vorgegeben, die die früher in § 3 Abs. 6 BDSG a.F. genannten Kriterien berücksichtigen muss.[13] Die im Folgenden erläuterten Probleme resultieren vielfach genau aus dieser Kategorie der *faktischen* Anonymität, die zunächst nur eine (ggf.) theoretische, später aber auch praktische Möglichkeit der Re-Individualisierung zulässt.[14]

III. Konstellationen eines nachträglich eintretenden Personenbezugs

8 Anonyme Daten können in verschiedenen Konstellationen zu personenbezogenen Daten werden. Ob die Daten dabei für den Verantwortlichen von Beginn an anonym sind oder durch ihn anonymisiert wurden, spielt eine untergeordnete Rolle, sofern die Anonymisierung technisch ordnungsgemäß durchgeführt wurde.[15]

---

genug für die Zukunft?, 2016, S. 25 f.; *Katko/Babaei-Beigi*, MMR 2014, 360, 361 f.; *Härting/Schneider*, CR 2015, 819, 822; *Spindler*, MedR 2016, 691 f.; *Boehme-Neßler*, DuD 2016, 419, 422; *Eßer* in Auernhammer, DSGVO/BDSG, 5. Aufl. 2017, § 3a Rz. 21b; s. ferner *Spyra*, GuP 2015, 142, 149; *Schaar*, ZD 2016, 224, 225.

7 S. aber die Ansätze bei *Baeriswyl*, digma 2013, 14, 15 ff.; *Marnau*, DuD 2016, 428, 429; *Specht*, GRUR-Int. 2017, 1040, 1046; *Wójtowicz/Cebulla*, PinG 2017, 186, 192.

8 Vgl. *Trepte*, Privatsphäre aus psychologischer Sicht in *Schmidt/Weichert*, Datenschutz, 2012, S. 59 ff. Zu den daraus resultierenden Fragen eines elektronischen Identitätsmanagements s. z.B. die Beiträge in *Hornung/Engemann* (Hrsg.), Der digitale Bürger und seine Identität, 2016.

9 S. hierzu *Säcker* in MünchKomm/BGB, 8. Aufl. 2018, § 12 Rz. 97 ff.

10 So die bekannte Formel des BVerfG im Volkszählungsurteil, BVerfG v. 15.12.1983 – 1 BvR 209/83, 1 BvR 269/83, 1 BvR 362/83, 1 BvR 420/83, 1 BvR 440/83, 1 BvR 484/83, BVerfGE 65, 1 (43).

11 Manche Persönlichkeitsrisiken können dagegen trotz wirksamer Anonymisierung weiterhin bestehen. Das gilt insbesondere für die Gefahr, Menschen aufgrund von Wissen zu diskriminieren, das durch anonymisierte Daten gewonnen wird; vgl. hierzu z.B. *Möller/Florax*, MMR 2002, 806, 807 f.; *Möller/Florax*, NJW 2003, 2724 f. Diese Dimension bleibt im Folgenden außer Betracht.

12 S. zu Methoden der Anonymisierung z.B. *Schefzig*, K&R 2014, 772, 776; aus rechtlicher Sicht grundlegend zu Anonymität und Pseudonymität *Roßnagel/Scholz*, MMR 2000, 721 ff. Auch das BVerfG verlangte weder im Volkszählungsurteil noch in späteren Entscheidungen, dass eine Anonymisierung die Möglichkeit einer Re-Identifizierbarkeit gänzlich ausschließen müsse; vgl. BVerfG v. 15.12.1983 – 1 BvR 209/83, 1 BvR 269/83, 1 BvR 362/83, 1 BvR 420/83, 1 BvR 440/83, 1 BvR 484/83, BVerfGE 65, 1 (49); BVerfG v. 24.9.1987 – 1 BvR 970/87, CR 1987, 872 = NJW 1987, 2805, 2807; BVerfG v. 28.9.1987 – 1 BvR 1063/87, CR 1987, 877 = NJW 1988, 962, 963.

13 So auch *Gola* in Gola, DS-GVO, 2. Aufl. 2018, Art. 4 Rz. 41.

14 Eine vergleichbare Konstellation zur Re-Individualisierung bei faktischer Anonymität kann sich hinsichtlich der Unterscheidung zwischen „einfachen" personenbezogenen Daten und besonderen Kategorien personenbezogener Daten ergeben. Letzteres sind gem. Art. 9 Abs. 1 DSGVO Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten sowie Daten zum Sexualleben oder der sexuellen Orientierung. Sowohl aus Sicht des Verantwortlichen als auch aus Gründen der Datenminimierung kann es – wenn dies den Verarbeitungszweck nicht behindert – sinnvoll oder sogar geboten sein, durch das Entfernen bestimmter Daten den Versuch zu unternehmen, besondere Kategorien personenbezogener Daten i.S.v. Art. 9 Abs. 1 DSGVO in „einfache" personenbezogene Daten umzuwandeln, die dann nicht mehr den erhöhten Verarbeitungsanforderungen des Art. 9 DSGVO, sondern nur noch den allgemeinen Voraussetzungen des Art. 6 DSGVO unterliegen. Je nach Art und Inhalt der verbliebenen Daten kann es dann dazu kommen, dass im Zuge der sukzessiven Verbesserung von Analyseverfahren oder durch das Hinzutreten von Zusatzinformationen nachträglich doch wieder Daten i.S.v. Art. 9 Abs. 1 DSGVO vorliegen, weil unter Berücksichtigung dieser Umstände die genannten Kategorien aus den Daten „hervorgehen". Diese Dimension wird hier nicht weiter verfolgt, die grundsätzlichen Problemlagen sind aber übertragbar.

15 S. zu den Anforderungen z.B. *Art. 29-Datenschutzgruppe*, Stellungnahme 5/2014 zu Anonymisierungstechniken, WP 216, 2014; *Hansen* in Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 4 Nr. 5 Rz. 50 ff. m.w.N. Die beiden hauptsächlichen Arten der Anonymisierung sind die Randomisierung und die Generalisierung. Randomisierung bezeichnet Techniken, die die Daten in einer Weise verändern, dass die direkte Verbindung zwischen Daten und betroffener Person entfernt wird; sind die Daten ausreichend unbestimmt, können sie nicht mehr einer bestimmten Person zugeordnet werden (s. *Art. 29-Datenschutzgruppe*, ebd., 14 ff.). Bei der Generalisierung werden die Merkmale betroffener Personen durch die Veränderung der entsprechenden Größenskala oder -ordnung generalisiert, d.h. durch einen weniger spezifischen Wert er-

9 Ein nachträglicher Personenbezug kann einerseits schlagartig, andererseits durch schleichende Wissensvermehrung eintreten. Beides ist durch das Erlangen von Zusatzwissen bedingt.[16]

1. Schlagartiges Eintreten des Personenbezugs

10 Schlagartig tritt ein Personenbezug ein, wenn der Verantwortliche Zusatzinformationen erhält, die eine unmittelbare Identifizierung der betroffenen Person ermöglichen. Verbleibt beispielsweise im Rahmen eines Pseudonymisierungsverfahrens[17] die Zuordnungsregel für die Erstellung von Pseudonymen bei einem vertrauenswürdigen Dritten, so sind die Daten für alle Verantwortlichen nicht personenbezogen, die weder faktisch noch rechtlich einen Zugriff auf die Zuordnungsregel haben.[18] Wird diese Regel aber später versehentlich oder absichtlich durch den vertrauenswürdigen Dritten veröffentlicht, so sind die Daten in diesem Moment für alle anderen Stellen personenbezogen, die sie in pseudonymer Form verarbeiten.[19] Ein ähnlicher Fall kann auftreten, wenn zwei Verarbeiter über Datensätze verfügen, die aufgrund hochspezifischer Muster miteinander verknüpfbar sind, und nur der eine Verarbeiter über identifizierende Merkmale verfügt. Veröffentlicht letzterer seine Datensätze nebst den identifizierenden Merkmalen, so werden die Daten auch bei ersterem personenbezogen.[20]

11 Der Personenbezug kann auch durch einzelfallbezogene Informationen schlagartig eintreten, wenn etwa (nur) ein konkretes Pseudonym aufgedeckt oder andere individuelle Zusatzinformationen verfügbar werden. Letzteres könnte sogar durch ein Auskunftsverlangen nach Art. 15 DSGVO eintreten. Agiert eine betroffene Person mit einem frei gewählten Nutzernamen gegenüber einem Verantwortlichen und hat dieser auch sonst keine Möglichkeit der Identifizierung, so wird der Anwendungsbereich des Datenschutzrechts schlagartig eröffnet, wenn die betroffene Person im Rahmen des Auskunftsbegehrens ihr Pseudonym offenlegt.

2. Schleichende Identifizierbarkeit

12 Ungleich komplexer ist das Phänomen einer schrittweisen, ggf. schwer oder gar nicht feststellbar eintretenden Identifizierbarkeit der betroffenen Person. Die Problematik wird durch ErwGr 26 Sätze 3 und 4 DSGVO verdeutlicht, der die Kriterien für die Identifizierbarkeit nach Art. 4 Nr. 1 DSGVO erläutert; sie lauten:

13 „[3]Um festzustellen, ob eine natürliche Person identifizierbar ist, sollten *alle Mittel* berücksichtigt werden, die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen *wahrscheinlich genutzt werden*, um die natürliche Person direkt *oder indirekt* zu identifizieren, wie beispielsweise das Aussondern. [4]Bei der Feststellung, ob Mittel nach allgemeinem Ermessen wahrscheinlich zur Identifizierung der natürlichen Person genutzt werden, sollten alle objektiven Faktoren, wie die *Kosten* der Identifizierung und der dafür erforderliche *Zeitaufwand*, herangezogen werden, wobei die zum Zeitpunkt der Verarbeitung *verfügbare Technologie* und *technologische Entwicklungen* zu berücksichtigen sind." [Hervorhebungen hinzugefügt]

a) Ausgangspunkt

14 Ausgangspunkt ist also eine Situation, in der weder beim Verantwortlichen noch bei einer anderen Person[21] Mittel vorliegen, um die betroffene Person zu identifizieren. In diesem Fall ist kein Personenbezug gegeben. Oftmals sind allerdings auf Seiten des Verantwortlichen oder einer anderen Person entsprechende Mittel vorhanden, so dass die Identifizierbarkeit von der Frage abhängt, ob diese Mittel auch nach allgemeinem Ermessen wahrscheinlich genutzt werden, um eine Identifizierung durchzuführen. Für die Antwort sind sämtliche Umstände des Einzelfalls in die Bewertung miteinzubeziehen, wobei unterschiedliche Gründe zu einer negativen Beurteilung der Wahrscheinlichkeit führen können: Die Mittel – Hard- und Software, personelle Ressourcen, Zusatzwissen durch weitere Daten, Nachforschungen etc. – sind beispielsweise für den Verantwortlichen absolut oder im Verhältnis zum erwarteten Ertrag *zu teuer*, oder ihr Einsatz erfordert *zu viel Zeit*.[22] Für die Beurteilung ist auf den jeweiligen *Stand der Technik* abzustellen.[23] Zusätzlich muss allerdings prognostiziert werden, wie sich die Technik im Verarbeitungszeitraum entwickeln wird. Diese Einschätzung ist anschließend bei der Beurteilung der Verhältnismäßigkeit zugrunde zu legen.[24] Dies wird durch ErwGr 26 S. 4 DSGVO explizit in den Blick genommen, der dazu verpflichtet, „technologische Entwicklungen" mit zu berücksichtigen. Die bloß abstrakte Möglichkeit, dass eine disrup-

---

setzt (etwa durch die Angabe einer Region statt einer Stadt oder eines Monats statt einer Woche, s. *Art. 29-Datenschutzgruppe*, ebd., 19 ff.).

16 Nachträgliches Erlangen von Zusatzwissen kann auch zu einem Wechsel innerhalb des Personenbezugs führen: von der bloßen Identifizierbarkeit einer betroffenen Person zu deren tatsächlicher Identifiziertheit. Beides erfüllt allerdings die Definition des personenbezogenen Datums nach Art. 4 Nr. 1 DSGVO.

17 Dazu aus rechtlicher Sicht grundlegend *Roßnagel/Scholz*, MMR 2000, 721 ff.; zur Einordnung der Pseudonymisierung nach der DSGVO s. instruktiv *Roßnagel*, ZD 2018, 243 ff.

18 Dies gilt trotz der Grundkonzeption der DSGVO, die ausweislich ErwGr 26 S. 2 DSGVO zumindest grundsätzlich davon ausgeht, dass pseudonyme Daten personenbezogene Daten sind. Hierdurch werden aber nur Fälle adressiert, in denen eine Zuordnung durch den jeweiligen Verantwortlichen gerade möglich ist (s. näher *Roßnagel*, ZD 2018, 243 ff.), während bei einer entsprechenden Rollentrennung gerade eine – relative – anonymisierende Wirkung eintritt (ebd., 245).

19 S. hierzu auch *Ziebarth* in Sydow, DSGVO, 2. Aufl. 2018, Art. 4 Rz. 99.

20 So im Fall der Bereitstellung anonymisierter Filmbewertungen durch die Firma Netflix, die sich tlw. durch einen Abgleich mit öffentlich verfügbaren Filmbewertungen des Kinoportals Internet Movie Database deanonymisieren ließen, s. dazu *Hornung/Herfurth*, Datenschutz bei Big Data in König/Schröder/Wiegand, Big Data, 2018, S. 164 f. Bei mindestens sechs bewerteten Filmen, die nicht unter den Top 500 waren, lag die Wahrscheinlichkeit einer Re-Identifizierung einer betroffenen Person bei ca. 84 %. War die Bewertung zweier Filme innerhalb eines Zeitraums von plus/minus drei Tagen bekannt, so lag die Wahrscheinlichkeit einer Re-Identifizierung bei immerhin 68 %, s. *Narayanan/Shmatikov*, Robust Deanonymization of Large Sparse Datasets in IEEE Computer Society, Proc. of 29th IEEE Symposium on Security and Privacy, 2008, S. 121.

21 Zum Problem, ob dies eine beliebige andere Person sein kann oder diese im Lager des Verantwortlichen stehen muss, s. *Klar/Kühling* in Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 4 Nr. 1 Rz. 25 ff.

22 *Roßnagel/Scholz*, MMR 2000, 721, 723 f.

23 *Karg* in Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 4 Nr. 1 Rz. 63.

24 *Art. 29-Datenschutzgruppe*, Stellungnahme 4/2007 zum Begriff „personenbezogene Daten", WP 136, 2007, S. 18; *Roßnagel*, ZD 2013, 562, 563, 565.

tive technische Innovation die Aufwandsprognose überholt, bleibt demgegenüber außer Betracht.[25]

b) Faktoren als Moving Target

15 Problematisch und von entscheidender Bedeutung ist, dass sich alle genannten Faktoren ändern können. Insbesondere bei umfassenden, auf langfristige Speicherung angelegten Big Data-Anwendungen besteht die Gefahr eines dynamischen „Hineinwachsens" in den Personenbezug während der Speicherdauer.[26] Werden anonymisierte Daten mit anderen, neuen Daten verknüpft, so kann dies bewirken, dass nach der Zusammenführung genügend Merkmale vorhanden sind, um die betroffene Person zu re-identifizieren.[27] Je größer die zur Verfügung stehende Datenbasis ist und je mehr Möglichkeiten bestehen, die verschiedenen Datensätze miteinander zu verknüpfen, desto vielfältiger sind auch die möglichen Erkenntnisse und Rückschlüsse, die dazu führen können, dass bestimmte Personen identifizierbar sind.[28]

16 Ähnliche Effekte können durch wissenschaftlich-technischen Fortschritt eintreten: Eine bisher nicht vorhandene oder zu teure Analysemethode wird entwickelt, am Markt verfügbar gemacht oder zu einem deutlich geringeren Preis angeboten als bisher. Durch derartige neue, effiziente und kostengünstige Werkzeuge sinkt der erforderliche Aufwand zur Datenauswertung,[29] und dies kann zu einer Wahrscheinlichkeitsprognose führen, nach der eine Identifizierbarkeit anzunehmen ist.[30] Dasselbe gilt für den Fall einer Steigerung des wirtschaftlichen Werts von Daten, wenn diese anonymisiert gespeichert sind, ihre personenbezogene Nutzung aber ökonomische Vorteile verspricht. Hierfür reichen schon begründete Hoffnungen auf derartige Vorteile aus, weil sie die Akteure zur De-Anonymisierung animieren können.[31]

17 Für die weitere rechtliche Bewertung ist wichtig, dass diese Prozesse vielfach gradueller Natur sind. Es wird deshalb häufig schwierig zu beurteilen – und deshalb umstritten – sein, wann die Grenze zur Identifizierbarkeit exakt bzw. „gerade so" überschritten wird.[32]

IV. Rechtsfolgen *de lege lata*

18 Tritt nachträglich ein Personenbezug ein, so ergeben sich daraus unterschiedliche Rechtsfolgen, die den jeweiligen Verantwortlichen vor Probleme stellen können. Dies gilt insbesondere dann, wenn der Verantwortliche auf die Beständigkeit seiner gewählten Anonymisierungstechniken vertraut und keinerlei oder nur wenige Vorsorgemaßnahmen für den Fall einer später eintretenden Identifizierbarkeit getroffen hat.

1. Sachliche Anwendbarkeit des Datenschutzrechts

19 Das Datenschutzrecht ist nach Art. 2 Abs. 1 DSGVO und § 1 Abs. 1 BDSG im Grundsatz[33] sachlich anwendbar, wenn personenbezogene Daten verarbeitet werden. Für das Vorliegen eines Personenbezugs reicht es bereits aus, wenn die betroffene Person lediglich identifizierbar ist (Art. 4 Nr. 1 DSGVO). Die DSGVO enthält keine Regelung, wonach nur ein anfänglicher Personenbezug zur Geltung des Datenschutzrechts führt . Eine derartige Bestimmung wäre auch widersinnig, würde die betroffene Person doch so um den Schutz des Datenschutzrechts gebracht, obwohl bei ihr die gleiche Schutzbedürftigkeit vorliegt wie bei einem von Anfang an bestehenden Personenbezug.

Ob die Daten i.S.v. Art. 4 Nr. 2 DSGVO verarbeitet werden, 20
richtet sich nach dem Einzelfall. Eine Unterscheidung nach einzelnen Verarbeitungsphasen, wie sie das BDSG a.F. enthielt, kennt die Verordnung nur noch in Ausnahmefällen (z.B. Artt. 13, 14 DSGVO, wo auf das Erheben abgestellt wird, s.u. IV.2.a)).[34] Es kommt deshalb z.B. nicht darauf an, ob man das nachträgliche Erlangen von Zusatzwissen als Datenerhebung einordnen kann. Nach dem BDSG a.F. wäre diese Frage hingegen relevant und zu diskutieren gewesen, da § 3 Abs. 3 BDSG a.F. das Erheben als das Beschaffen von Daten über den Betroffenen definierte und damit eine aktive Komponente enthielt.[35]

Auch für Art. 4 Nr. 2 DSGVO lässt sich allerdings bezweifeln, 21
ob eine Verarbeitung vorliegt, wenn die nachträglich personenbezogenen Daten in keiner Weise verwendet werden, sondern sich ausschließlich das außerhalb der konkreten Anwendung befindliche Zusatzwissen des Verantwortlichen erweitert. Ein datenschutzrechtlich relevanter Vorgang setzt nämlich zumindest voraus, dass die Daten zu einem bestimmten Zweck abgerufen, zusammengestellt, ausgewertet oder ansonsten zielgerichtet zur Kenntnis genommen werden sollen.[36] Da aber keine explizite Kenntnis des bestehenden Personenbezugs auf Seiten des Verantwortlichen erforderlich ist,[37] ist beispielsweise bei jedem Zugriff auf die nachträglich personenbezogenen Daten sowie bei jeder Umspeicherung derselben von einer datenschutzrechtlich relevanten Verarbeitung auszugehen. Der Fall einer Erweiterung des Zusatzwissens ohne Verarbeitungsvorgang dürfte daher nur selten relevant werden.

Damit lässt sich festhalten, dass ab dem Moment, in dem die 22
Kriterien des ErwGr 26 Satz 3 und 4 DSGVO erfüllt werden,

---

25 Vgl. *Kühling/Klar*, NJW 2013, 3611, 3613 f.

26 *Roßnagel*, ZD 2013, 562, 563 und 566; *Marnau*, DuD 2016, 428, 429; s. zum Folgenden schon *Hornung/Herfurth*, Datenschutz bei Big Data in König/Schröder/Wiegand, Big Data, 2018, S. 165 f.

27 *Marnau*, DuD 2016, 428, 429.

28 *Martini*, DVBl. 2014, 1481, 1482, 1487; *Marnau*, DuD 2016, 428; *Saruns-ki*, DuD 2016, 424, 427.

29 Vgl. auch *Hammer/Knopp*, DuD 2015, 503, 506 f.

30 *Weichert* in Däubler et al., DS-GVO/BDSG, 2018, Art. 4 Rz. 76, 80.

31 Vgl. *Wójtowicz/Cebulla*, PinG 2017, 186, 189.

32 So auch *Buchholtz/Stentzel* in Gierschmann et al., DS-GVO, 2018, Art. 4 Nr. 1 Rz. 7.

33 Die Fragen der Automatisierung bzw. des Dateisystems (Art. 2 Abs. 1 DSGVO) bleiben hier außer Betracht, da sie ohnehin nur noch eine untergeordnete Rolle spielen, s. *v. Lewinski* in Auernhammer, DSGVO/BDSG, 6. Aufl. 2018, Art. 2 Rz. 5.

34 S. daneben Art. 5 Abs. 1 lit. b, Art. 6 Abs. 4, Art. 15 Abs. 1 lit. g, Art. 17 Abs. 1 lit. a, lit. f., Art. 25 Abs. 2, Art. 40 Abs. 2 lit. c DSGVO.

35 S. *Dammann* in Simitis, BDSG, 8. Aufl. 2014, § 3 Abs. 3 Rz. 102.

36 *Herbst* in Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 4 Nr. 2 Rz. 28; *Weichert* in Däubler et al., DS-GVO/BDSG, 2018, Art. 4 Rz. 44; vgl. zum BDSG a.F. LAG Hamm, ZD 2012, 183, 184 f.; *Gola/Klug/Körffer* in Gola/Schomerus, BDSG, 12. Aufl. 2015, § 3 Rz. 42; *Buchner* in Taeger/Gabel, BDSG, 2. Aufl. 2013, § 3 Rz. 42.

37 Vgl. *Klar/Kühling* in Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 4 Nr. 1 Rz. 23.

im Grundsatz das gesamte Datenschutzrecht Anwendung findet.[38]

2. Probleme der datenschutzrechtliche Vorgaben

23 Die konkret eintretenden Rechtsfolgen, die sich aus der Geltung des Datenschutzrechts ergeben, können je nach Art der Daten und ihres Verwendungszusammenhangs divergieren. Manche Normen sind immer, andere dagegen nur unter zusätzlichen Tatbestandsvoraussetzungen zu beachten. Etliche Bestimmungen der DSGVO und des neuen BDSG werfen in der Konstellation des nachträglich eintretenden Personenbezugs allerdings Probleme auf.

a) Grundsätzliche Herausforderungen

24 Tritt der Personenbezug nachträglich ein, so sind zunächst die Datenschutzgrundsätze des Art. 5 DSGVO einzuhalten, die einerseits eine „objektive Dimension"[39] aufweisen und andererseits unmittelbare Geltung beanspruchen. Es handelt sich mithin nicht um bloße Programmsätze,[40] auch wenn die konkreten Rechtswirkungen aufgrund der Unbestimmtheit einiger Grundsätze bislang nicht vollständig geklärt sind.[41] Die Anwendbarkeit von Art. 5 Abs. 1 DSGVO führt dazu, dass der Verantwortliche für die fortgesetzte Verarbeitung der bisher nicht personenbezogenen Daten nunmehr eine Verarbeitungsgrundlage benötigt, Transparenzvorgaben einhalten muss und den Grundsatz von Treu und Glauben zu beachten hat (lit. a), einen eindeutigen und legitimen Zweck festlegen muss (lit. b), im Umfang der Verarbeitung beschränkt ist (lit. c, e), sowie die Daten ggf. berichtigen und auf den neuesten Stand zu bringen (lit. d) und technisch zu sichern hat (lit. f).

aa) Handlungspflichten

25 In einigen Fällen löst Art. 5 DSGVO unmittelbar Handlungspflichten aus, v.a. hinsichtlich der Verarbeitungsgrundlage (i.V.m. Art. 6 DSGVO) und bei Zweckbindung, Datenminimierung und Speicherbegrenzung. In anderen Fällen wird Art. 5 DSGVO vor allem durch andere Vorschriften der Verordnung konkretisiert. Dies führt beim nachträglichen Personenbezug teilweise zu Problemen, die sich beispielhaft an den transparenzorientierten Informationspflichten der Artt. 13, 14 DSGVO verdeutlichen lassen. Diese setzen tatbestandlich voraus, dass personenbezogene Daten erhoben werden. Der in Art. 4 Nr. 2 DSGVO genannte, aber nicht legaldefinierte Vorgang des Erhebens wird als erstmaliges Gelangen in den Verfügungsbereich des Verantwortlichen beschrieben und setzt typischerweise ein aktives Handeln voraus.[42] Beides ist in den hier beschriebenen Konstellationen zwar gegeben, es fehlt jedoch im Zeitpunkt des Erhebens am Personenbezug.

26 Bei wortlautorientierter Auslegung ließe sich folglich vertreten, dass die Informationspflichten bei nachträglichem Personenbezug nicht greifen. Allerdings wird dies bereits durch die englische Sprachfassung von Artt. 13, 14 DSGVO relativiert, die nicht einheitlich den Begriff des Erhebens (in der Terminologie der Verordnung: collect) verwendet, sondern im Falle von Art. 14 DSGVO „obtain" (dies wird in der deutschen Fassung in Abs. 1 mit „erhoben", in Abs. 3 aber mit „Erlangung" bezeichnet). Dies deutet darauf hin, dass Artt. 13, Art. 14 DSGVO nicht zu sehr an eine bestimmte Verarbeitungsphase gekoppelt werden sollten. Aus der Perspektive der betroffenen Person und mit Blick auf das Telos des Grundrechtsschutzes (Art. 1 Abs. 2 DSGVO) spricht außerdem alles dafür, den Begriff der Erhebung i.S.d. Artt. 13, 14 DSGVO risikobezogen weiter zu verstehen als nach § 3 Abs. 3 BDSG a.F.[43] Unter einer solchen risikobezogenen Perspektive besteht nämlich kein Unterschied zwischen einer erstmaligen Erhebung personenbezogener Daten bei Dritten und dem nachträglichen Erlangen von Zusatzwissen, das Daten personenbezogen werden lässt. Dieser Fall sollte deshalb ebenfalls unter die Transparenzpflichten subsumiert werden.[44]

27 Da die Zusatzinformationen typischerweise nicht vom Betroffenen erlangt werden und Art. 13 DSGVO erkennbar von einem direkten Kontakt ausgeht, ist Art. 14 DSGVO einschlägig. Ob die Informationspflicht nach Art. 14 Abs. 5 DSGVO ausgeschlossen ist, muss im Einzelfall geprüft werden. Art. 14 Abs. 3 DSGVO enthält verschiedene Fristen für die zu erfüllende Information. Diese beginnen ab dem Zeitpunkt des nachträglichen Personenbezugs zu laufen und ermöglichen angemessene Einzelfalllösungen; die Informationspflicht kann dabei sogar entfallen, wenn ihre Umsetzung *unverhältnismäßig* wäre (Art. 14 Abs. 5 lit. b DSGVO).

bb) Probleme der Erfüllbarkeit

28 Bei vielen anderen Normen fehlt eine solche Regelung hingegen; sie gelten ihrem Wortlaut nach unmittelbar bei Verarbeitung personenbezogener Daten. Legt man dies zugrunde, müssten Verantwortliche ggf. völlig überraschend über eine Verarbeitungsgrundlage verfügen (Art. 6 Abs. 1 DSGVO), die Einhaltung der Datenschutzgrundsätze nachweisen (Art. 5 Abs. 2 DSGVO), technische und organisatorische Maßnahmen ergreifen (Art. 24 DSGVO), datenschutzfreundliche Technologien und Voreinstellungen einsetzen (Art. 25 DSGVO), einen

38 So auch *Wójtowicz/Cebulla*, PinG 2017, 186, 191; *Kühling/Klar*, NJW 2013, 3611, 3614; i.E. wohl auch *Härting*, NJW 2013, 2065, 2066; für das alte Recht *Roßnagel/Scholz*, MMR 2000, 721, 722 f.

39 *Herbst* in Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 5 Rz. 1.

40 *Roßnagel* in Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 5 Rz. 23, 188; *Schantz* in BeckOK BDSG/DSGVO, 27. Edition 2019, Art. 5 Rz. 2; *Kramer* in Auernhammer, DSGVO/BDSG, 6. Aufl. 2018, Art. 5 Rz. 5; *Pötters* in Gola, DS-GVO, 2. Aufl. 2018, Art. 5 Rz. 4; *Ziegenhorn/von Heckel*, NVwZ 2016, 1585, 1589.

41 S. *Roßnagel*, ZD 2018, 339; die Unbestimmtheit hat auch Folgen für die Bußgeldbewehrung in Art. 83 Abs. 5 lit. a DSGVO, die vielfach aufgrund primärrechtlicher Vorgaben (Art. 49 Abs. 1 GRCh) eingeschränkt wird, s. *Hoeren*, ZD 2016, 459, 462; *Roßnagel* in Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, Art. 5 Rz. 18.

42 *Roßnagel* in Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 4 Nr. 2 Rz. 15; *Herbst* in Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 4 Nr. 2 Rz. 21; weiter *Dix* in Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 13 Rz. 5.

43 Ebenso für den Datenempfangs im Falle einer unverlangten Spontanübermittlung *Bäcker* in Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 14 Rz. 11.

44 Sofern man vertritt, dass eine nachträgliche Veränderung der Informationen, die nach Artt. 13, 14 DSGVO bereitgestellt wurden, ebenfalls mitzuteilen ist (*Art. 29-Datenschutzgruppe*, Leitlinien für Transparenz gemäß der Verordnung 2016/679, WP 260 rev.01, 2018, S. 20; *Knyrim* in Ehmann/Selmayr, DS-GVO, 2. Aufl. 2018, Art. 13 Rz. 12; *Dix* in Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 13 Rz. 7; a.A. *Veil* in Gierschmann et al., DS-GVO, 2018, Art. 13 und 14 Rz. 45), kann man auch mit einer Vergleichbarkeit zur hiesigen Konstellation argumentieren.

Vertreter benennen (Art. 27 DSGVO), spezifische Verträge mit Auftragnehmern schließen (Art. 28 DSGVO), ein Verarbeitungsverzeichnis vorhalten (Art. 30 DSGVO), IT-Sicherheitsmaßnahmen berücksichtigen (Art. 32 DSGVO), eine Datenschutz-Folgenabschätzung durchgeführt haben (Art. 35 DSGVO), einen Datenschutzbeauftragten benennen (Art. 37 DSGVO i.V.m. § 38 BDSG n.F.) und Anforderungen an die Übermittlung in Drittstaaten einhalten (Art. 44 ff. DSGVO).

29 Die unmittelbare Erfüllung dieser Vorschriften in der Sekunde eines nachträglich eintretenden Personenbezugs ist allerdings erkennbar unmöglich und damit zumindest bei solchen Verantwortlichen unverhältnismäßig, die nicht gezielt auf eine De-Anonymisierung hinarbeiten.[45] Auch wenn insoweit weder eine gesetzliche Regelung noch irgendein normativer Anhaltspunkt besteht, wird man dem Verantwortlichen dementsprechend eine angemessene Frist zur Erfüllung der einzelnen Pflichten einräumen müssen.[46] Diese richtet sich nach dem erforderlichen Umfang für die Umsetzung und wird bei riskanten Datenverarbeitungen kürzer ausfallen müssen. Der Verantwortliche muss außerdem erkennbar auf die Herstellung eines rechtsgemäßen Zustands hinarbeiten; ihm sollte die *temporäre Privilegierung* nicht (mehr) zuerkannt werden, wenn er diese zum Nachteil der betroffenen Personen ausnutzt.

b) Besonderheiten des schleichenden Personenbezugs

30 Besondere Herausforderungen wirft die Fallgruppe der schleichenden Identifizierbarkeit von betroffenen Personen auf, also die Fälle, in denen nach den Kriterien von ErwGr 26 DSGVO „gerade so" von einer identifizierbaren Person auszugehen ist. In der Praxis wird dies regelmäßig Konstellationen erfassen, in denen eine tatsächliche Identifizierung zwar möglich und unter Risikogesichtspunkten hinreichend wahrscheinlich ist, wegen des erheblichen Aufwands aber (zumindest im Regelbetrieb) gerade unterbleibt.

aa) Passives und aktives Wissen

31 Wenn das Wissen um die konkrete betroffene Person zwar abstrakt beim Verantwortlichen vorhanden, jedoch nicht konkret und *aktiv* verfügbar ist, führt dies zu erheblichen Friktionen bei der Anwendung des Datenschutzrechts. Viele Regelungen setzen nämlich ein *aktives* Wissen über die betroffene Person voraus. Nur wenn diese konkret bekannt ist, kann von ihr eine Einwilligung eingeholt (Art. 6 Abs. 1 Unterabs. 1 lit. a, Art. 9 Abs. 2 lit. a i.V.m. Art. 7, 8 DSGVO) oder geprüft werden, ob ihre Interessen, Grundrechte oder Grundfreiheiten die berechtigten Interessen des Verantwortlichen überwiegen (Art. 6 Abs. 1 Unterabs. 1 lit. f DSGVO).[47] Ohne die Kontaktdaten zu kennen, können die Informationspflichten nach Artt. 13, 14 DSGVO nicht oder nur durch öffentliche Informationen (Art. 14 Abs. 5 lit. b DSGVO) erfüllt werden. Schließlich enthält die Verordnung an einer Vielzahl von Stellen risikobezogene Abwägungen,[48] die man zwar grundsätzlich typisiert durchführen kann, die im Einzelfall aber aufgrund von Besonderheiten der betroffenen Person anders ausfallen können (z.B. Artt. 24, 25, 32, 33, 34, 35 DSGVO).[49]

32 Unter Umständen müsste der Verantwortliche zur Einhaltung datenschutzrechtlicher Pflichten also eine „gerade so" identifizierbare betroffene Person zunächst tatsächlich identifizieren, um von ihr anschließend eine Einwilligung einzuholen, sie zu informieren oder das Risiko einer Verarbeitung sie betreffender Daten abzuschätzen. Mit Blick auf den Schutzzweck des Datenschutzes wäre dies allerdings widersinnig, da die Risiken der Datenverarbeitung durch die tatsächliche Identifizierung deutlich erhöht werden. In der Praxis dürfte bei der tatsächlichen Identifizierung von „gerade so" identifizierbaren betroffenen Personen überdies ein deutliches Risiko von fehlerhaften Zuordnungen bestehen („false positives"), was sowohl für den Verantwortlichen (Risiko fehlerhafter und damit rechtswidriger Datenverarbeitungen) als auch für die betroffenen Personen (Nachteile aufgrund fehlerhafter Daten; Übermittlung an Nichtberechtigte) zusätzliche Risiken hervorruft.

bb) Reichweite und Grenzen von Art. 11 DSGVO

33 Dieses Problem hat der europäische Gesetzgeber mit Art. 11 DSGVO zu adressieren versucht. Allerdings wirft die Auslegung dieser Vorschrift erhebliche Unsicherheiten auf und ist in ihrem Anwendungsbereich beschränkt.

34 *Dispens:* Weitgehende Einigkeit besteht dahin, dass Art. 11 DSGVO Konstellationen erfasst, in denen betroffene Personen – entsprechend den allgemeinen Kriterien, die EuGH und BGH nunmehr für die Speicherung von IP-Adressen durch Webseitenbetreiber konkretisiert haben[50] – zwar identifizierbar, nicht aber durch den Verantwortlichen konkret identifiziert sind.[51] Dieser verfolgt keinen Verarbeitungszweck, zu dessen Erfüllung er die Identität aktiv ermitteln muss. Wohl aber hätte er die Möglichkeit, dies durch die Aufbewahrung, Einholung oder Verarbeitung von „zusätzlichen Informationen" zu tun. Art. 11 Abs. 1 DSGVO entbindet ihn insoweit davon,[52] von dieser tatsächlichen Möglichkeit „zur bloßen Einhaltung" der Verordnung Gebrauch zu machen.

35 *Zusätzlich Informationen:* Die Norm wird in der Literatur vor allem auf verschiedene Konstellationen der Nutzung von Pseudonymen[53] oder die nicht mit sicher identifizierten Personen

45 So für das bisherige Recht *Roßnagel/Scholz*, MMR 2000, 721, 731.

46 S. in diesem Sinne *Roßnagel/Scholz*, MMR 2000, 721, 731.

47 Dies hat auch Folgewirkungen für den Einsatz von Einwilligungen bei anderen Anforderungen, z.B. nach Art. 22 Abs. 2 lit. c, Art. 49 Abs. 1 Satz 1 lit. a DSGVO.

48 Zum sog. risikobezogenen Ansatz der DSGVOs. *Veil*, ZD 2015, 347; *Gellert*, CLSR 34 (2018), 279; kritisch *Roßnagel*, DuD 2016, 565; zurückhaltend zum Neuheitsgrad zu Recht *Gellert*, EDPL 2016, 481 („we have always managed risiks in data protection law").

49 S. z.B. explizit Art. 35 Abs. 9 DSGVO, wonach ggf. der Standpunkt der betroffenen Person einzuholen ist.

50 EuGH v. 19.10.2016 – C-582/14, ECLI:EU:C:2016:779, CR 2016, 791 m. Anm. *Nink* – Breyer und BGH v. 16.5.2017 – VI ZR 135/13, ECLI:DE:BGH:2017:160517UVIZR135.13.0, NJW 2017, 2416.

51 BGH v. 16.5.2017 – VI ZR 135/13, ECLI:DE:BGH:2017:160517UVIZR 135.13.0, CR 2017, 662 m. Anm. *Keppeler*; *Wolff* in BeckOK BDSG/DSGVO, 27. Edition 2019, Art. 11 Rz. 12; *Kampert* in Sydow, DSGVO, 2. Aufl. 2018, Art. 11 Rz. 4; s. bzgl. des Ausschlusses von anonymisierten Daten z.B. *Klabunde* in Ehmann/Selmayr, DS-GVO, 2. Aufl. 2018, Art. 11 Rz. 13.

52 Die Pflicht, zur Einhaltung der Verordnung in dieser Weise vorzugehen, lässt sich auf Art. 24 DSGVO zurückführen, s. *Veil* in Gierschmann et al., DS-GVO, 2018, Art. 11 Rz. 24.

53 *Schwartmann/Jaspers/Jacquemain* in Schwartmann et al., DS-GVO/BDSG, 2018, Art. 11 Rz. 6; *Veil* in Gierschmann et al., DS-GVO, 2018,

verbundene Datenverarbeitung im Internet bezogen.[54] Sie erfasst indes grundsätzlich auch die hier diskutierten Konstellationen, in denen nachträglich „schleichend" eine Identifizierbarkeit eingetreten ist. Allerdings hilft sie dem Verantwortlichen nur begrenzt weiter. Soweit die Tatbestandsmerkmale der „zusätzlichen Informationen" und des „aufzubewahren, einzuholen oder zu verarbeiten" diskutiert werden, wird der Dispens nämlich regelmäßig so verstanden, dass die „zusätzlichen Informationen" solche von dritter Seite sein müssen.[55] Verfüge der Verantwortliche hingegen über alle Informationen, um die Zuordnung (ggf. mit einem gewissen technischen Aufwand) selbst vorzunehmen, so komme eine Freistellung von Regeln der Verordnung nicht in Betracht.[56]

36 *Fortbestehen des Dilemmas:* Gegen diese Auslegung sprechen zwar Gleichbehandlungs- und Schutzzweckgesichtspunkte, weil der Verantwortliche im Falle der faktisch möglichen Erlangung externen Zusatzwissens privilegiert würde, im Falle der faktisch möglichen aufwendigen internen Ermittlung der betroffenen Person diese aber durchführen müsste, obwohl sie grundrechtlich gleichermaßen kontraproduktive Effekte für die betroffene Person hätte. Selbst wenn man aber diesem weiten Verständnis von Art. 11 DSGVO folgt, lösen sich die oben beschriebenen Probleme aus zwei Gründen nicht auf:

37 *(1) Klärung der Identifizierbarkeit:* Zum einen muss der Verantwortliche bereits auf einer vorgelagerten Ebene klären, ob er überhaupt Daten einer identifizierbaren Person verarbeitet – nämlich für die Antwort auf die Frage, ob er überhaupt in den Anwendungsbereich von Art. 11 DSGVO (bzw. der Verordnung überhaupt) fällt und dessen Pflichten einhalten muss (also z.B. nach Abs. 2 nachzuweisen hat, dass er die betroffene Person nicht identifizieren kann).

38 *(2) Rechtsfolgen:* Zum anderen entbindet Art. 11 DSGVO (ohnehin nur implizit)[57] keineswegs von allen Pflichten der Verordnung. Vom Sinn und Zweck der Norm her kann sich diese nur auf Vorschriften beziehen, die eine sichere Kenntnis der betroffenen Person erfordern. Dies sind alle Normen, die eine Kommunikation mit der betroffenen Person oder die Zuordnung konkreter Daten zu ihr erfordern.[58] Ersteres betrifft v.a. die Betroffenenrechte, für die Art. 11 Abs. 2 DSGVO eine unglücklich formulierte Sonderregelung trifft, deren konkrete Reichweite kontrovers diskutiert wird.[59] Andere Pflichten kann der Verantwortliche demgegenüber ohne weiteres erfüllen, ohne konkret zu wissen, um welche betroffenen Personen es sich handelt – für die Umsetzung von Maßnahmen des Datenschutzes durch Technikgestaltung (Art. 25 Abs. 1 DSGVO), den Abschluss von Verträgen mit Auftragsverarbeitern (Art. 28 DSGVO), das Anlegen eines Verzeichnisses von Verarbeitungstätigkeiten (Art. 30 DSGVO), das Ergreifen von Maßnahmen der Datensicherheit (Art. 32 DSGVO), die Durchführung einer Datenschutz-Folgenabschätzung (Art. 35 DSGVO) oder einer Zertifizierung (Art. 42 DSGVO), die Benennung eines Datenschutzbeauftragten (Art. 37 DSGVO) oder die Einhaltung der Beschränkungen für Drittlandsübermittlungen (Art. 44 ff. DSGVO) mag es mitunter nützlich sein, die betroffenen Personen zu kennen – prinzipiell erforderlich ist es nicht.

V. Lösungsansätze

39 Trotz Art. 11 DSGVO bestehen also für Verantwortliche, die nachträglich anonyme Datenbestände mit anderen Informationen anreichern, erhebliche Rechtsunsicherheiten. Außerdem kann selbst bei rein passivem Verhalten eines Verantwortlichen sein anonymer Datenbestand schleichend personenbezogen werden, wenn sich frei verfügbares Zusatzwissen erweitert oder verfügbare Datenverarbeitungstechnologien an Effizienz gewinnen.

1. Lösungsansätze *de lege lata*

Nach geltendem Recht bieten sich verschiedene Ansätze, um 40
diese Probleme zu minimieren. Im Ergebnis bieten sie aber nur unvollkommene Lösungen.

a) Technische Lösungsansätze

Technische Ansätze könnten in der Vermeidung der Identifi- 41
zierbarkeit und (wenn dies nicht erfolgreich ist) in ihrer Beseitigung liegen. Greift beides nicht, könnten technische Verfahren zumindest dem Verantwortlichen die Identifizierbarkeit anzeigen.

aa) Vermeidung und unmittelbare Beseitigung der Identifizierbarkeit

Für den ersten Ansatz bedarf es also verbesserter und erweiter- 42
ter technisch-organisatorischer Verfahren zur Anonymisierung personenbezogener Daten und zur dauerhaften Verhinderung der Re-Individualisierung. Diese können dazu beitragen, das schlagartige oder schleichende Eintreten der Anwendbarkeit des Datenschutzrechts zu verhindern. Als *präventive* Maßnahme kommt beispielsweise die Abschottung von Datensammlungen in Betracht (so dass kein neues Zusatzwissen hinzukommt, auch und gerade bei Unternehmensfusionen), die regelmäßige Analyse neuer Angriffsszenarien und neuer Entwicklungen im Bereich von De-Anonymisierungstechniken oder vertragliche Mitteilungspflichten mit Auftragsverarbeitern und anderen Vertragspartnern.[60] Wenn Daten an Dritte übermittelt werden, kann es bei vertrauenswürdigen Empfängern sinnvoll sein, zusätzlich die gewählte Anonymisierungstechnik

---

Art. 11 Rz. 60; *Weichert* in Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 11 Rz. 12; *Wolff* in BeckOK BDSG/DSGVO, 27. Edition 2019, Art. 11 Rz. 10a; ausführlich *Hansen* in Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 11 Rz. 16 ff.

54 *Wolff* in BeckOK BDSG/DSGVO, 27. Edition 2019, Art. 11 Rz. 10a.

55 *Wolff* in BeckOK BDSG/DSGVO, 27. Edition 2019, Art. 11 Rz. 16; *Weichert* in Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 11 Rz. 13; die Tatbestandsmerkmale werden in der Kommentarliteratur nur selten überhaupt diskutiert.

56 *Weichert* in Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 11 Rz. 13; dahingehend auch *Wirtz* in Taeger/Gabel, DSGVO/BDSG, 3. Aufl. 2019, Art. 11 Rz. 6; *Wolff* in BeckOK BDSG/DSGVO, 27. Edition 2019, Art. 11 Rz. 16, 17a; *Wedde* in Däubler et al., DS-GVO/BDSG, 2018, Art. 11 Rz. 8, 18.

57 Vgl. *Wolff* in BeckOK BDSG/DSGVO, 27. Edition 2019, Art. 11 Rz. 19.

58 *Wirtz* in Taeger/Gabel, DSGVO/BDSG, 3. Aufl. 2019, Art. 11 Rz. 12; *Wolff* in BeckOK BDSG/DSGVO, 27. Edition 2019, Art. 11 Rz. 18 f.; *Kampert* in Sydow, DSGVO, 2. Aufl. 2018, Art. 11 Rz. 7; *Veil* in Gierschmann et al., DS-GVO, 2018, Art. 11 Rz. 17 ff.

59 Vgl. *Hansen* in Simitis/Hornung/Spiecker gen. Döhmann, Datenschutzrecht, 2019, Art. 11 Rz. 33 f.; *Wolff* in BeckOK BDSG/DSGVO, 27. Edition 2019, Art. 11 Rz. 26; *Veil* in Gierschmann et al., DS-GVO, 2018, Art. 11 Rz. 38 ff.

60 S. z.B. *Wojtowicz/Cebulla*, PinG 2017, 186, 191.

offenzulegen, so dass der Dritte weiß, wie er die Daten zu verarbeiten hat, um Re-Identifizierbarkeit zu verhindern.[61] Wird der Personenbezug erkannt, könnte er unter Einsatz neuer, nunmehr dem *Stand der Technik* entsprechender Verfahren unmittelbar wieder beseitigt werden.[62]

43 Allerdings hat dieser Weg inhärente Grenzen. Zunächst handelt es sich um einen permanenten Wettlauf mit neuen Entwicklungen, die gerade auf eine Re-Individualisierung zielen. Da letztere vielfach ökonomische Vorteile verspricht, steht zu befürchten, dass die in der Praxis verfügbaren Forschungs- und Entwicklungsressourcen stark zu Ungunsten der Anonymisierungstechnologien allokiert würden.[63] Dem müsste mit öffentlicher Forschung entgegengewirkt werden; dies wird aber nur begrenzt möglich sein. Deshalb ist zwar die Forderung zu unterstützen, „Schutzreserven" bei der Anonymisierung einzubauen, um zukünftigen Risiken vorzubeugen.[64] Dies verlagert das Problem des technischen Wettlaufs aber nur, ohne es grundsätzlich zu lösen. Aus rechtlicher Sicht wird der freiwillige Einsatz effektiver und ggf. überobligatorischer Anonymisierungstechnologien sicherlich bei der Abwägung nach Art. 6 Abs. 1 Unterabs. 1 lit. f. DSGVO berücksichtigt werden. Wenn diese Technologien allerdings im Einzelfall gerade versagen, wird die Einzelfallbetrachtung wieder relevant.

44 Außerdem versagt die Verbesserung der Anonymisierung, wenn der Verantwortliche die Umstände, die zu einer schleichenden Identifizierbarkeit führen, nicht ändern kann oder nicht ändern will. So kann die Anreicherung des Datenbestandes um Zusatzinformationen Ausfluss der Einführung eines digitalisierten Produktionssystems sein, dessen Funktionalität durch innovative Anonymisierungstechniken eingeschränkt würde.[65] Die Abschottung von Datenbeständen ist auch dann nicht zielführend, wenn das Geschäftsmodell eines Unternehmens gerade auf der Zusammenführung und kontextübergreifenden Analyse von Daten basiert.

bb) Transparenz der Identifizierbarkeit

45 Der zweite technische Ansatz könnte darauf zielen, dem Verantwortlichen zumindest deutlich zu machen, dass ein Personenbezug nachträglich eingetreten ist.[66] Dies würde es (im Rahmen einer periodischen Prüfung innerhalb des Datenschutz-Managements)[67] ermöglichen, sodann entweder Maßnahmen zur Re-Anonymisierung zu ergreifen oder so rasch wie möglich die Einhaltung der datenschutzrechtlichen Vorgaben sicherzustellen. Denkbar wäre sogar, die nunmehr identifizierbare betroffene Person automatisiert zu informieren, so dass sie ggf. von ihren Betroffenenrechten Gebrauch machen kann.

46 Auch dieser Ansatz dürfte in der Praxis allerdings schwer umzusetzen sein. Die Frage der Identifizierbarkeit ist gemäß ErwGr 26 DSGVO nach wertenden Kriterien zu bestimmen, die einer Automatisierung nur begrenzt zugänglich sind. Gerade in den hier diskutierten Grenzfällen dürfte dies rasch an Grenzen stoßen. Überdies laufen Systeme, die automatisiert eine Identifizierbarkeit prüfen, rasch Gefahr, ihrerseits datenschutzrechtliche Probleme zu verursachen. Wenn nämlich regelmäßig geprüft wird, ob konkrete betroffene Personen „gerade so" identifizierbar sind, so würde kontinuierlich angestrebt, eine erfolgte Anonymisierung zu brechen. Dies läuft deren Sinn zuwider und könnte rechtlich mit Art. 11 Abs. 1 DSGVO in Konflikt kommen (s.o. IV.2.b)).

47 Denkbar erscheint immerhin, für konkrete und grundsätzliche Änderungen der Rahmenbedingungen (z.B. das Zuspeichern weiterer Informationen) durch technische Mechanismen zu prüfen, ob hierdurch ein Personenbezug entsteht. Überdies könnten sich derartige Mechanismen auch auf Datenbankstrukturen und das Auffinden von Datenkategorien beziehen, die bei typisierter Betrachtung für eine De-Anonymisierung anfällig sind.[68] Hierdurch könnten weitere Prüfprozesse angestoßen werden, ohne konkrete betroffene Personen aus dem Status der „gerade so" Identifizierbarkeit ans Licht zu zerren. Freilich setzen derartige Verfahren Erkenntnisse darüber voraus, ob bestimmte Datensammlungen nach Größe, Datenstruktur oder den Besonderheiten von Meta- oder Inhaltsdaten dazu tendieren, ein Risiko der De-Anonymisierung zu verursachen.

b) Präventive rechtliche Maßnahmen

48 Für die Fallgruppe der „gerade so" personenbezogenen Daten dürfte es regelmäßig wenig zielführend sein, im Zweifel von der Anwendbarkeit des Datenschutzrechts auszugehen,[69] denn das Problem liegt gerade darin, dass die Anwendbarkeit vieler Normen ohne genaue Kenntnis der betroffenen Person erhebliche Schwierigkeiten verursacht. In speziellen Fallgestaltungen könnte man dem Risiko der De-Anonymisierung aufgrund eines schleichenden Personenbezugs jedoch durch präventive rechtliche Maßnahmen begegnen. Wenn Daten beispielsweise zunächst personenbezogen erhoben und sodann anonymisiert werden, im Anschluss jedoch eine Personenbeziehbarkeit droht, könnte bereits zu Beginn (auch) für den Fall der Weiterverarbeitung unter diesen Bedingungen eine Einwilligung eingeholt werden.[70] Wurden die Daten dagegen von Anfang an in

---

61 *Art. 29-Datenschutzgruppe*, Stellungnahme 5/2014 zu Anonymisierungstechniken, WP 216, 2014, S. 30.

62 Dahingehend *Baeriswyl*, digma 2013, 14, 17. Dem rechtlichen Problem, dass mindestens für eine juristische Sekunde eine Bestimmbarkeit und damit einhergehend die Anwendbarkeit des Datenschutzrechts gegeben ist, könnte man durch eine risikoadäquate Auslegung und teleologische Reduktion der entsprechenden Normen begegnen.

63 Dies gilt in identischer Weise bei Verschlüsselungstechnologien. So sollen allein in der Zentralen Stelle für Informationstechnik im Sicherheitsbereich (Zitis) bis 2020 400 Mitarbeiter arbeiten. Diese Behörde wurde allein zu dem Zweck geschaffen, um effektive Entschlüsselungstechniken zu entwickeln. Siehe hierzu *Biermann/Beuth/Steiner*, Innenministerium plant drei neue Internet-Eingreiftruppen, http://www.zeit.de/digital/internet/2016-07/cyberangriffe-hacker-innenministerium-thomas-de-maiziere/komplettansicht?print.

64 Vorschlag bei *Schaar*, ZD 2016, 224, 225.

65 Zu diesem Problem der Datenschutzrelevanz von Produktionsdaten in der Industrie 4.0 *Seifert*, Arbeit in der digitalen Fabrik am Beispiel von Wertschöpfungsnetzwerken in Hornung, Rechtsfragen der Industrie 4.0, 2018, S. 178 ff.

66 In diese Richtung *Baeriswyl*, digma 2013, 14, 17.

67 Hierfür *Wójtowicz/Cebulla*, PinG 2017, 186, 190 f.; *Eßer* in Auernhammer, DSGVO/BDSG, 5. Aufl. 2017, § 3a Rz. 21b; *Marnau*, DuD 2016, 428, 429; ähnlich *Scholz* in Simitis, BDSG, 8. Aufl. 2014, § 3 Abs. 6a Rz. 219b.

68 S. für Ansätze zur Abschätzung der Erfolgswahrscheinlichkeit einer Re-Identifizierung z.B. *Rocher/Hendrickx/de Montjoye*, NATURE COMMUNICATIONS (2019) 10:3069, https://doi.org/10.1038/s41467-019-10933-3.

69 Hierfür wohl *Klabunde* in Ehmann/Selmayr, DS-GVO, 2. Aufl. 2018, Art. 4 Rz. 17.

70 Dahingehend auch *Härting*, NJW 2013, 2065, 2066; angesichts der praktischen Probleme kritisch *Baeriswyl*, digma 2013, 14, 16. Die Frage der

anonymer Form erhoben oder empfangen, ist dieser Weg verschlossen.

49 Ein sinnvolles Instrument können überdies Selbstverpflichtungen der Verantwortlichen sein, anonymisierte Daten nicht zu re-identifizieren[71] bzw. „gerade so" personenbezogene Daten nicht durch Anreicherung mit weiteren Daten in den Bereich der Identifiziertheit zu überführen. Dies könnte entweder mit einer einseitigen Erklärung oder – vorzugswürdig – mittels der Unterwerfung unter eine bindende und sanktionsbewehrte Verhaltensregel nach Art. 40 DSGVO erfolgen.[72]

50 Eine solche Selbstverpflichtung würde zwar nicht als solche den Anwendungsbereich des Datenschutzrechts ausschließen, da dieser gesetzlich geregelt ist. Vertretbar erscheinen aber folgende Effekte:

- *Verhinderung der Identifizierbarkeit:* Selbstverpflichtungen könnten Einfluss auf die Kriterien in ErwGr 26 S. 3 und 4 DSGVO nehmen und so dazu führen, dass eine Identifizierbarkeit bei „gerade so" personenbezogenen Daten verneint wird.[73] Anhaltspunkte für diesen Effekt lassen sich der Rechtsprechung des EuGH entnehmen. Danach werden gesetzlich verbotene Mittel vernünftigerweise nicht zur Identifizierung der betreffenden Person eingesetzt.[74] Eine vergleichbare Wirkung ließe sich auch bei einer – effektiven und sanktionsbewehrten – Selbstverpflichtung annehmen, wenn diese verbietet, „gerade so" personenbezogene Daten zu re-identifizieren.
- *Einfluss auf Abwägungsentscheidungen:* Selbstverpflichtungen könnten zugunsten des Verantwortlichen eine Abwägung nach Art. 6 Abs. 1 Unterabs. 1 lit. f DSGVO bzw. den sonstigen risikobezogenen Normen der DSGVO beeinflussen.[75] Verantwortliche könnten sich insofern auf eine generalisierende Interessensabwägung beschränken, was dazu führen könnte, dass sogar in bestimmten Big Data-Bereichen (z.B. solche, in denen keine sensiblen Daten verarbeitet werden) eine Verarbeitung von „gerade so" personenbezogenen Daten weitgehend zugelassen würde. Erst bei Kenntnis von entgegenstehenden individuellen Umständen der betroffenen Person wäre eine Neubewertung durchzuführen.

51 Derartige Selbstverpflichtungen könnten künftig sehr sinnvolle Instrumente sein. Allerdings dürfen sie nicht als echte Substitute zu einer Anonymisierung begriffen werden, sofern diese (z.B. nach den Grundsätzen der Datenminimierung oder Speicherbegrenzung nach Art. 5 Abs. 1 lit. c, e DSGVO) rechtlich erforderlich, technisch möglich und zumutbar ist. In diesem Fall ist die effektive Anonymisierung eine Rechtspflicht, die nicht durch das bloße Versprechen ersetzt werden kann, einen etwaigen Personenbezug nicht wieder herzustellen. Außerdem hätten ansonsten diejenigen, die sich um eine tatsächliche Anonymisierung bemühen, wirtschaftliche Nachteile, weil sie einen höheren technischen Aufwand haben und zugleich die Qualität der Daten durch die Anonymisierungsmaßnahmen (Generalisierung, Randomisierung)[76] typischerweise unschärfer wird; letzteres kann die Auswertungsmöglichkeiten und damit den Wert der Daten beeinträchtigen.

2. Lösungen de lege ferenda

52 Erweisen sich die oben aufgezeigten Lösungen als nicht hinreichend, können unterschiedliche Maßnahmen *de lege ferenda* ergriffen werden. So könnten in die DSGVO beispielsweise Konkretisierungen für die Kriterien aus ErwGr 26 S. 3 und 4 DSGVO bzw. für den Moment, ab dem von einer Anwendbarkeit des Datenschutzrechts auszugehen ist, aufgenommen werden. Entsprechende Kriterien zu entwickeln, erscheint allerdings schwierig, da die denkbaren Verarbeitungskonstellationen sehr heterogen sind und sich außerdem rasch ändern können.[77] Insofern dürfte es vorzugswürdig sein, innerhalb der DSGVO Konkretisierungen durch den *Europäischen Datenschutzausschuss* oder durch Selbstregulierungen für bestimmte Geschäftsfelder (mittels Codes of Conduct) vorzunehmen.

53 Daneben können auch gesetzliche Vorsorgeregelungen für den Umgang mit noch nicht personenbezogene Daten ergriffen werden, wie sie bereits im Modernisierungsgutachten aus dem Jahre 2001 empfohlen wurden.[78] Neben einer strikten Zweckbegrenzung könnten insofern Datenminimierung und Löschverpflichtungen mögliche Ansätze sein, um eine Re-Identifizierung betroffener Personen zu verhindern. Vergleichbare Regelungen könnten sich Unternehmen auch selbst geben und so ihrerseits darauf hinwirken, die Gefahr eines schleichenden Personenbezugs zu begrenzen. Des Weiteren könnten bestimmte Analysemethoden verboten oder Anonymisierungsstandards normiert werden, bei deren Einhaltung eine widerlegliche Vermutung bestünde, dass personenbezogene Daten hinreichend anonymisiert wurden.[79]

54 Abseits solcher Vermutungsregelungen sollte man auch den europäischen Weg überdenken, wonach anonymisierte Daten überhaupt nicht reguliert werden, während auf (auch „gerade so") personenbezogene Daten das gesamte Datenschutzrecht Anwendung findet. Anregungen könnten insofern dem japanischen Datenschutzrecht entnommen werden. Seit dessen Reform im Jahr 2017 enthält der „Act on the Protection of Personal Information" (APPI) nämlich auch Vorgaben zum Umgang mit anonymisierten Daten.[80] Unter anderem ist es nach Art. 36 Abs. 5 bzw. Art. 38 APPI Verantwortlichen verboten,

---

Umsetzbarkeit der Zulässigkeitsanforderungen an die Einwilligung dürfte kritisch sein und kann hier nicht diskutiert werden.

71 Ähnlich bereits *Roßnagel/Pfitzmann/Garstka*, Modernisierung des Datenschutzes, 2001, S. 69.

72 Der Katalog der Regelungsgegenstände in Art. 40 Abs. 2 DSGVO nennt zwar nur die Pseudonymisierung, nicht die Anonymisierung bzw. deren Aufrechterhaltung. Die Liste ist aber explizit nicht abschließend.

73 Für den Fall von Vertragsstrafen *Arning/Rothkegel* in Taeger/Gabel, DSGVO/BDSG, 3. Aufl. 2019, Art. 4 Rz. 31.

74 EuGH v. 19.10.2016 – C-582/14 , ECLI:EU:C:2016:779 Rz. 46, CR 2016, 791 m. Anm. *Nink* – Breyer.

75 Vgl. *Klar/Kühling* in Kühling/Buchner, DS-GVO/BDSG, 2. Aufl. 2018, Art. 4 Nr. 1 Rz. 17, die der Unterscheidung zwischen Identifiziertheit und Identifizierbarkeit im Rahmen der Interessenabwägung Bedeutung zukommen lassen wollen; in eine ähnliche Richtung auch *Baeriswyl*, digma 2013, 14, 16.

76 S. zu den Methoden Fn. 15.

77 Diese Volatilität lässt es auch unwahrscheinlich erscheinen, dass konkretisierende Fallgruppen der Rechtsprechung das Problem lösen, zumal diese nicht eigeninitiativ tätig werden kann.

78 S. *Roßnagel/Pfitzmann/Garstka*, Modernisierung des Datenschutzes, 2001, S. 68 ff.; dahingehend auch *Baeriswyl*, digma 2013, 14, 17.

79 Ähnlich *Specht*, GRUR-Int. 2017, 1040, 1046, die aber eine unwiderlegliche Vermutung präferiert.

80 S. ausführlich *Geminn/Laubach/Fujiwara*, ZD 2018, 413, 417 ff.; grundlegend zum neuen japanischen Datenschutzrecht *Hoeren/Wada*, ZD 2018, 3; *Geminn/Fujiwara*, ZD 2016, 363.

anonymisierte Daten mit anderen Daten zusammenzuführen, um die betroffene Person zu identifizieren.[81]

55 Ein solches Verbot ist dem deutschen Recht auch nicht fremd. Vielmehr existiert mit § 21 BStatG bereits heute eine vergleichbare Vorschrift für den Bereich der Bundesstatistiken. Ein Re-Identifizierungsverbot ließe sich insofern auch in die DSGVO einfügen:[82] Danach könnte es Verantwortlichen verboten sein, durch Anreicherung aus anonymen Daten („gerade so") personenbeziehbare Daten oder aus personenbeziehbaren Daten personenbezogene Daten zu machen. Freilich bestünde auch in diesem Fall noch das Grundproblem, dass Kriterien entwickelt werden müssten, um zu ermitteln, wann „gerade so" personenbezogene Daten vorlägen und das Re-Identifizierungsverbot einschlägig wäre. Auch muss bedacht werden, dass ein derartiges Verbot Gefahr laufen könnte, völlig legitime innovative Geschäftsmodelle zu verhindern. Schließlich mag es Verantwortliche geben, die trotz Deanonymisierung ihre Daten rechtskonform verarbeiten, weil sie sich z.B. auf Art. 6 Abs. 1 Unterabs. 1 lit. f DSGVO stützen können und auch im Übrigen mit der Anwendung des Datenschutzrechts kein grundsätzliches Problem haben.

VI. Fazit

56 Angesichts steigender Datenmengen und neuer Analysemethoden dürften es zukünftig Anonymisierungsverfahren immer seltener schaffen, auf Dauer einen hinreichenden Wirkungsgrad zu erreichen.[83] Dies kann Verantwortliche vor einige Probleme stellen. Will man dennoch Big Data-Anwendungen mit dem Persönlichkeitsschutz der betroffenen Personen in Einklang bringen, sollten Verantwortliche technische und rechtliche Präventionsmaßnahmen ergreifen.

57 Für die nähere Zukunft ist allerdings selbst dann keine vollständige Rechtssicherheit zu erlangen. Hierfür bedarf es *erstens* weiterer Konkretisierungen, wann man bei Big Data-Anwendungen von einer Identifizierbarkeit der betroffenen Personen ausgehen muss. Hierzu sind Taxonomien und Best Practices zu entwickeln. *Zweitens* sollte empirisch untersucht werden, wie groß das Problem des schleichenden Personenbezugs tatsächlich in der Praxis ist. Insbesondere sind hierbei Fallgruppen zu erarbeiten, in denen es zu einer nachträglichen Identifizierbarkeit kommt oder kommen kann. *Drittens* muss näher betrachtet werden, in welchen dieser Fallgruppen grundsätzlich legitime innovative Geschäftsmodelle verfolgt werden, die man beschränken oder verhindern würde, wenn man z.B. ein Re-Identifizierungsverbot einführen würde.

58 Erst mittels derartiger Untersuchungen wird sich abschließend klären lassen, ob dem Problem mit dem geltenden Recht angemessen begegnet werden kann oder bzw. welche Maßnahmen ergriffen werden müssen. Denjenigen Unternehmen, die betroffen sind, sollten nichtsdestotrotz die Herausforderungen mit den unter V.1. genannten Ansätzen adressieren, um nicht in Haftungsprobleme zu laufen, für die sie nicht gerüstet sind.

Prof. Dr. Gerrit Hornung, LL.M.

Universitätsprofessor an der Universität Kassel, Fachgebiet Öffentliches Recht, IT-Recht und Umweltrecht; Direktor am Wissenschaftlichen Zentrum für Informationstechnik-Gestaltung (ITeG) der Universität Kassel

IT-Recht, Datenschutzrecht, E-Government

gerrit.hornung@uni-kassel.de

https://www.uni-kassel.de/fb07/hornung

Bernd Wagner

Wissenschaftlicher Mitarbeiter an der Universität Kassel, Fachgebiet Öffentliches Recht, IT-Recht und Umweltrecht und Wissenschaftlichen Zentrum für Informationstechnik-Gestaltung (ITeG) der Universität Kassel

Datenschutzrecht, Rechtsfragen von smarten Assistenzsystemen

bernd.wagner@uni-kassel.de

81 *Geminn/Laubach/Fujiwara*, ZD 2018, 413, 419.

82 Hierfür z.B. auch *Specht*, GRUR-Int. 2017, 1040, 1046; kritisch *Ohm*, UCLA Law Review (57) 2010, 1701, 1758 f.

83 So auch *Ernst* in Paal/Pauly, DS-GVO/BDSG, 2. Aufl. 2018, Art. 4 Rz. 50; *Roßnagel*, SVR 2014, 281, 284; *Tene/Polonetsky*, Stanford Law Review Online (64) 2012, 63, 65; *Boehme-Neßler*, DuD 2016, 419, 422 f., geht angesichts von Big Data-Anwendungen sogar von der völligen Wirkungslosigkeit von Anonymisierungstechniken aus.

Rechtsprechung

EuGH: Arbeitsteiliges Zusammenwirken datenschutzrechtlich Verantwortlicher – Fashion ID

Richtlinie 95/46/EG Art. 2, 7, 10, 22, 23 und 24

1. Die Art. 22 bis 24 der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24.10.1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr sind dahin auszulegen, dass sie einer nationalen Regelung, die es Verbänden zur Wahrung von Verbraucherinteressen erlaubt, gegen den mutmaßlichen Verletzer von Vorschriften zum Schutz personenbezogener Daten Klage zu erheben, nicht entgegenstehen.

2. Der Betreiber einer Website wie die Fashion ID GmbH & Co. KG, der in diese Website ein Social Plugin einbindet, das den Browser des Besuchers dieser Website veranlasst, Inhalte des Anbieters dieses Plugins anzufordern und hierzu personenbezogene Daten des Besuchers an diesen Anbieter zu übermitteln, kann als für die Verarbeitung Verantwortlicher i.S.v. Art. 2 Buchst. d der Richtlinie 95/46 angesehen werden. Diese Verantwortlichkeit ist jedoch auf den Vorgang oder die Vorgänge der Verarbeitung personenbezogener Daten beschränkt, für den bzw. für die er tatsächlich über die Zwecke und Mittel entscheidet, d.h. das Erheben der in Rede stehenden Daten und deren Weitergabe durch Übermittlung.