Prof. Dr. Louisa Specht, Universität Passau

Das Verhältnis möglicher Datenrechte zum Datenschutzrecht

I. Einleitung

Vielfach ist in den letzten Jahren als Reaktion auf eine zunehmende Datengetriebenheit der Wirtschaft über ein mögliches „Datenrecht" diskutiert worden. Diese Diskussion leidet jedoch daran, dass sie mit ganz unterschiedlichen Intentionen geführt wird. Beabsichtigt die EU-Kommission mit ihrem „Datenerzeugerrecht"[1] im Wesentlichen klare Regeln für Datenmärkte zu schaffen, existieren ebenso Ansätze, die v.a. den Betroffenen an den mit den ihn betreffenden personenbezogenen Daten generierten Gewinnen beteiligen und ihm daher über die bloße Abwehrbefugnis des Datenschutzrechts hinausgehende Rechtspositionen an Daten zuweisen wollen.[2]

Zweiter Angriffspunkt der Diskussion ist, dass ein mögliches Datenrecht sehr heteronome Fallkonstellationen erfassen soll, in denen unterschiedliche Interessenlagen bestehen. Eine umfassende Aufarbeitung und Analyse dieser Fallgruppen ist bislang nicht erfolgt. Es fragt sich bereits, ob all diese Fallkonstellationen mit einem einheitlichen Datenrecht gelöst werden können oder ob es möglicherweise sektorspezifischer Lösungen bedarf.

Auf einer abstrakteren Ebene sind die Argumente für und wider möglicher Ausgestaltungs- und Zuweisungsoptionen eines Datenrechts bereits umfassend ausgetauscht,[3] ebenso wie bereits über eine möglicherweise fehlende ökonomische[4] und verfassungsrechtliche[5] Legitimation diskutiert wurde. Ohne auf diese Streitpunkte im Einzelnen eingehen zu wollen,

---

[1] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions, "Building a European Data Economy", COM 2017(9), S.13 ff.
[2] In diese Richtung etwa: *Schwartmann/Hentsch*, PinG 2016, 117 ff.
[3] Vgl. insb. *Becker*, GRUR 2017, 346 ff.; *Wiebe*, GRUR 2017, 338 ff.; *Börding/Jülicher/Röttgen/Schönfeld*, CR 2017, 134 ff.; *Wandtke*, MMR 2017, 6 ff.; *Fezer*, MMR 2017, 3 ff.; *Drexl*, Designing Competitive Markets for Industrial Data - Between Propertisation and Access, 2016, MPI for Innovation & Competition Research Paper No. 16-13, abrufbar unter: https://ssrn.com/abstract=2862975; *Kerber*, GRUR Int. 2016, 989 ff.; *Spindler*, JZ 2016, 805 ff.; *Heymann*, CR 2016, 650 ff.; *Härting*, CR 2016, 646 ff.; *Specht*, CR 2016, 288 ff.; *Dorner*, CR 2014, 617; *Hoeren*, MMR 2013, 486, 488; *Zech*, CR 2015, 137; *ders*., Information als Schutzgegenstand, 2012.
[4] *Kerber*, GRUR Int. 2016, 989 ff.
[5] *Wiebe/Schur*, ZUM 2017, 461 ff.

sei an dieser Stelle jedenfalls daran erinnert, dass ein mögliches Recht an Daten nicht unbedingt ein allumfassendes, eigentumsähnlich gestaltetes Recht sein muss. Ebenso ist es möglich, über Zugriffsrechte an Daten nachzudenken[6] oder Einzelbefugnisse branchenspezifisch zuzuweisen.[7] Bereits heute lassen sich Daten als Gegenstand von Verträgen erfassen und zwar sowohl als Leistungsgegenstand,[8] als auch als Gegenleistung.[9] Alternativ zu einem Recht an Daten könnten daher auch Standardvertragsklauseln die Befugnisse an Daten interessengerecht verteilen.

All diese Befugnisse an Daten, die sich durch Zuweisung exklusiver oder nicht-exklusiver Rechte sowie vertragsrechtlich verteilen ließen, müssen sich jedoch die Frage nach ihrem Verhältnis zum Datenschutzrecht gefallen lassen. Dieses Verhältnis zu erörtern, ist Gegenstand des vorliegenden Beitrags. Das Datenschutzrecht lässt dabei Differenzierungsmöglichkeiten zwischen verschiedenen Datenverarbeitungszwecken zu. Es bietet sich daher an, von einem phänomenologischen Befund möglicher Anwendungsfälle eines Datenrechts auszugehen (II.) und in einem nächsten Schritt die verschiedenen Rollen des Datenschutzrechts bei der Ausgestaltung möglicher Datenrechte zu erörtern (III.). Dabei kann es sich in Anbetracht der Vielzahl möglicher Fallkonstellationen nicht um eine abschließende, sondern allein um eine beispielhafte Aufzählung handeln. Der Beitrag schließt mit einem Fazit und einer Zusammenfassung der Ergebnisse (IV).

II. Anwendungsfälle

Mögliche Rechte an Daten würden sehr heteronome Fallkonstellationen betreffen. Diese Fallkonstellationen lassen sich einteilen in solche Fälle, in denen Zugriffs- und Nutzungsinteressen verschiedener Akteure aus kommerziellen Gründen bestehen und solche Fälle, in denen die Interessen der datenverarbeitenden Stelle jedenfalls primär auf die Verfolgung nicht-kommerzieller Interessen, z.B. Sicherheitsinteressen, wissenschaftliche Forschung, Archivierungszwecke etc. gerichtet sind.

---

[6] Dazu v.a. *Drexl*, Designing Competitive Markets for Industrial Data - Between Propertisation and Access, 2016, MPI for Innovation & Competition Research Paper No. 16-13, abrufbar unter: https://ssrn.com/abstract=2862975.

[7] Dazu jüngst: *Dreier*, in: Weller et all Tagungsband zum XI. Heidelberger Kunstrechtstag, im Erscheinen.

[8] *Specht*, Ökonomisierung informationeller Selbstbestimmung - Die zivilrechtliche Erfassung des Datenhandels, 2012.

[9] *Specht*, JZ 2017, 763 ff.; *Metzger*, AcP 2016, 817 ff.

So haben beim autonom fahrenden PKW sowohl der Autohersteller, als auch der Hersteller der im PKW verbauten Software ein Interesse an Rechtspositionen an den verschiedenen Daten über das Fahrverhalten des Eigentümers, weil sich diese lukrativ an Versicherungen weiterreichen lassen. Krankenkassen und Produzenten haben ein Interesse an den mittels Smart Devices (etwa Fitnesstrackern oder entsprechender Apps) generierten Daten, um ihre Tarife gezielter dem individuellen Verhalten der Betroffenen anpassen zu können und damit das Eigenrisiko des Versicherungsträgers zu verringern.

Bewertungsportale und Soziale Netzwerke haben ein Interesse an einem möglichst umfassenden Recht an den auf ihren Seiten generierten Bewertungen und anderen Daten, sind diese doch häufig der wesentliche Vermögenswert, über den sie verfügen.

Weitere Anwendungsfälle sind Datenerhebungen im Smart Home und über das Smart Metering, etwa Datenerhebungen über das Heizverhalten, das Sicherheitsverhalten (automatische Verriegelung von Türen, Zeitschaltuhren bei Lampen, automatische Regulierung der elektrischen Jalousien etc.), den Wasserverbrauch etc.

All diese Datenerhebungen zielen in der Regel darauf, sie mittels Big-Data Anwendungen umfassend auszuwerten, Nutzerprofile zu bilden und damit individualisierte Werbung entwickeln und schalten zu können. In dieselbe Richtung zielen Kundenkartensysteme, mit denen das Einkaufsverhalten analysiert werden soll oder Clickstream-Analysen im Netz.

Neben der Schaltung individualisierter Werbung ist die Auswertung von Daten aber auch zur Verhaltensvorhersage z.B. von Wählern, Versicherungsnehmern, Arbeitnehmern etc. interessant. Denn durch die Auswertung personenbezogener Daten lässt sich besonders präzise die Persönlichkeit der Betroffenen ablesen. Bereits 2012 wurde der Nachweis erbracht, dass man aus durchschnittlich 68 Facebook-Likes eines Users vorhersagen kann, welche Hautfarbe er hat (95-prozentige Treffsicherheit), ob er homosexuell ist (88-prozentige Treffsicherheit), ob Demokrat oder Republikaner (85 Prozent). Auch Intelligenz,

Religionszugehörigkeit, Alkohol-, Zigaretten- und Drogenkonsum lassen sich berechnen.[10] Anhand von zehn Facebook-Likes lässt sich eine Person besser einschätzen als dies ein durchschnittlicher Arbeitskollege könnte. 70 Likes reichen, um die Menschenkenntnis eines Freundes, 150 um die der Eltern zu überbieten. Mit 300 Likes lässt sich das Verhalten einer Person eindeutiger vorhersagen als dies deren Partner könnte. Und mit noch mehr Likes lässt sich sogar übertreffen, was Menschen von sich selber zu wissen glauben.[11] Selbst der Staat könnte Interesse an diesen Daten zur Prävention von Straftaten haben. *Mayer-Schöneberger/Cukier* beschreiben schon 2013, wie aufgrund von personenbezogenen Daten die Wahrscheinlichkeit des Einzelnen zur Begehung von Straftaten abgeschätzt werden kann.[12]

Neben der individuellen Werbeansprache und der Verhaltensvorhersage existieren aber durchaus auch anders gelagerte Interessen zur Datenerhebung. So werden gewisse Daten autonom fahrender Fahrzeuge benötigt, um das Fahrzeug überhaupt autonom fahren lassen zu können (bspw. die Bewegungsdaten des PKW). In der Industrie 4.0 werden unterschiedlichste Daten zu unterschiedlichsten Zwecken generiert. In der medizinischen Forschung werden Daten jedenfalls auch zu wissenschaftlichen Zwecken verarbeitet. Dass hinter all diesen Datenverarbeitungen jedenfalls auch ein kommerzielles Interesse stehen kann, sollte den Blick darauf, dass die Datenverarbeitung hier in erster Linie zu Zwecken des wissenschaftlichen Fortschritts, zur Weiterentwicklung der Sicherheit von Produkten oder auch zur Verbesserung der Produktsicherheit und damit letztlich auch im Interesse der Allgemeinheit erfolgt, nicht verstellen. Diese gesamtgesellschaftlich relevanten Interessen müssen datenschutzrechtlich möglicherweise anders behandelt werden, als rein kommerzielle Interessen.

III. Verhältnis zwischen Datenrechten und Datenschutz

[10] *Grassegger/Krogerus*, Das Magazin Nr. 48/2016, „Ich habe nur gezeigt, dass es die Bombe gibt", abrufbar unter: https://www.dasmagazin.ch/2016/12/03/ich-habe-nur-gezeigt-dass-es-die-bombe-gibt/, zuletzt abgerufen am 15.08.2017.
[11] *Grassegger/Krogerus*, Das Magazin Nr. 48/2016, „Ich habe nur gezeigt, dass es die Bombe gibt", abrufbar unter: https://www.dasmagazin.ch/2016/12/03/ich-habe-nur-gezeigt-dass-es-die-bombe-gibt/, zuletzt abgerufen am 15.08.2017.
[12] *Mayer-Schöneberger/Cukier*, Big Data, 2013, S. 199; zur Verhaltensvorhersage mittels Big Data-Analysen vgl. auch: *Boehme-Neßler*, DuD 2016, 419, 421.

In der Gemengelage unterschiedlicher Fallkonstellationen und Interessenlagen das Verhältnis zwischen verschiedenartig denkbaren Rechtspositionen in unterschiedlichsten Fallkonstellationen und dem Datenschutzrecht zu erörtern, scheint nicht trivial. Im Grundsatz lässt sich das Verhältnis zwischen einem Datenrecht, das auch an personenbezogenen Daten bestehen soll, und dem Datenschutzrecht auf dreierlei Art und Weise denken.

1. Das Datenschutzrecht als Instrument der Zuweisung von Rechten an Daten

Das Datenschutzrecht kann erstens als Zuweisungsinstrument möglicher Datenrechte herangezogen werden. Dies erfordert es freilich, das Datenschutzrecht aus seinem bisherigen Grundverständnis als alleiniges Schutzinstrument zugunsten des Betroffenen, das sich einer Kommerzialisierung verschließt, herauszulösen. Unabhängig davon, ob dies aufgrund des Menschenwürdebezugs des informationellen Selbstbestimmungsrechts und den Aussagen im Volkszählungsurteil (*„Der Einzelne hat nicht ein Recht im Sinne einer absoluten, uneinschränkbaren Herrschaft über "seine" Daten;[…]. Information, auch soweit sie personenbezogen ist, stellt ein Abbild sozialer Realität dar, das nicht ausschließlich dem Betroffenen allein zugeordnet werden kann")* überhaupt möglich[13] und wünschenswert ist, kann ein dem datenschutzrechtlich Betroffenen zustehendes „Datenrecht" überhaupt nur dort überzeugende Lösungen liefern, wo personenbezogene Daten in Rede stehen. Für ein auch nicht-personenbezogene Daten betreffendes Recht gewährleistet es indes kein taugliches Zuordnungskriterium. Es wird in vielen Situationen allerdings nur schwer möglich sein, personenbezogene von nicht-personenbezogenen Daten zu differenzieren. Einerseits ist der Begriff des Personenbezugs im Datenschutzrecht sehr weit,[14] sodass eine Vielzahl der betroffenen Daten personenbezogen sein werden. Andererseits ist es jedenfalls theoretisch durchaus möglich, durch Anonymisierung den Personenbezug zu beseitigen oder von Beginn an nicht-personenbezogene Daten zu verarbeiten, etwa Daten über das Wetter, die Bodenbeschaffenheit etc. Auch nicht-personenbezogene Daten können aber durch Hinzufügung weiterer Daten wiederum zu personenbezogenen Daten werden, sodass es

[13] Vgl. hierzu: *Specht/Rohmer*, PinG 2016, 127.

[14] Zur Reichweite des Personenbezugs vgl. insb. *EuGH*, GRUR Int. 2016, 1169 – *Breyer; Klabunde,* in: Ehmann/Selmayr, Datenschutz-Grundverordnung, 1. Aufl. (2017), Art. 4 Rdnr. 5 ff.; *Ziebart,* in: Sydow, Europäische Datenschutzgrundverordnung, 1. Aufl. (2017), Art. 4 Rdnr. 7 ff.; *Ernst*, in: Paal/Pauly, Datenschutz-Grundverordnung, 1. Aufl. (2017), Art. 4 Rdnr. 3 ff.; *Gola,* in: Gola, Datenschutz-Grundverordnung, 1. Aufl. (2017), Art. 4 Rdnr. 3 ff.

widersinnig scheint, bei der Etablierung von Rechten an Daten zwischen personenbezogenen und nicht-personenbezogenen Daten zu differenzieren.

2. Das Datenschutzrecht als Instrument zur Beteiligung des Betroffenen

Ist die Funktion des Datenschutzrechts als Zuweisungsinstrument beschränkt, so ließe es sich weiterhin als Beteiligungsinstrument des Betroffenen an den mit „seinen" personenbezogenen Daten generierten Gewinnen denken.[15] Unklar ist hierbei aber, nach welchen Grundsätzen eine solche Beteiligung erfolgen könnte. Welcher Gewinnanteil eines Unternehmens auf die Verarbeitung eines konkreten Datums entfällt, ist kaum feststellbar. Praktisch nur schwerlich umsetzbar erscheint auch die Etablierung einer „Verwertungsgesellschaft Daten", denn wer weiß schon, wo er welche Daten hinterlässt? Die Datenerhebung erfolgt oft genug mit nur rudimentärer Kenntnis des Betroffenen (man denke nur an Cookies, Datenauswertungen in Sozialen Netzwerken oder bei Kundenkartenprogrammen). Eine Meldung der Datenhingabe wäre aber zwingend erforderlich, um eine Ausschüttung für die Datenverarbeitung zu erhalten.

Ob das Datenschutzrecht einer solchen Beteiligung des Betroffenen entgegenstehen würde, weil es den Betroffenen nicht dazu animieren soll, die ihn betreffenden personenbezogenen Daten zu einem möglichst hohen Preis und in möglichst großer Anzahl hinzugeben, sondern es ihn gerade vor einer nicht mehr der Kontrolle des Betroffenen unterliegenden Datenverarbeitung schützen soll, ist sicherlich streitbar. Hier bestehen Schutzpflichten des Staates, den Bürger nicht zum reinen Objekt der Datenverarbeitung verkommen zu lassen. Das Märchen, dass eine Beteiligungsmöglichkeit der Betroffenen an den mit ihren Daten generierten Gewinnen auch zu einem bewussteren Umgang mit den eigenen personenbezogenen Daten führen wird, soll hier gar nicht erst erzählt werden. Im Gegenteil: Ein selbstbestimmter, bewussterer Umgang mit personenbezogenen Daten wird nur dann erfolgen, wenn es endlich gelingt, dem Betroffenen vor Augen zu führen, in welche Datenverarbeitungen er einwilligt und welche Rechte ihm zur Verfügung stehen. Die Visualisierung von Informationen scheint hier jedenfalls ein Versuch wert zu sein.

[15] Hierzu statt vieler: *Schwartmann/Hentsch*, PinG 2016, 117.

Nichtsdestotrotz zeigt aber insbesondere die im Entwurf vorliegende Richtlinie für digitale Inhalte, dass es vermehrt zu einer Kommerzialisierung personenbezogener Daten kommt, die auch durch den Gesetzgeber anerkannt werden soll. Eine – sicherlich schwierig zu begründende – Vereinbarkeit des Richtlinienentwurfs für digitale Inhalte mit Art. 8 GrCh unterstellt, ließe sich einfachgesetzlich jedenfalls dann, wenn Daten als Gegenleistung im synallagmatischen Vertrag hingegeben werden, ein Abschlag auf das zu erwerbende Produkt verpflichtend ausgestalten. Eine Entsprechung der urheberrechtlichen Verpflichtung zur Zahlung einer angemessenen Vergütung, § 32 UrhG, scheint hier theoretisch denkbar, praktisch aber kaum umsetzbar, solange eine konkrete Berechnungsmethode für den Wert von Daten fehlt. Die ökonomische Forschung in diesem Bereich steht leider noch am Anfang.

3. Datenschutz als Instrument der Beschränkung eines Datenrechts

Werden Rechte an Daten einer anderen Person als dem Betroffenen zugewiesen, beschränkt das Datenschutzrecht ein solches Recht, wie auch das Recht am eigenen Bild mögliche Urheber- oder Leistungsschutzrechte an einer Fotografie beschränkt. Das würde für Ausschließlichkeitsrechte an Daten ebenso gelten wie für bloße Zugriffsrechte. Denn auch der Zugriff auf Daten ist eine datenschutzrechtlich relevante Handlung, die dem Verbotsprinzip unterliegt. Eine Beschränkung durch das Datenschutzrecht trifft ebenso einen rein vertragsrechtlichen Umgang mit Daten.

a) Reichweite der Beschränkung durch das Datenschutzrecht

Theoretisch lässt sich das Verhältnis zwischen möglichen Rechtspositionen an Daten und dem Datenschutzrecht damit durchaus sinnvoll denken. Es stellt sich jedoch das Problem, dass die Beschränkung durch das Datenschutzrecht so weit reichen kann, dass mögliche Datenrechte oder auch vertragsrechtliche Positionen an Daten jedenfalls in ihrer Nutzungskomponente gänzlich entleert werden. Datenrechte sollen die Realität einfangen, in der zunehmend mit Daten umgegangen, in der sie zum dominierenden Wirtschaftsfaktor werden.[16] Jedenfalls einer Reihe von, wenn auch nicht allen Anwendungsfällen eines möglichen Datenrechts, ist der massenhafte Umgang, insbesondere die intendierte Auswertung von Daten mittels Big-

[16] Vgl. hierzu eingehend: *Van Asbroeck/Debussche/César*, Building the European Data Economy, Data Ownership, White Paper, 2017.

Data Analysemethoden gemein.[17] Die Datenschutzgrundverordnung ist aber auf einen solch massenhaften Umgang mit personenbezogenen Daten nicht zugeschnitten. Möchte man sich nicht darauf verlassen, dass im Einzelfall ein Erlaubnistatbestand die Datenverarbeitung rechtfertigt, wird man in der Regel eine datenschutzrechtliche Einwilligung einholen. Diese Einwilligung muss informiert erfolgen, d.h. dem Betroffenen sind alle Informationen über die Datenverarbeitung mitzuteilen, damit er überhaupt einwilligen kann. Dies erscheint aber umso schwieriger, je mehr Daten erhoben werden und je weiter der Verarbeitungszweck reicht. Ob eine Informiertheit im Falle von Big-Data Anwendungen überhaupt hergestellt werden kann, ist mehr als fraglich. Die jederzeitige Widerruflichkeit der Einwilligung führt außerdem dazu, dass auch der Inhaber möglicher Datenrechte sich nicht darauf verlassen kann, mit den Daten tatsächlich nach seinem Belieben verfahren zu können. Weiterhin problematisch ist die Einhaltung vom Zweckbindungs-, Transparenz- und Datenminimierungsgrundsatz.

Erscheint die Einwilligung zunehmend ungeeignet, eine Datenverarbeitung in möglichen Anwendungsfällen eines Datenrechts zu rechtfertigen oder verstößt die Mehrzahl der intendierten Anwendungsfälle eines möglichen Datenrechts per se gegen datenschutzrechtliche Grundsätze, so müsste konstatiert werden, dass sich Datenrecht und Datenschutz trotz einer theoretisch möglichen Ausgestaltung ihres Verhältnisses nicht sinnvoll gemeinsam denken lassen und es für eine Förderung der datengetriebenen Ökonomie, wie sie derzeit im Entstehen und politisch gewollt ist, Änderungen des Datenschutzrechts bedarf.

aa) Zweckbindungsgrundsatz

Bereits Art. 8 GrCh enthält die Vorgabe, dass personenbezogene Daten nur für festgelegte Zwecke verarbeitet werden dürfen. Der Zweckbindungsgrundsatz ist das beherrschende Prinzip des Datenschutzrechts.[18] Er legitimiert die Verarbeitung der Daten und erfordert es, dass der Zweck der Datenverarbeitung gem. Art. 5 Abs. 1 lit. b) Hs. 1 festgelegt, eindeutig und legitim sein muss. Das Merkmal der Festlegung ist dabei formal zu verstehen, die Eindeutigkeit

[17] Zu den möglichen Anwendungsfällen von Big-Data-Analysen vgl. *Orthmann/Schwierig*, NJW 2014, 2984, 2984.

[18] *Dammann*, ZD 2016, 307, 311; *Frenzel,* in: Paal/Pauly (o. Fußn. 14), Art. 5 Rdnr. 23: „Dreh- und Angelpunkt"; *Schantz,* in: BeckOK Datenschutzrecht, 20. Ed. (2017), Art. 5 DSGVO Rdnr. 13: „beherrschendes Konstruktionsprinzip".

richtet sich an den materiellen Zweckgehalt.[19] Legitim ist ein Zweck zunächst dann, wenn der Betroffene den Verantwortlichen durch Einwilligung ermächtigt hat, die ihn betreffenden personenbezogenen Daten zu verarbeiten. Weiterhin ist der Zweck legitim, der gesetzlich vorgesehen ist.[20] Es kommt aber nicht nur darauf an, dass die Datenverarbeitung insgesamt rechtmäßig, sondern dass der Zweck nicht von der Rechtsordnung missbilligt ist. Dabei sind auch ethische Erwägungen und gesellschaftliche Gewohnheiten zu berücksichtigen.[21] Ein rechtlich missbilligter Zweck wäre etwa die Diskriminierung bestimmter Personengruppen aus rassistischen Motiven.[22] Steht der Zweck aber insgesamt mit der Rechtsordnung im Einklang, so ist er legitim. Es handelt sich damit lediglich um einen groben Filter, illegitime Zwecke von vornherein auszuscheiden.[23]

Der Zweck ist vor der Datenverarbeitung festzulegen, eine Verarbeitung zu noch unbekannten Zwecken scheidet aus.[24] Auch eine pauschale Zweckangabe ist nicht ausreichend.[25] Dies folgt bereits daraus, dass die Zweckbindung als Rechtmäßigkeitsvoraussetzung der Datenverarbeitung nur bei eindeutig festgelegten Zwecken sinnvoll ist.[26] Nach dem Grundsatz der Erforderlichkeit dürfen nur solche Daten erhoben werden, die der Zweckerreichung dienen.[27] Für die Zweckerfüllung nicht mehr erforderliche Daten sind zu löschen.[28] Die erforderliche Präzision der Zweckangabe hängt zwar vom Einzelfall ab, jedenfalls aber darf der Zweckbindungsgrundsatz nicht durch einen allumfassenden Primärzweck ausgehebelt werden.

---

[19] *Frenzel,* in: Paal/Pauly, (o. Fußn. 14), Art. 5 Rdnr. 27.
[20] *Frenzel,* in: Paal/Pauly, (o. Fußn. 14), Art. 5 Rdnr. 28.
[21] Art. 29 Gruppe, S. 20, opinion 03/13 on purpose limitation, 00569/13/ENWP203, abrufbar unter: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf, zuletzt abgerufen am: 09.09.2017; *Monreal*, ZD 2016, 507, 509.
[22] Vgl. *Helbig*, K&R 2015, 145, 146.
[23] *Schantz,* in: BeckOK Datenschutzrecht (o. Fußn. 18), Art. 5 DSGVO Rdnr. 17.
[24] *BVerfG*, NJW 1984, 419, 422 - Volkszählung; *Schantz,* in: BeckOK Datenschutzrecht (o. Fußn. 18), Art. 5 DSGVO Rdnr. 13
[25] *Culik/Döpke*, ZD 2017, 226, 227; *Bergmann/Möhrle/Herb,* Datenschutzrecht, 50. EL (2016), § 4 Rdnr. 43.
[26] *Kring*, Big Data und der Grundsatz der Zweckbindung, 2015, S. 555 m.w.Nachw., abrufbar unter: https://subs.emis.de/LNI/Proceedings/Proceedings232/551.pdf, zuletzt abgerufen am: 11.08.2017.
[27] Zum Grundsatz der Erforderlichkeit vgl. *Gola/Klug/Körffer*, in: Gola/Schomerus, BDSG, 12. Aufl. (2015), § 28 Rdnr. 14 ff.; *Culik/Döpke*, ZD 2017, 226, 227.
[28] Art. 29 Gruppe, opinion 03/13 on purpose limitation, 00569/13/ENWP203, abrufbar unter: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf, zuletzt abgerufen am: 09.09.2017.

Den Zweck der Datenverarbeitung flexibel zu halten, ist aber gerade Wesensmerkmal der Auswertung großer Datenmengen.[29] Über den Einsatz verschiedener Analyse-Algorithmen wird nach bislang unbestimmten Zusammenhängen zwischen den Daten gesucht, indem Daten, die auf den ersten Blick nichts miteinander zu tun haben, zueinander in Beziehung gesetzt werden.[30] Big-Data Analysen auf einen Zweck zu begrenzen, erscheint daher schwierig.

(1) Datenverarbeitung zu statistischen Zwecken

Das BVerfG hat allerdings bereits im Volkszählungsurteil festgestellt, dass bei der Datenerhebung für statistische Zwecke eine enge und konkrete Zweckbindung der Daten nicht verlangt werden kann. Denn es gehöre zum Wesen der Statistik, dass die Daten nach ihrer statistischen Aufbereitung für die verschiedensten, nicht von vornherein bestimmbaren Aufgaben verwendet werden sollen.[31] Dies gilt gleichermaßen für Big-Data Analysemethoden, weshalb es naheläge, auch für sie eine konkrete, enge Zweckbindung nicht zu verlangen. Statistische Zwecke beschränken sich nicht von vornherein auf eine bestimmte inhaltliche Verarbeitung von Daten, sondern Statistik ist zunächst einmal lediglich ein Verfahren, das zu allen möglichen inhaltlichen Zwecken angewendet werden kann.[32] Die Datenschutzgrundverordnung lässt nicht eindeutig darauf schließen, ob mit den statistischen Zwecken allein solche Datenverarbeitungen erfasst sein sollen, die im öffentlichen Interesse liegen, oder auch Datenverarbeitungen zu kommerziellen Zwecken. Der Wortlaut von Art. 5 Abs. 1 lit. b) Hs. 2 DSGVO legt eher nahe, dass allein die Archivzwecke im öffentlichen Interesse liegen müssten, nicht aber auch die statistischen Zwecke. Die Vorgängernorm Art. 6 Abs. 1 lit. b) S. 2 der Datenschutzrichtlinie[33] lässt sich dagegen eher so auslegen, dass die statistischen Zwecke jedenfalls nicht im kommerziellen Interesse liegen dürfen.[34] Dies erschließt sich aus

[29] *Weichert*, ZD 2013, 251, 256; *Culik/Döpke*, ZD 2017, 226, 230.
[30] *Boehme-Neßler* (oben Fn.12); *Kring* (o. Fußn. 26), S. 553 m.w.Nachw., abrufbar unter: https://subs.emis.de/LNI/Proceedings/Proceedings232/551.pdf, zuletzt abgerufen am 11.08.2017.
[31] *BVerfG*, NJW 1984, 419, 423 – Volkszählung.
[32] *Richter*, DuD 2015, 735, 738.
[33] 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.
[34] Ebenso: *Richter*, DuD 2015, 735, 738; *Culik/Döpke*, ZD 2017, 226, 230; kommerzielle Zwecke dagegen jedenfalls nicht von vorneherein ausschließend: Art. 29 Gruppe, S. 28, opinion 03/13 on purpose limitation, 00569/13/ENWP203, abrufbar unter: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf, zuletzt abgerufen am 09.09.2017.

der im Zusammenhang erfassten Nennung anderer nicht-kommerzieller Zwecke (historische und wissenschaftliche Zwecke), die dem geänderten Kommissionsentwurf entstammt.[35]

Auch das BVerfG wollte mit dem Begriff der Statistik allein solche Datenverarbeitungen privilegieren, die im öffentlichen Interesse (hier: einer Volkszählung) erfolgen, nicht aber gleichzeitig auch kommerzielle Zwecke. Gleiches gilt für die Privilegierung statistischer Zwecke in der Datenschutzrichtlinie. Bei Berücksichtigung dieser teleologischen und historischen Erwägungen lässt sich nicht begründen, dass die Zweckangabe von Big-Data Analysemethoden ähnlich weit ausfallen darf, wie dies bei statistischen Zwecken im öffentlichen Interesse der Fall ist.

(2) Datenverarbeitung für Werbezwecke als ausreichende Zweckangabe?

Geht man davon aus, dass ein wesentlicher Anteil von Datenverarbeitungen zum Zweck der Markt- und Meinungsforschung bzw. zur anschließenden Kundenprofilbildung und individuellen Werbeansprache erfolgt, stellt sich die Frage, ob sich als legitimer Zweck nicht die Werbung bzw. das Marketing eignen würde. Vertreten ließe sich hier einerseits, unter den Zweck „Werbung" oder „Marketing" würden eine Reihe von Werbemaßnahmen vereint (Kundenansprache durch Zeitung, Telefonmarketing, Email-Ansprache, Echtzeitwerbung im Internet etc.) aber selbst Produkt- und Dienstleistungsforschung ließen sich hierunter fassen, sodass die Zweckbestimmung zu unbestimmt sei. Andererseits könnte ebenso argumentiert werden, dem Kunden komme es allein auf den „Endzweck" der Werbeansprache an, unabhängig davon, in welcher Form diese vorgenommen wird und welche Tätigkeiten ihr vorangehen.[36] Hierfür spricht auch ErwG 47 S. 7 DSGVO, der „Zwecke der Direktwerbung" explizit als legitimen Zweck im Rahmen der Interessenabwägung anerkennt, ohne dass dieser präzisiert werden müsste. Eine Festlegung auf entsprechende Zwecke der Direktwerbung kommt damit durchaus in Betracht, ist aber nicht unumstritten.

(3) Datenverarbeitung zu Zwecken der Persönlichkeitsprofilbildung

Die Auswertung und Zusammenführung von Daten zu Persönlichkeitsprofilen, wie sie z.T. durch Big-Data Analysetools im Vorfeld intendiert ist, wäre von dieser Zweckbestimmung aber

[35] Vgl. KOM(92)0422, S. 30, 43.
[36] Zum Meinungsstand vgl. *Kring* (o. Fußn. 26), S. 553 m.w.Nachw. in Fußn. 59-67, abrufbar unter: https://subs.emis.de/LNI/Proceedings/Proceedings232/551.pdf, zuletzt abgerufen am 11.08.2017.

dennoch nicht erfasst, sondern ein eigener und zudem illegitimer Zweck. Denn das BVerfG hat sowohl im Volkszählungsurteil, als auch in seinem Urteil zur Verfassungsmäßigkeit einer Repräsentativstatistik festgehalten, dass eine umfassende Registrierung und Katalogisierung der Persönlichkeit durch die Zusammenführung einzelner Lebens- und Personaldaten zur Erstellung von Persönlichkeitsprofilen der Bürger selbst in der Anonymität statistischer Erhebungen unzulässig ist.[37] Das BVerfG schlussfolgert die Unzulässigkeit der Erstellung von Teil- oder Totalabbildungen der Person aus der unverzichtbaren Menschenwürdegarantie des Art. 1 GG. Gilt dies selbst für den durch die Rechtsprechung privilegierten Zweck der statistischen Erhebung im öffentlichen Interesse, so muss dies erst recht für den nicht-privilegierten kommerziellen Zweck der Persönlichkeitsprofilbildung durch Auswertung und Zusammenführung von Daten mittels Big-Data Analysemethoden gelten.

In der Literatur wird diese Auffassung jedenfalls dann für die Erstellung von Persönlichkeitsprofilen geteilt, wenn nicht nur Einzeldaten zusammengetragen, sondern auch ausgewertet werden mit dem Ziel der Abbildung der Konsumentenpersönlichkeit.[38] Dort, wo Daten nur als Einzeldaten in Dateien gesammelt werden, ohne dass diese Sammlung mehr Informationen enthielte als die Summe der Einzelinformationen, soll eine Datenverarbeitung dagegen zulässig sein können.[39] Das OLG Frankfurt erachtet eine Datenverarbeitung im Einzelfall selbst dann als zulässig, wenn sich aus der Gesamtzahl der ermittelten Lebensumstände ein relativ detailliertes Gesamtbild eines Persönlichkeitsprofils erstellen lässt.[40] Die Rechtsprechung des OLG Frankfurt dürfte mit dem Volkszählungsurteil, das explizit von einem Menschenwürdeverstoß bei Voll- oder Teilabbildung (freilich kann hier aber nur eine Teilabbildung ab einem bestimmten Grad, der im Einzelfall zu bestimmen sein wird, gemeint sein) der Person spricht, nicht in Einklang stehen. Es ist kein kommerzielles Interesse ersichtlich, das eine derart starke Gefährdung des Persönlichkeitsrechts des Betroffenen, wie sie durch die Bildung von Persönlichkeitsprofilen eintritt, rechtfertigen könnte. Auch zwischen Fallkonstellationen zu differenzieren, in denen eine Datenauswertung bereits stattgefunden oder noch nicht stattgefunden hat, ist mit Blick auf die Gefahr für das Persönlichkeitsrecht

[37] *BVerfG*, NJW 1984, 419, 424 – Volkszählung; *BVerfG*, NJW 1969, 1707, 1707 – Repräsentativstatistik; *Roßnagel*, ZD 2013, 562, 565; *Schaar*, RDV 2013, 223, 225.
[38] *Wittig*, RDV 2000, 59, 61.
[39] *Wittig*, RDV 2000, 59, 61; *Moos*, MMR 2006, 718, 721.
[40] *Moos*, MMR 2006, 718, 721; *OLG Frankfurt/M.*, CR 2001, 294, 296; vgl. zu dieser Frage auch: *Scholz*, in: Roßnagel, Handbuch Datenschutzrecht, 2003, S. 1833, 1864.

nicht angezeigt. Denn die Möglichkeit der Auswertung kann mit Hilfe der heute zur Verfügung stehenden Analysemethoden durch einen einzigen Klick vollzogen werden. Unzulässig ist daher bereits die Voll- oder Teilabbildung des Betroffenen durch die Zusammenstellung von Einzeldaten zu einem Persönlichkeitsprofil und dies auch dann, wenn diese Sammlung in Ermangelung einer Auswertung der Einzeldaten nicht mehr Informationen enthält als die Summe der Einzelinformationen.

Werden Daten mit dem Ziel der Analyse mittels Big-Data Anwendungen erhoben, so steht dies regelmäßig im Konflikt mit dem Zweckbindungsgrundsatz, wenn man die Festlegung auf Zwecke der Direktwerbung für nicht ausreichend erachtet oder wenn auch über diesen Zweck hinausgehende Zwecke verfolgt werden. Die Zusammenführung von Daten zur Teil- oder Totalabbildung einer Person ist als illegitimer Zweck nicht geeignet, eine Datenverarbeitung zu rechtfertigen.

(4) Durchbrechung des Zweckbindungsgrundsatzes

Der Zweckbindungsgrundsatz wird allerdings in seiner durch die Datenschutzgrundverordnung erlangten Fassung durchbrochen. Nicht neu ist dabei allerdings, dass eine Verarbeitung zu anderen Zwecken als dem Primärzweck möglich ist mit Einwilligung des Betroffenen. Ist also bei Big-Data Analysen nicht im Vorfeld erkennbar, für welche Zwecke die Daten ausgewertet werden sollen, sondern ergibt sich dies erst zu einem späteren Zeitpunkt, wäre eine Zweckänderung mit Einwilligung des Betroffenen durchaus erreichbar. Ob dies in der Praxis in Anbetracht der Vielzahl möglicher Zwecke einer Datenauswertung mittels Big-Data Analysemethoden allerdings umgesetzt werden kann, erscheint mehr als fraglich.[41]

Eine Durchbrechung des Zweckbindungsgrundsatzes kann auch auf Grundlage einer Rechtsvorschrift der Union oder aber eines Mitgliedstaates erfolgen und dies selbst dann, wenn Primär- und Sekundärzweck nicht miteinander vereinbar sind. Hier hat der Gesetzgeber insoweit wesentlichen Spielraum zur Durchbrechung des Zweckbindungsgrundsatzes durch Art. 6 Abs. 4 DSGVO und ist allein an die Vorgaben des Art. 23 DSGVO gebunden.[42]

[41] Vgl. hierzu etwa: *Culik/Döpke*, ZD 2017, 226, 228.
[42] Im Einzelnen: *Culik/Döpke*, ZD 2017, 226, 228.

Ohnehin aber verlangt es der Zweckbindungsgrundsatz einzig, dass Daten nicht zu Zwecken weiterverarbeitet werden, die nicht mit dem Primärzweck der Datenerhebung unvereinbar sind. Sind Primär- und Sekundärzweck aber miteinander vereinbar, so bedarf es für die Weiterverarbeitung weder einer Einwilligung des Betroffenen, noch einer Rechtsgrundlage im nationalen oder im Unionsrecht.[43] Der Primärzweck, auf den sich die Verarbeitung bezieht, wird damit zum Maßstab der Beurteilung, welche Weiterverarbeitung gestattet ist.[44] Ob eine Vereinbarkeit von Primär- und Sekundärzweck vorliegt, richtet sich maßgeblich nach ErwG 50 S. 6 DSGVO. Danach ist v.a. zu berücksichtigen,

> *„ob ein Zusammenhang zwischen den Zwecken, für die die personenbezogenen Daten erhoben wurden, und den Zwecken der beabsichtigten Weiterverarbeitung besteht, in welchem Kontext die Daten erhoben wurden, insbesondere die vernünftigen Erwartungen der betroffenen Person, die auf ihrer Beziehung zu dem Verantwortlichen beruhen, in Bezug auf die weitere Verwendung dieser Daten, um welche Art von personenbezogenen Daten es sich handelt, welche Folgen die beabsichtigte Weiterverarbeitung für die betroffenen Personen hat und ob sowohl beim ursprünglichen als auch beim beabsichtigten Weiterverarbeitungsvorgang geeignete Garantien bestehen."*

Im Ergebnis ist also eine Interessenabwägung unter Einbeziehung aller Einzelfallumstände vorzunehmen.[45] Es existieren aber auch von vorneherein privilegierte Sekundärzwecke, wie statistische und wissenschaftliche Zwecke, Art. 89 DSGVO.[46] In ErwG 157 DSGVO werden dabei ausdrücklich die potentiellen Erkenntnisgewinne für die Medizin durch die Verknüpfung von Informationen als zulässiger wissenschaftlicher Sekundärzweck hervorgehoben.[47] Das auf die Unvereinbarkeit mit dem Ursprungszweck reduzierte Verbot der Weiterverarbeitung enthält

[43] ErwG 50 S. 1, 2 DSGVO; *Härting*, Datenschutz-Grundverordnung, 2016, Rdnr. 515; *Culik/Döpke*, ZD 2017, 226, 230.
[44] *Frenzel,* in: Paal/Pauly (o. Fußn. 14), Art. 5 DSGVO Rdnr. 30; zum Prinzip der kompatiblen Weiterverarbeitung vgl. auch: Monreal, ZD 2016, 507 ff.
[45] *Härting* (o. Fußn. 43), Rdnr. 516 ff.; *Culik/Döpke*, ZD 2017, 226, 229.
[46] Zur Auslegung der statistischen Zwecke vgl. bereits oben.
[47] *Grages,* in: Plath, BDSG/DSGVO, 2. Aufl. (2017), Art. 89 DSGVO Rdnr. 2; vgl. auch: *Paal/Hennemann*, NJW 2017, 1679, 1700; zu Big Data in der Medizin: *Schwab/Becker*, ZD 2015, 151 ff.; *Spindler*, MedR 2016, 691 ff.; *Timm*, MedR 2016, 681.

weiterhin ein Wertungselement, das auch andere als die in Art. 89 DSGVO benannten Zwecke zulässig erscheinen lässt.[48]

Für das Verbot der Weiterverarbeitung muss außerdem nachgewiesen werden, dass die Weiterverarbeitung mit dem Ursprungszweck nicht zu vereinbaren ist, was die Darlegungslast zugunsten einer Lockerung der Zweckbindung modifiziert.[49] Erreicht die Datenverarbeitung aber auch zu einem grds. legitimen Sekundärzweck einen solchen Umfang, dass aus den Daten potentiell ein Persönlichkeitsprofil zusammengestellt werden könnte, so dürfte eine Weiterverarbeitung zu diesen Zwecken regelmäßig nicht mit dem Ursprungszweck vereinbar sein. Der Sekundärzweck wird hierdurch zu einem von der Rechtsordnung missbilligten Zweck.[50] Insgesamt lässt sich aber sagen, dass dann, wenn die Daten zu einem legitimen Zweck erhoben wurden und der Sekundärzweck ausreichend eng und legitim gefasst wird, eine Big-Data Analyse zu diesem Zweck zulässig sein kann.[51] Eine generelle Ausnahme zugunsten von Big-Data Analysen kennt die Datenschutzgrundverordnung allerdings nicht, sodass es stets einer umfassenden Interessenabwägung im Einzelfall bedarf.[52]

bb) Grundsatz der Datenminimierung und der Speicherbegrenzung, Transparenzgrundsatz

Nach dem Grundsatz der Datenminimierung müssen personenbezogene Daten dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein.[53] Erheblichkeit meint dabei, dass die Datenverarbeitung geeignet sein muss, den verfolgten Zweck zu erreichen.[54] Die Verarbeitung personenbezogener Daten muss ferner auf das für die verfolgten Zwecke notwendige Maß begrenzt und die personenbezogenen Daten, die verarbeitet werden, müssen dem Zweck angemessen sein. Dies verlangt eine wertende Betrachtung, ob die Verarbeitung von Daten in diesem Umfang im engeren Sinne verhältnismäßig ist.[55] Die Rechtmäßigkeit der Datenverarbeitung orientiert sich damit wesentlich an dem mit der Datenverarbeitung verfolgten Zweck. Da sich dieser bereits nur

[48] *Frenzel,* in: Paal/Pauly (o. Fußn. 14), Art.5 DSGVO Rdnr. 30.
[49] *Frenzel,* in: Paal/Pauly (o. Fußn. 14), Art.5 DSGVO Rdnr. 30.
[50] Siehe hierzu bereits oben.
[51] *Dammann*, ZD 2016, 307, 313 ff.
[52] Sehr viel weitergehender: *Helbig*, K&R 2015, 145 ff.
[53] *Reimer,* in: Sydow (o. Fußn. 14), Art. 6 Rdnr. 67; *Frenzel,* in: Paal/Pauly, (o. Fußn. 14), Art.5 DSGVO Rdnr. 34 ff.; *Schantz,* in: BeckOK Datenschutzrecht, (o. Fußn. 18), Art. 5 DSGVO Rdnr. 24 ff.
[54] *Schantz,* in: BeckOK Datenschutzrecht, (o. Fußn. 18), Art. 5 DSGVO Rdnr. 24.
[55] *Frenzel,* in: Paal/Pauly, (o. Fußn. 14), Art.5 DSGVO Rdnr. 35; *Schantz,* in: BeckOK Datenschutzrecht, (o. Fußn. 18), Art. 5 DSGVO Rdnr. 25, 26.

schwerlich für Big-Data Analysen festlegen lässt, besteht bei Big-Data Analysen regelmäßig auch ein hohes Risiko, gegen den Grundsatz der Datenminimierung zu verstoßen. Gleiches gilt für den Grundsatz der Speicherbegrenzung, Art. 5 Abs. 1 lit. e) DSGVO, der eine Speicherung über den Verarbeitungszweck hinaus untersagt sowie für den Transparenzgrundsatz, der es u.a. erforderlich macht, den Zweck der Datenverarbeitung dem Betroffenen nachvollziehbar darzulegen.[56]

Die betroffene Person hat außerdem das Recht, nicht einer ausschließlich auf einer automatisierten (z.B. durch Big-Data Algorithmen erfolgten) Verarbeitung beruhenden Entscheidung unterworfen zu werden, die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt, Art. 22 DSGVO. Gemeint ist etwa die allein auf Algorithmen beruhende Ablehnung eines Darlehensvertrags.[57]

cc) Informierte Einwilligung

Ein weiteres grundlegendes Problem ist die Einholung einer informierten Einwilligung in Fällen, in denen eine massenhafte Datenauswertung erfolgen soll. Dies liegt einerseits daran, dass bereits der Zweck der Datenverarbeitung nur schwerlich präzise angegeben werden kann (s.o.).[58] Gelingt dies noch, so stellt sich dennoch die Frage, wie die Rechtswirksamkeit der Einwilligung sichergestellt werden kann. Hier stellen sich mannigfaltige Probleme der zur Einwilligung erforderlichen Informationsvermittlung, wobei es sich um allgemeingültige Probleme der Einwilligung handelt, die nicht allein den Bereich massenhafter Datenverarbeitung betreffen. Ob und wie eine tatsächlich selbstbestimmte Entscheidung über datenschutzrechtliche Belange gewährleistet werden kann, erscheint derzeit mehr als fraglich. Beim autonomen Fahren ließe sich beispielsweise darüber nachdenken, ob eine wirksame Einwilligung zur Datenübermittlung bereits im Kaufzeitpunkt des PKW eingeholt werden kann und wie weit diese reichen könnte. Ohne hier auf alle Probleme der informierten Einwilligung und ihrer Sinnkrise im digitalen Zeitalter eingehen zu können, lässt sich doch jedenfalls statuieren, dass die Wirksamkeit der datenschutzrechtlichen Einwilligung ganz

[56] Vgl. im Einzelnen: *Frenzel,* in: Paal/Pauly, (o. Fußn. 14) Art. 5 DSGVO Rdnr. 21.
[57] Erwägungsgrund 71; *Dix*, STADTFORSCHUNG UND STATISTIK 2016, S. 59, 61, abrufbar unter: https://www.eaid-berlin.de/wp-content/uploads/2016/05/StSt-1-2016_Dix.pdf, zuletzt abgerufen am: 08.09.2017.
[58] Siehe hierzu bereits oben.

erheblich in Frage steht und damit zum Unsicherheitsfaktor wird, wenn es um die Einhaltung datenschutzrechtlicher Vorgaben geht.[59]

dd) Erlaubnistatbestände

Kann die intendierte Auswertung und Zusammenführung von Daten nicht oder nur mit nicht unerheblicher Rechtsunsicherheit auf die Einwilligung gestützt werden, stellt sich letztlich die Frage, ob nicht ein Erlaubnistatbestand die entsprechende Datenverarbeitung gestattet. In Betracht kommt hier insbesondere Art. 6 Abs. 1 lit. f DSGVO. Danach ist eine Datenverarbeitung rechtmäßig, wenn sie zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt. Die Verarbeitung sensibler Daten ist nach Art. 9 DSGVO grundsätzlich untersagt und nur in den engen Grenzen des Art. 9 Abs. 2 DSGVO ausnahmsweise zulässig. Eine solche Ausnahme ist beispielsweise unter bestimmten Umständen gegeben, wenn die Datenverarbeitung auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats, aus Gründen eines wichtigen öffentlichen Interesses oder auch für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke erforderlich ist, Art. 9 Abs. 2 lit. g), lit. j) DSGVO.[60]

Während es Art. 9 Abs. 2 lit. g), j) DSGVO den Mitgliedstaaten erlaubt, eine Ausnahmeregelung zur Verarbeitung sensibler personenbezogener Daten zu erlassen und sie so legitim auszugestalten, verlangt Art. 6 Abs. 1 lit. f DSGVO zur Beurteilung der Rechtmäßigkeit der Datenverarbeitung eine Abwägung in jedem Einzelfall. Art. 6 Abs. 1 lit. f DSGVO gilt dabei gerade für Gleichordnungsverhältnisse unter Privaten.[61] Im Wege der Abwägung werden die zu wahrenden berechtigten Interessen des Verantwortlichen bzw. eines Dritten und die berechtigten Rechte und Interessen des Betroffenen zueinander ins Verhältnis gesetzt. Das berechtigte Interesse des Verantwortlichen bzw. des Dritten ist dabei weit zu verstehen und kann nach ErwG 47 S. 7 DSGVO auch in gerade in der Verarbeitung zum Zwecke der

[59] Vgl. dazu eingehend: *Specht/Schröder/Bienemann*, Die Chancen der Visualisierung, Handbuch Datenrecht in der Digitalisierung, im Erscheinen; *Culik/Döpke*, ZD 2017, 226, 229.
[60] Zur Anwendung von Big-Data Analysemethoden auf sensible Daten, vgl. *Schneider*, ZD 2017, 303 ff.
[61] *Frenzel,* in: Paal/Pauly (o. Fußn. 14), Art. 6 Rdnr. 27.

Direktwerbung liegen.[62] Die Erfassung auch wirtschaftlicher Interessen erfolgte bereits im Anwendungsbereich des § 28 BDSG. Dabei galt aber jedenfalls im deutschen Recht bislang, dass die berechtigten Interessen der verantwortlichen Stelle nicht eine beliebige Zweckentfremdung der gespeicherten Daten rechtfertigen.[63] Soll der Zweckbindungsgrundsatz nicht unterlaufen werden, muss dies auch im Anwendungsbereich der DSGVO weiterhin Geltung beanspruchen können. Dies bedeutet aber, dass die massenhafte Datenauswertung über den Primärzweck hinaus nicht über Art. 6 Abs. 1 lit. f DSGVO gerechtfertigt werden kann.

b) Lösungsmöglichkeit: Erlaubnistatbestand zwecks Anonymisierung von Daten

Eine Möglichkeit, Daten unter Einhaltung der datenschutzrechtlichen Vorgaben auch über Big-Data Analysemethoden zu verarbeiten, ist die Anonymisierung der Daten. Anonymisieren ist nach ErwG 26 DSGVO das Verändern personenbezogener Daten derart, dass die hinter den Einzelangaben über persönliche oder sachliche Verhältnisse stehende betroffene Person nicht bzw. nicht mehr identifiziert werden kann.[64] Eine bloße Pseudonymisierung, die die Möglichkeit der Identifizierung nicht gänzlich ausschließt, genügt nicht.

Ob eine Identifikation der betroffenen Person bei den derzeit und zukünftig zur Verfügung stehenden Möglichkeiten der De-Anonymisierung überhaupt gänzlich ausgeschlossen werden kann, erscheint zwar fraglich,[65] soll für die nachfolgenden Ausführungen aber unterstellt sein. Hier könnte es durchaus sinnvoll sein, technische Standards zu normieren, bei deren Einhaltung eine Anonymisierung unwiderleglich vermutet und eine De-Anonymisierung gesetzlich verboten, ggf. sogar strafbar oder als Ordnungswidrigkeit ausgestaltet, jedenfalls aber mit einem Bußgeld belegt wird. Sollen datengetriebene Geschäftsmodelle jedenfalls dort unterstützt werden, wo sie auch im gesellschaftlichen Interesse liegen (Forschung und Entwicklung, medizinische Versorgung, vernetztes Fahren etc.), so erscheint dies unerlässlich.

Auch eine Anonymisierung der Daten erfordert es aber, die Daten zunächst nicht anonymisiert zu speichern, um sie anschließend dem Anonymisierungsvorgang zu unterziehen. In Bereichen

[62] Vgl. auch: *Frenzel,* in: Paal/Pauly (o. Fußn. 14), Art. 6 Rdnr. 28.
[63] *Simitis*, in: Simitis, Bundesdatenschutzgesetz, 8. Aufl. (2014), § 28 Rdnr. 99; *Mattke,* Adressenhandel, 1995, S. 191; *Breinlinger,* RDV 1997, 247, 249 ff.
[64] Vgl. *Ernst,* in: Paal/Pauly (o. Fußn. 14), Art. 4 DSGVO Rdnr. 48.
[65] Hierzu eingehend: *Boehme-Neßler* (o.Fußn. 12), S. 422.

wie der Erhebung von Fahrverhaltensdaten zur Produktverbesserung aber auch beim Einsatz von Smart Devices, die nun einmal einer bestimmten Person zugeordnet sind, erscheint es schwierig, wenn nicht gar ausgeschlossen, bereits die Erhebung der Daten anonymisiert erfolgen zu lassen. Da die Datenerhebung zu Zwecken der Auswertung mittels Big-Data Analysemethoden auch nur schwerlich auf einen Erlaubnistatbestand oder eine Einwilligung gestützt werden kann, ließe sich über einen Erlaubnistatbestand ähnlich § 44a UrhG zur kurzfristigen Zwischenspeicherung zwecks Anonymisierung der Daten nachdenken. Dies wäre ein wesentlicher Schritt, um gerade solche Datenverarbeitungen zu rechtfertigen, an denen Gesellschaft, Politik und Wissenschaft ein Interesse haben. Daten aus vernetzten Fahrzeug, Smart Devices etc. ließen sich so rechtssicher erheben, das informationelle Selbstbestimmungsrecht des Betroffenen würde aber dadurch geschützt, dass die Daten automatisiert in anonymisierte Daten umgewandelt und die Ausgangsdaten anschließend gelöscht würden. Auch hier bedarf es aber ausreichender Regulierung der Anonymisierungstechnik, um die Löschung unwiederbringlich auszugestalten und das informationelle Selbstbestimmungsrecht damit ausreichend zu schützen.

Alternativ zu einem entsprechend eindeutig ausgestalteten Erlaubnistatbestand, der freilich einer Einigung auf europäischer Ebene bedürfte, könnte es sich auch anbieten, jedenfalls für die Verarbeitung nicht-sensibler Daten Leitlinien für die Abwägung im Rahmen des Art. 6 Abs. 1 lit. f DSGVO zu erlassen, die die Anwendung des Erlaubnistatbestands auf die gesamtgesellschaftlich erwünschten Datenverarbeitungen bei entsprechender Anonymisierung der Daten festschreiben. Auch auf diesem Wege ließe sich sicherlich zu mehr Rechtssicherheit beitragen, als es derzeit ohne leitende Vorgaben zur Interessenabwägung der Fall ist.

IV. Fazit

Im Ergebnis existieren drei Möglichkeiten, das Verhältnis von Datenrechten und Datenschutz auszugestalten. Das Datenschutzrecht könnte zunächst als Zuweisungskriterium für ein Recht an personenbezogenen Daten fungieren sowie als Beteiligungsinstrument des Betroffenen im Falle von Datenhingaben als Gegenleistung im Vertragsverhältnis. Für beide Mechanismen müsste das Datenschutzrecht seines rein ideellen Schutzes des informationellen

Selbstbestimmungsrechtes entkleidet und als auch dem Schutz kommerzieller Interessen dienend anerkannt werden.

Das Datenschutzrecht als Zuweisungskriterium taugt aber bereits deshalb nicht, weil es für nicht-personenbezogene Daten versagt. Verschiedene Zuweisungskriterien für personenbezogene und nicht-personenbezogene Daten zu etablieren, scheint aufgrund der Umwandlungsmöglichkeit beider Datenkategorien nicht zweckdienlich. Das Datenschutzrecht als Beteiligungsinstrument scheitert derzeit noch an der fehlenden Wertbestimmungsmöglichkeit von Daten, ist aber jedenfalls im Falle einer Verabschiedung der Richtlinie über digitale Inhalte zwingend mit zu bedenken, auch wenn hier sicherlich zunächst ein rechtspolitischer Konsens zu erzielen ist, ob einer solchen Beteiligung des Betroffenen nicht das informationelle Selbstbestimmungsrecht entgegensteht.

Zumindest aber beschränkt das Datenschutzrecht ein mögliches Datenrecht unabhängig von dessen Ausgestaltung und dies in einer Art und Weise, dass es ein Datenrecht jedenfalls in seinem Nutzungsumfang ganz erheblich beschränkt, wenn nicht gar gänzlich entleert. Dies wäre insbesondere misslich, wenn anstelle eines umfassenden Datenrechts mit Nutzungs- und Ausschlussfunktion lediglich Einzelnutzungsbefugnisse oder Zugriffsrechte zugewiesen würden. Diese wären für den Rechteinhaber möglicherweise weitgehend wertlos. Eine ganz erhebliche datenschutzrechtliche Beschränkung ergibt sich dabei für Daten, die über Big-Data Analysemethoden zu kommerziellen Zwecken ausgewertet werden sollen, aber auch eine Datenverarbeitung zu Forschungszwecken oder auch zur Produktweiterentwicklung ist mit erheblichen rechtlichen Risiken belastet, was insbesondere für die Datenerhebung beim autonomen bzw. automatisierten Fahren gilt. Soll eine vermehrt datengetriebene Wirtschaft tatsächlich auf rechtssicherer Grundlage agieren können, empfiehlt sich ein Erlaubnistatbestand ähnlich § 44a UrhG, der kurzfristige Zwischenspeicherungen zu Zwecken der Anonymisierung von Daten gestattet oder aber die Ausgestaltung von Leitlinien zur Abwägung im Rahmen des Art. 6 Abs. 1 lit. f DSGVO, die ebenfalls zu mehr Rechtssicherheit beitragen würden.